

# NSX-T 管理ガイド

更新日：2017 年 12 月 21 日

VMware NSX-T Data Center 2.1



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。このドキュメントに関するご意見およびご感想は、[docfeedback@vmware.com](mailto:docfeedback@vmware.com) までお送りください。

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

ヴァイ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 © 2014 - 2017 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

## VMware NSX-T の管理について 9

### 1 論理スイッチと仮想マシン接続の設定 10

BUM フレーム レプリケーション モードの理解 11

論理スイッチの作成 12

レイヤー 2 ブリッジ 13

ブリッジ クラスタの作成 14

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 15

NSX Edge アップリンク用の VLAN 論理スイッチの作成 17

論理スイッチへの仮想マシンの接続 19

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 19

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 20

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 25

レイヤー 2 接続のテスト 26

### 2 論理スイッチ ポート 30

論理スイッチ ポートの作成 30

論理スイッチ ポート アクティビティの監視 31

### 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 33

QoS スイッチング プロファイルの理解 34

カスタムの QoS スイッチング プロファイルの設定 35

ポート ミラーリング スイッチング プロファイルの理解 37

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 37

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 39

IP アドレス検出 スイッチング プロファイルの理解 39

IP アドレス検出 スイッチング プロファイルの設定 40

SpoofGuard の理解 41

ポート アドレス バインドの設定 42

スイッチ アドレス バインドの設定 42

SpoofGuard のスイッチング プロファイルの設定 43

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 44

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 44

MAC 管理 スイッチング プロファイルの理解 45

MAC 管理 スイッチング プロファイルの設定 46

カスタム プロファイルと論理スイッチの関連付け 47

論理ポートとカスタム プロファイルの関連付け 48

## 4 Tier-1 論理ルーター 50

- Tier-1 論理ルーターの作成 51
- Tier-1 分散論理ルーターのダウンリンク ポートの追加 52
- 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 53
- Tier-1 論理ルーターのスタティック ルートの設定 55

## 5 Tier-0 論理ルーター 58

- Tier-0 分散論理ルーターの作成 59
- Tier-0 と Tier-1 の接続 60
  - 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 62
- VLAN 論理スイッチへの Tier-0 論理ルーターの接続 63
  - Tier-0 分散論理ルーターおよび TOR の接続の確認 64
- ループバック ルーター ポートの追加 66
- スタティック ルートの設定 67
  - スタティック ルートの確認 68
- BGP 設定オプション 70
  - Tier-0 論理ルーター上の BGP の設定 71
  - Tier-0 サービス ルーターからの BGP 接続の確認 74
- Tier-0 分散論理ルーター上の BFD の設定 75
- Tier-0 分散論理ルーターのルート再配分を有効にする 76
  - North-South 接続とルート再配分の確認 76
- ECMP ルーティングの理解 79
  - 2 番目の Edge ノードのアップリンク ポートの追加 79
  - 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 81
  - ECMP ルーティング接続の確認 82
- IP プリフィックス リストの作成 83
- ルート マップの作成 84
- 転送タイマーの設定 85

## 6 ネットワーク アドレス変換 87

- Tier-1 NAT 88
  - Tier-1 ルーター上の送信元 NAT の設定 88
  - Tier-1 ルーター上での宛先 NAT の設定 90
  - 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 92
  - 物理アーキテクチャへの Tier-1 NAT ルートのアドバタイズ 92
  - Tier-1 NAT の確認 93
- Tier-0 NAT 94
  - 再帰 NAT 94

## 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 98

- ファイアウォール ルール セクションの追加 99

ファイアウォール ルール セクションの削除	100
セクション ルールを有効または無効にする	100
セクション ログの有効化または無効化	100
ファイアウォール ルールについて	101
ファイアウォール ルールの追加	102
ファイアウォール ルールの削除	105
デフォルトの分散ファイアウォール ルールの編集	106
ファイアウォール ルールの順序の変更	107
ファイアウォール ルールのフィルタ	107
ファイアウォール除外リストの設定	108
ファイアウォールの有効化と無効化	108
論理ルーターへのファイアウォール ルールの追加または削除	109

## 8 分散ネットワーク暗号化 110

分散ネットワーク暗号化について	111
DNE がネットワーク パケットを処理する方法	113
DNE 設定の管理	114
暗号化ルール セクションの追加、編集および削除	114
セクション内のすべての暗号化ルールの有効化と無効化	115
セクション内のすべての暗号化ログの有効化と無効化	116
暗号化ルールについて	116
暗号化ルールの追加、クローン作成および削除	118
暗号化ルールの編集	118
暗号化ルールの有効化と無効化	121
暗号化ルールのログの記録の有効化と無効化	122
暗号化ルールの順序の変更	122
暗号化ルールのフィルタリング	123
キー ポリシーについて	123
キー ポリシーの追加、編集および削除	124
キー ポリシーのローテーション	125
キー ポリシーの失効	125

## 9 オブジェクト、グループ、サービス、仮想マシンの管理 127

IP セットの作成	127
IP アドレス プールの作成	128
MAC セットの作成	128
NSGroup の作成	129
サービスとサービス グループの設定	130
NSService の作成	131
仮想マシンのタグの管理	131

## 10 論理ロード バランサ 133

- キー ロード バランサの概念 134
  - ロード バランサ リソースの拡張 134
  - サポートされているロード バランサの機能 135
  - ロード バランサ トポロジ 136
- ロード バランサ コンポーネントの構成 137
  - ロード バランサの作成 138
  - アクティブ健全性モニターの構成 139
  - パッシブ健全性モニターの設定 142
  - ロード バランシング用サーバ プールの追加 143
  - 仮想サーバ コンポーネントの設定 147

## 11 DHCP 166

- DHCP サーバ プロファイルの作成 166
- DHCP サーバの作成 167
- 論理スイッチへの DHCP サーバの接続 168
- 論理スイッチからの DHCP サーバの切り離し 168
- DHCP リレー プロファイルの作成 168
- DHCP リレー サービスの作成 169
- 分散論理ルーター ポートへの DHCP サービスの追加 169

## 12 メタデータ プロキシ 170

- メタデータ プロキシ サーバの追加 170
- 論理スイッチへのメタデータ プロキシ サーバの接続 171
- 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 172

## 13 IP アドレス管理 173

- IP アドレス ブロックの管理 173
- IP アドレス ブロックのサブネットの管理 174

## 14 NSX ポリシー 175

- 概要 175
- 適用ポイントの追加 176
- 通信プロファイルの追加 177
- サービスの追加 178
- ドメインの追加 178
- NSX Policy Manager のバックアップの設定 180
- NSX Policy Manager のバックアップ 180
- NSX Policy Manager のリストア 181
- vIDM ホストと NSX Policy Manager の関連付け 182
- ロールの割り当ての管理 183

## 15 運用管理 184

- ライセンス キーの追加 185
- ユーザー アカウントとロールベースのアクセス コントロールの管理 185
  - CLI ユーザーのパスワードの変更 186
  - 認証ポリシーの設定 186
  - vIDM ホストからの証明書サムプリントの取得 187
  - vIDM ホストと NSX-T の関連付け 188
  - NSX Manager、vIDM、および関連コンポーネント間の時刻の同期 188
  - ロールベースのアクセス制御 190
  - ロールの割り当ての管理 195
- 証明書の設定 195
  - 証明書署名要求ファイルの作成 195
  - CA 証明書のインポート 197
  - 証明書のインポート 197
  - 自己署名証明書の作成 198
  - 証明書の置き換え 199
  - 証明書失効リストのインポート 199
  - CSR の証明書のインポート 200
- アプライアンスの設定 201
- コンピュート マネージャの追加 201
- タグの管理 202
- オブジェクトの検索 203
- リモート サーバの SSH フィンガープリントの検索 204
- NSX Manager のバックアップとリストア 205
  - NSX Manager 設定のバックアップ 206
  - NSX Manager 構成のリストア 208
  - NSX Controller クラスタのリストア 211
- DNE Key Manager のバックアップとリストア 213
- アプライアンスとアプライアンス クラスタの管理 214
  - NSX Manager の管理 214
  - NSX Controller クラスタの管理 215
  - NSX Edge クラスタの管理 221
- ログ収集システム メッセージ 227
  - リモート ログの設定 228
  - ログ メッセージ ID 229
- IPFIX の設定 230
  - スイッチの IPFIX プロファイルの設定 231
  - ファイアウォールの IPFIX コレクタの設定 232
- トレースフローによるバケットのバスのトレース 233
- ポート接続情報の表示 235
- 論理スイッチ ポート アクティビティの監視 235

ポート ミラーリング セッションの開始	236
ファブリック ノードの監視	238
仮想マシンで実行中のアプリケーションのデータの表示	238
プリンシパル ID の表示	239
サポート バンドルの収集	239



# VMware NSX-T の管理について

『NSX-T 管理ガイド』には、VMware NSX-T® 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。

# 論理スイッチと仮想マシン接続の設定

## 1

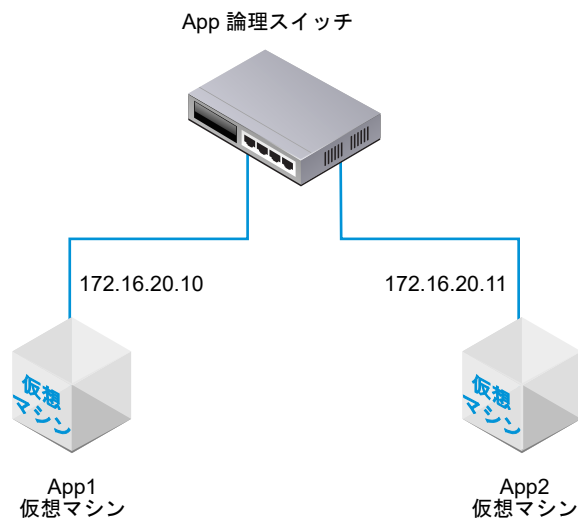
NSX-T 論理スイッチは、基盤となるハードウェアから完全に分離された仮想環境内で、切り替え機能、ブロードキャスト、不明のユニキャスト、マルチキャスト (BUM) トラフィックを再現します。

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。

値の VNI プールを表示および編集するには、NSX Manager にログインし、[ファブリック] - [プロファイル] の順に移動して、[設定] タブをクリックします。プールが小さすぎると、すべての VNI 値が使用されている場合、論理スイッチの作成に失敗します。論理スイッチを削除した場合、VNI 値 が再利用されるのは 6 時間後になります。

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プランニングすることが重要です。

図 1-1. 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 台の仮想マシンを配置するホストやホスト 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ります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、レプリケーターはありません。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

- トランスポート 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。

- トランスポート ノードがトランスポート 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。[1 章 論理スイッチ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 クラスター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スポート ゾーンを選択します。

同じトランスポート 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

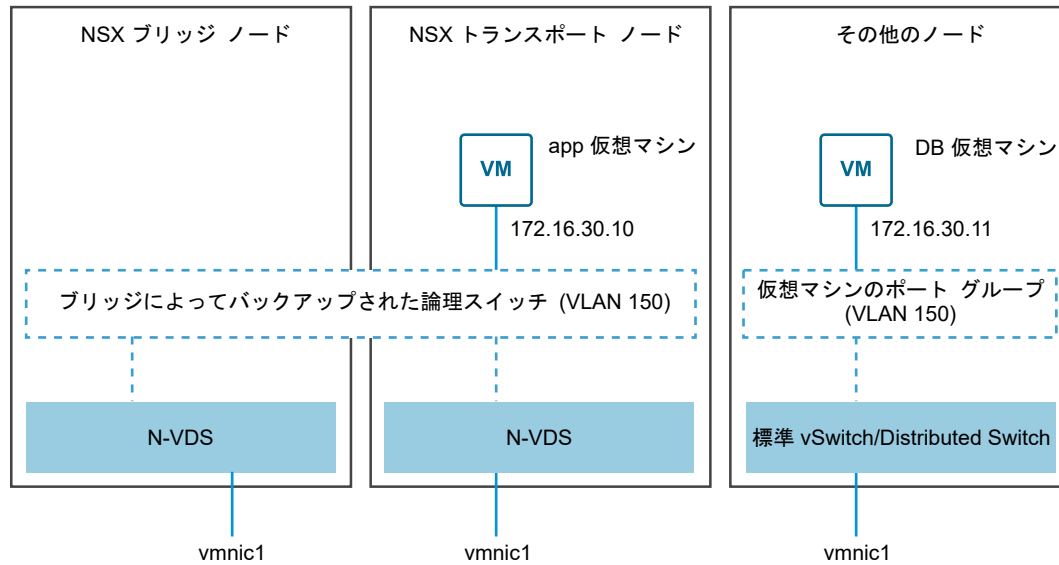
NSX-T 論理スイッチが VLAN でバックアップされたポート グループへのレイヤー 2 接続を必要とする場合、あるいは NSX-T 環境の外部にあるゲートウェイなどの別のデバイスにアクセスする必要がある場合は、NSX-T レイヤー 2 ブリッジを使用することができます。これは、物理ワークロードと仮想ワークロード上でサブネットを分割する必要がある移行シナリオで特に役に立ちます。

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 台の 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。これにより、NSX で管理されている分散仮想スイッチ（以前はホストスイッチと呼ばれていた N-VDS）を、ブリッジで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 1-2. 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 クラスタに属しています。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、ブリッジでバックアップされる論理スイッチと呼ばれます。ブリッジでの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 ゾーンに配置する必要があります。

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で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）仮想マシンを実行する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 Distributed Switch 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 はブリッジで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 台の端末装置の 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 1-2. ブリッジ トポロジ](#)を参照してください。

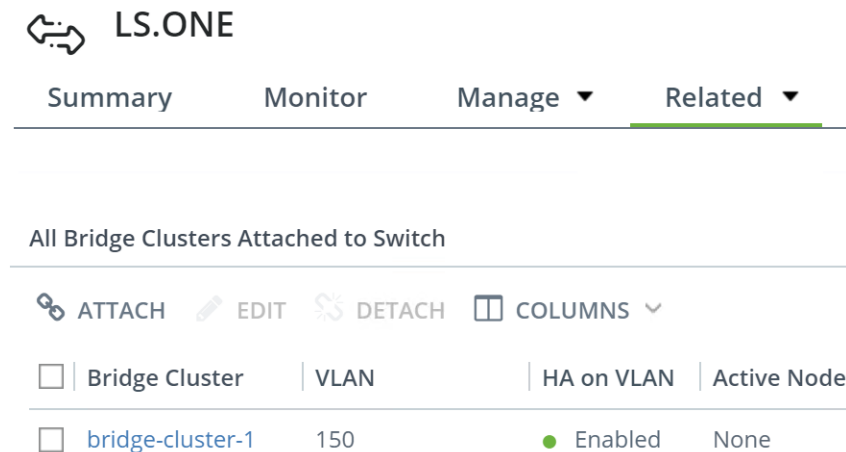
### 前提条件

- 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 ▼

<input type="checkbox"/>	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。

## 結果

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 1-2. ブリッジ トポロジ](#) 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 を送信する必要があります。

[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,
```



```

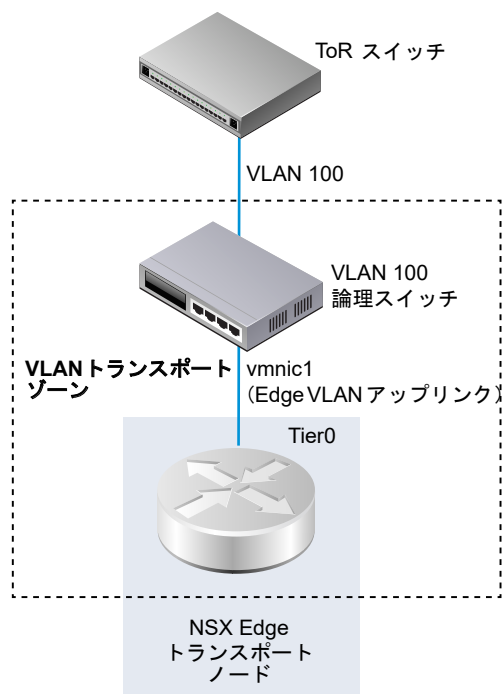
    "multicast_broadcast": 0
  },
  "tx_bytes": {
    "total": 8610134,
    "multicast_broadcast": 0
  },
  "rx_packets": {
    "total": 230,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "last_update_timestamp": 1454979822860,
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"
}

```

## 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、実際に構築するトポロジについて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たものです。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-switches` コマンドを実行します。次はその例です。

```
nsx-edge1> get host-switches

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 NSX Manager (`https://<nsx-mgr>`) 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。

#### 結果

**注：** 同じ VLAN ID を持つ 2 台の VLAN 論理スイッチがある場合、同じ Edge N-VDS (以前のホストスイッチ) に接続することはできません。VLAN 論理スイッチとオーバーレイ論理スイッチがあり、VLAN 論理スイッチの VLAN ID がオーバーレイ論理スイッチのトランスポート VLAN ID と同じ場合も、同じ Edge N-VDS に接続することはできません。

## 次のステップ

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

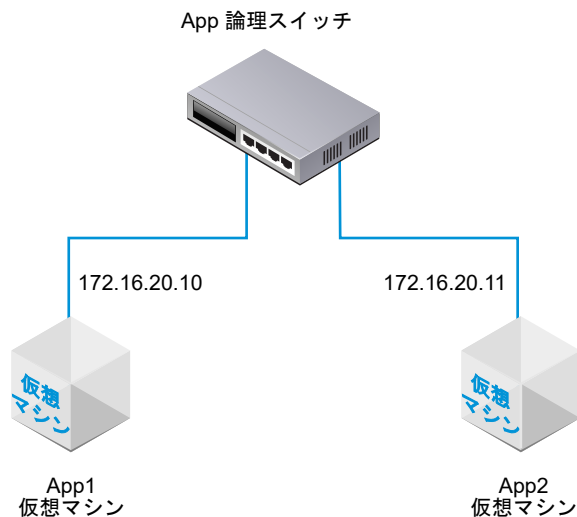
仮想マシンを論理スイッチに接続する設定は、ホストによって異なります。

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。

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)		✓ 接続中
ネットワークアダプタ 2	lswitch301 (nsx.LogicalSwitch)		✓ 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。

## 結果

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、管理と操作の状態で 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。『NSX-T 管理ガイド』で「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。

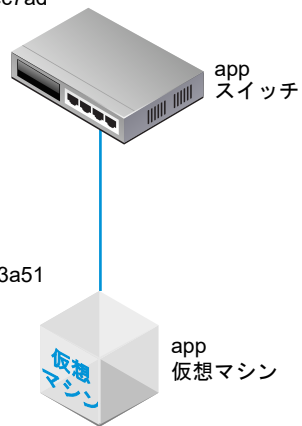
## スタンドアロン ESXi にホストされている仮想マシンの NSX-T 論理スイッチへの接続

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	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": [
    "instanceUid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:[50066bae-0f8a-386b-e62e-b0b9c6013a51]",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUid:4206f47d-fe77-08c5-5bf7-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 /vmsvc/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 /vmsvc/power.off 5]
Powering off VM:

[user@host:~] [vim-cmd /vmsvc/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】

```
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】

```
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。
- 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 /vmsvc/power.on 9]
```

Powering on VM:



## 結果

NSX Manager のユーザー インターフェイスの [スイッチング] > [ポート] で、仮想マシンの externalId と一致する VIF 接続 ID を検出し、管理および運用の状態が [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

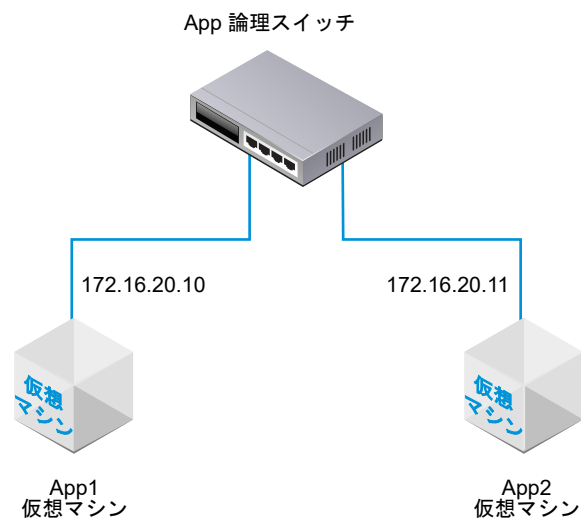
論理ルーターを追加します。

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。『NSX-T 管理ガイド』で「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。



## 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

## 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。

## 結果

[スイッチング] > [ポート] 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

論理ルーターを追加します。

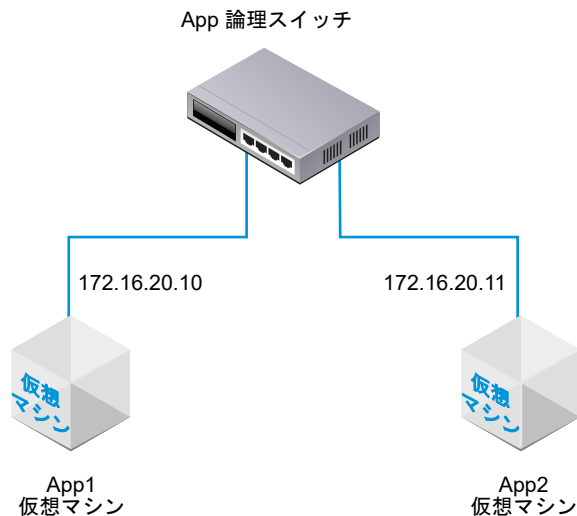
論理スイッチ ポート上でアクティビティを監視して、問題をトラブルシューティングできます。『NSX-T 管理ガイド』で「論理スイッチ ポート アクティビティの監視」を参照してください。

# 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 1-3. 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>

## 結果

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 ポート

# 2

論理スイッチには複数のスイッチ ポートがあります。ルータ、仮想マシン、またはコンテナなどのエンティティは、論理スイッチ ポートを介して論理スイッチに接続できます。

この章には、次のトピックが含まれています。

- [論理スイッチ ポートの作成](#)
- [論理スイッチ ポート アクティビティの監視](#)

## 論理スイッチ ポートの作成

論理スイッチ ポートを使用すると、異なるネットワーク コンポーネント、仮想マシン、またはコンテナを論理スイッチに接続できます。

仮想マシンを論理スイッチに接続する方法については、[論理スイッチへの仮想マシンの接続](#)を参照します。コンテナから論理スイッチへの接続の詳細については、『NSX-T Container Plug-in for Kubernetes - インストールおよび管理ガイド』を参照してください。

---

**注：** コンテナの論理スイッチ ポートにバインドされる IP アドレスと MAC アドレスは、NSX Manager によって割り当てられます。アドレスのバインドは手動で変更しないでください。

---

### 前提条件

論理スイッチ ポートが作成されていることを確認します。[1 章 論理スイッチと仮想マシン接続の設定](#)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)] を選択します。
- 3 [ポート (Ports)] タブをクリックします。
- 4 [追加 (Add)] をクリックします。

- 5 [全般 (General)] タブで、ポートの詳細を完了します。

オプション	説明
名前と説明	名前を入力します。必要に応じて説明も入力します。
論理スイッチ	ドロップダウン リストから論理スイッチを選択します。
管理ステータス	[上 (Up)] または [下 (Down)] を選択します。
添付ファイルの種類	[なし (None)] または [VIF] を選択します。
添付ファイル ID	添付ファイルの種類が VIF の場合、添付ファイル ID を入力します。

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

## 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する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。

ポートのステータスと統計情報が表示されます。

- 5 ホストが学習した MAC アドレスの CSV ファイルをダウンロードするには、[MAC テーブルをダウンロード (Download MAC Table)] をクリックします。

**注：** ホストが KVM の場合、MAC テーブルのダウンロードはサポートされていないため、エラー メッセージが表示されます。

- 6 ポート上のアクティビティを監視するには、[追跡を開始 (Begin Tracking)] をクリックします。

ポート追跡ページが開きます。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。

## 結果

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。



# 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

## 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イッチ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
- スイッチセキュリティ
- 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。

---

デフォルトスイッチングプロファイルやカスタムスイッチ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に関連付けます。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に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に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に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イッチ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イッチ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、デフォルトスイッチングプロファイルまたはカスタムスイッチングプロファイルに関連付けできます。スイッチングプロファイルを論理スイッチに関連付けたり、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](#)
- [論理ポートとカスタム 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、入力方向と出力方向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。これらの設定は帯域幅を保証するものではありませんが、ネットワーク帯域幅の使用を制限する際に利用できます。実際の帯域幅は、ポートのリンク速度またはスイッチング プロファイルの値のいずれか低い方によって決まります。

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、入力方向と出力方向を設定して、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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [スイッチング プロファイル (Switching Profiles)] タブをクリックします。
- 4 [追加 (Add)] をクリックして、[QoS] を選択します。

## 5 QoS スイッチング プロファイルの項目をすべて入力します。

オプション	説明
名前と説明	<p>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。</p> <p>オプションで、プロファイルの変更内容を入力できます。</p>
モード	<p>[モード] ドロップダウン メニューから [信頼される (Trusted)] または [信頼されない (Untrusted)] のいずれかのオプションを選択します。</p> <p>「信頼される」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 アドレス 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 アドレス 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 アドレス 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が使用されます。VLAN ベースの論理ポートの場合、IP/IPv6 パケットの DSCP 値は設定された値が使用されます。「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>
優先順位	<p>CoS の優先順位を設定します。</p> <p>優先順位は 0 から 63 までの値で、0 が最も高い優先順位になります。</p>
サービスのクラス	<p>CoS の値を設定します。</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>
入力方向	<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 トラフィックのカスタム値を指定します。</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 サイズの設定範囲内となります。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、入力方向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 と設定すると、ポリシーによって帯域幅が制限されます。20 バイトでは、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>
入力方向ブロードキャスト	<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 トラフィックにカスタム値を設定します。</p> <p>デフォルト値は 0 で、入力方向ブロードキャスト トラフィックが無効になります。</p> <p>たとえば、論理スイッチの平均帯域幅を 50 Kbps に設定すると、ポリシーによって帯域幅が制限されます。60 バイトでは、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>
出力方向	<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 トラフィックのカスタム値を指定します。</p> <p>デフォルト値は 0 で、出力方向のトラフィックが無効になります。</p>

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

6 [保存 (Save)] をクリックします。

#### 結果

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

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または論理ポートに接続し、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](#)または[論理ポートとカスタム プロファイルの関連付け](#)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

異なる宛先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となる宛先論理ポート ID の IP アドレスを指定します。

## 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 パネルで [スイッチング] をクリックします。
- 3 [スイッチング プロファイル] タブをクリックします。
- 4 [追加] をクリックして、[ポート ミラーリング] を選択します。
- 5 ポート ミラーリングのスイッチング プロファイルの項目をすべて指定します。

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witch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。
方向	この送信元を [入力方向]、[出力方向] または [双方向] 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。 入力方向は、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。 出力方向は、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。
パケット廃棄	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 の 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 アドレス 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 は入力方向を表わし、0 は出力方向を表わします。</li> <li>■ 残りの 6 ビットは未使用です。</li> </ul>
宛先	ミラーリング セッションのコレクタの宛先 ID を入力します。 宛先の IP アドレス 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。宛先 IP アドレスは、カンマ区切りで最大 3 つまで追加することができます。

- 6 [保存] をクリックします。

## 結果

カスタムのポート ミラーリング スwitch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

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に適用します。[カスタム プロファイルと論理スイッチの関連付け](#)または[論理ポートとカスタム プロファイルの関連付け](#)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ことを確認します。

### 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 スヌーピング、ARP スヌーピングまたは VM Tools を使用して仮想マシンの MAC アドレスと 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。

VM Tools は、ESXi ホストの仮想マシン上で実行されるソフトウェアで、MAC アドレスや IP アドレスを含む仮想マシンの構成情報を提供します。この IP アドレス検出方法は、ESXi ホストで実行されている仮想マシンにのみ使用できます。

**注：** Linux 仮想マシンの場合、ARP Flux (ARP 変動) の問題によって ARP スヌーピングが不正な情報を取得する可能性があります。この問題は ARP フィルタによって回避できます。詳細については、<http://linux-ip.net/html/ether-arp.html#ether-arp-flux> を参照してください。

## IP アドレス検出スイッチング プロファイルの設定

ARP スヌーピング、DHCP スヌーピングまたは VM Tools 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。VM Tools の IP アドレス検出は、ESXi ホストの仮想マシンのみで使用可能です。

### 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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [スイッチング プロファイル (Switching Profiles)] タブをクリックします。
- 4 [追加 (Add)] をクリックして、[IP アドレス検出 (IP Discovering)] を選択します。
- 5 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。
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。



オプション	説明
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。
VMware Tools	[VMware Tools (VM Tools)] ボタンを切り替えて、機能を有効にします。このオプションは、ESXi ホストの仮想マシンでのみ使用可能です。 VMware Tools は、ESXi ホストの仮想マシン上で実行されるソフトウェアで、仮想マシンの MAC アドレスと IP アドレスを提供します。

6 [保存 (Save)] をクリックします。

## 結果

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または論理ポートに接続し、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](#)または[論理ポートとカスタム プロファイルの関連付け](#)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なりすましを防ぐ。
- 仮想マシンの IP アドレスがユーザーの介入なしで変更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 の設定で仮想マシンの IP アドレスを変更する場合、対応する既存のポート/スイッチ アドレス バインドに新しい IP アドレスが適用されるまで、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。各ネットワーク アダプタで SpoofGuard を有効にすると、規定された MAC アドレスおよび対応する IP アドレスのパケットが精査されます。

#### 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 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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [スイッチング プロファイル (Switching Profiles)] タブをクリックします。
- 4 [追加 (Add)] をクリックして、[SpoofGuard (Spoof Guard)] を選択します。  
[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。
- 5 プロファイル名を設定します。プロファイルの説明を追加することもできます。

- 6 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。

- 7 [保存 (Save)] をクリックします。

#### 結果

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

論理スイッチまたは論理ポートに SpoofGuard プロファイルに関連付けます。[カスタム プロファイルと論理スイッチの関連付け](#)または[論理ポートとカスタム プロファイルの関連付け](#)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 リストの宛先 MAC 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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [スイッチング プロファイル (Switching Profiles)] タブをクリックします。
- 4 [追加 (Add)] をクリックして、[スイッチ セキュリティ (Switch Security)] を選択します。

## 5 スイッチ 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、プロファイルの変更内容を入力できます。
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 の宛先の MAC アドレスに対する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 の宛先の MAC アドレス リストから宛先の MAC アドレスをクリックし、宛先を承認してトラフィックの送信を許可します。
DHCP フィルタ	[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。 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。 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。
非 IP トラフィックをブロック	[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。 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。 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。
レート制限	入力方向または出力方向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。 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。 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。

## 6 [保存 (Save)] をクリックします。

### 結果

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または論理ポートに接続し、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](#)または[論理ポートとカスタム プロファイルの関連付け](#)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 アドレス変更機能を使用すると、仮想マシンの MAC アドレスを変更できます。仮想マシンがポートに接続している場合、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、パケットの送信元 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送信元 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。このエージング 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 プロファイルの設定

MAC 管理スイッチ プロファイルを作成して、MAC アドレスを管理できます。

### 前提条件

MAC 管理スイッチング プロファイルの概念について理解します。[MAC 管理スイッチング 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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [スイッチング プロファイル (Switching Profiles)] タブをクリックします。
- 4 [追加 (Add)] をクリックして、[MAC 管理 (MAC Management)] を選択します。
- 5 MAC 管理プロファイルの項目をすべて指定します。

オプション	説明
名前と説明	MAC 管理プロファイルに名前を割り当てます。 オプションで、プロファイルの変更内容を入力できます。
MAC の変更	MAC アドレスの変更機能を有効または無効にします。
ステータス	MAC 学習機能を有効または無効にします。

- 6 [保存 (Save)] をクリックします。

### 結果

MAC 管理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

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に適用します。[カスタム プロファイルと論理スイッチの関連付け](#)または[論理ポートとカスタム プロファイルの関連付け](#)を参照してください。

# カスタム プロファイルと論理スイッチの関連付け

プロファイルがスイッチのすべてのポートに適用されるように、論理スイッチにカスタムのスイッチング プロファイルを関連付けることができます。

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witchング プロファイルが上書きされます。このカスタムのスイッチング 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：** カスタムのスイッチング 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。[3 章 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](#)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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [スイッチ (Switches)] タブをクリックします。
- 4 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をクリックします。
- 5 [管理 (Manage)] タブをクリックします。
- 6 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)]
  - [MAC 管理 (MAC Management)]
- 7 [変更 (Change)] をクリックします。
- 8 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。



- 9 [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のスイッチング プロファイルが関連付けられました。

- 10 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。
- 11 (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。[論理ポートとカスタム プロファイルの関連付け](#)を参照してください。

## 論理ポートとカスタム プロファイルの関連付け

論理ポートは、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。[3 章 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](#)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 パネルで [スイッチング (Switching)] をクリックします。
- 3 [ポート (Ports)] タブをクリックします。
- 4 カスタムのスイッチング プロファイルを適用する論理ポートをクリックします。
- 5 [管理 (Manage)] タブをクリックします。
- 6 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)]
  - [MAC 管理 (MAC Management)]



- 7 [変更 (Change)] をクリックします。
- 8 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。
- 9 [保存 (Save)] をクリックします。

これで、論理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。

- 10 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

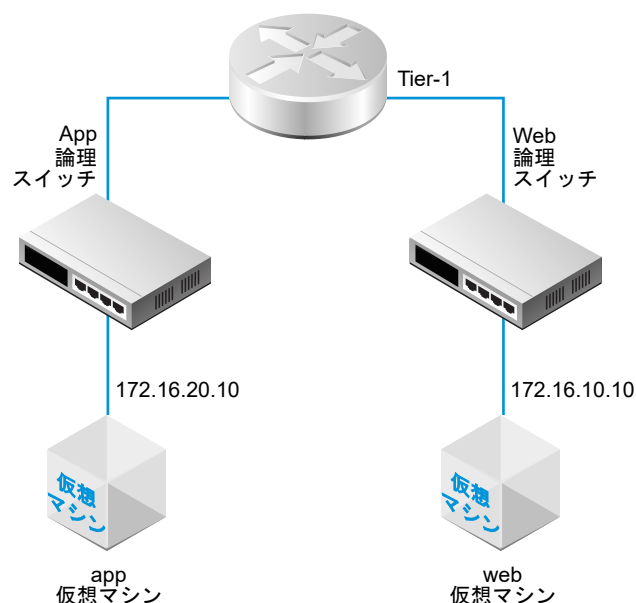
論理スイッチ ポート上でアクティビティを監視して、問題をトラブルシューティングできます。『NSX-T 管理ガイド』で「論理スイッチ ポート アクティビティの監視」を参照してください。

## Tier-1 論理ルーター

NSX-T 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 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 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。

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プランニングが重要です。

図 4-1. Tier-1 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 論理ルーターに接続された 2 台の論理スイッチを示したものです。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 台の仮想マシンを配置するホストやホスト 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。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。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 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 論理ルーターのスタティック ルートの設定

## Tier-1 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 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 論理ルーターのトポロジを理解します。[4 章 Tier-1 論理ルーター](#)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 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 論理ルーターに接続する Tier-0 論理ルーターを選択します。

Tier-0 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) フェイルオーバー モードを選択します。

オプション	説明
ブリエンプティブ	優先ノードで障害が発生し、リカバリした場合、そのピアが先取りされ、アクティブ ノードになります。ピアの状態はスタンバイに変わります。デフォルトのオプションです。
非ブリエンプティブ	優先ノードで障害が発生し、リカバリした場合、ピアがアクティブ ノードかどうか確認します。アクティブな場合、優先ノードがピアを先取りせず、スタンバイ ノードになります。

- 7 (オプション) この Tier-1 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 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。

- 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、新しい論理ルーターがクリック可能なリンクとして表示されます。

## 結果

この論理ルーターが 5,000 台以上の仮想マシンをサポートしている場合には、Edge クラスタの各ノードで次のコマンドを実行して、ARP テーブルのサイズを増やす必要があります。

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

この変更は保持されないため、データプレーンまたはノードの再起動後にコマンドを再度実行する必要があります。

## 次のステップ

Tier-1 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 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

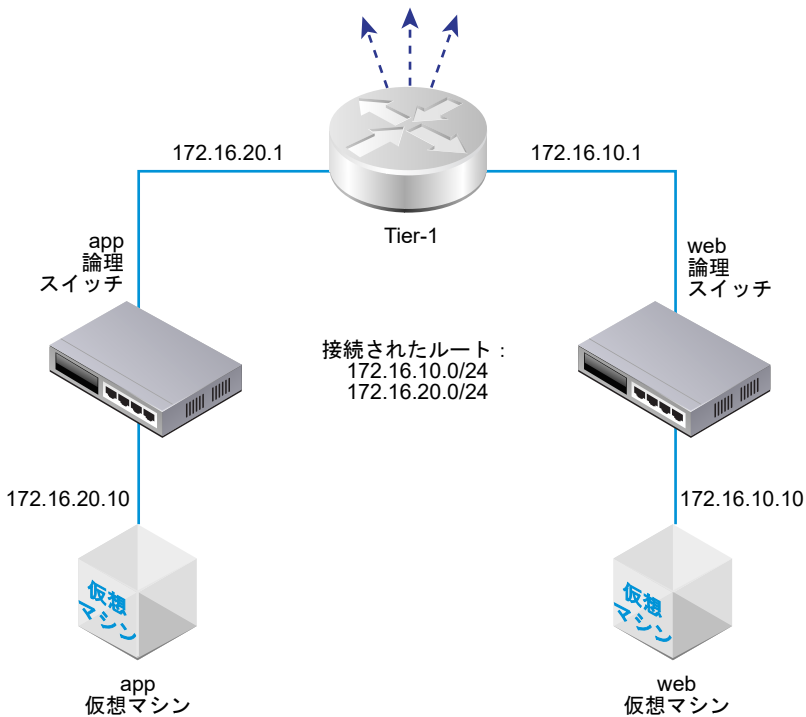
ルートのアドバタイズを有効にして、仮想マシンと外部の物理ネットワーク間、または同じ Tier-0 分散論理ルーターに接続された異なる Tier-1 分散論理ルーター間に North-South 接続を提供します。[Tier-1 分散論理ルーター上でのルートのアドバタイズの設定](#)を参照してください。

## 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。

## 接続されたルートのアドバタイズ



### 前提条件

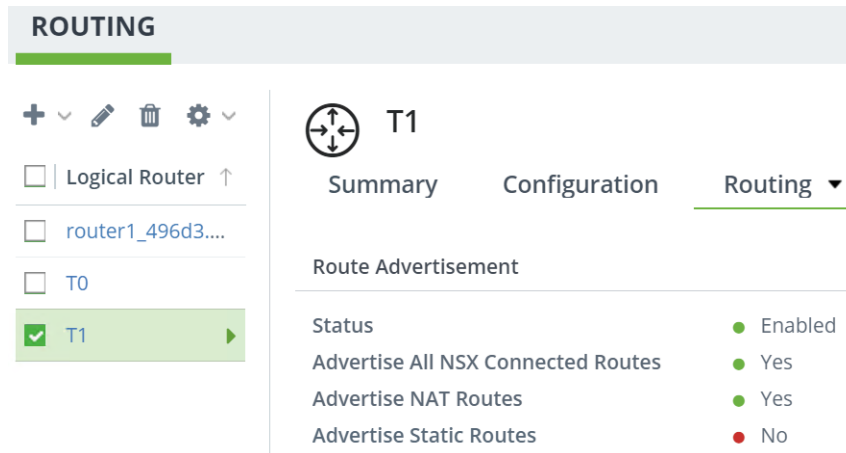
- 仮想マシンが論理スイッチに接続されていることを確認します。 [1 章 論理スイッチと仮想マシン接続の設定](#)を参照してください。
- Tier-1 分散論理ルーターのダウンリンク ポートが設定されていることを確認します。 [Tier-1 分散論理ルーターのダウンリンク ポートの追加](#)を参照してください。

### 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。



- 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。[5 章 Tier-0 論理ルーター](#)を参照してください。

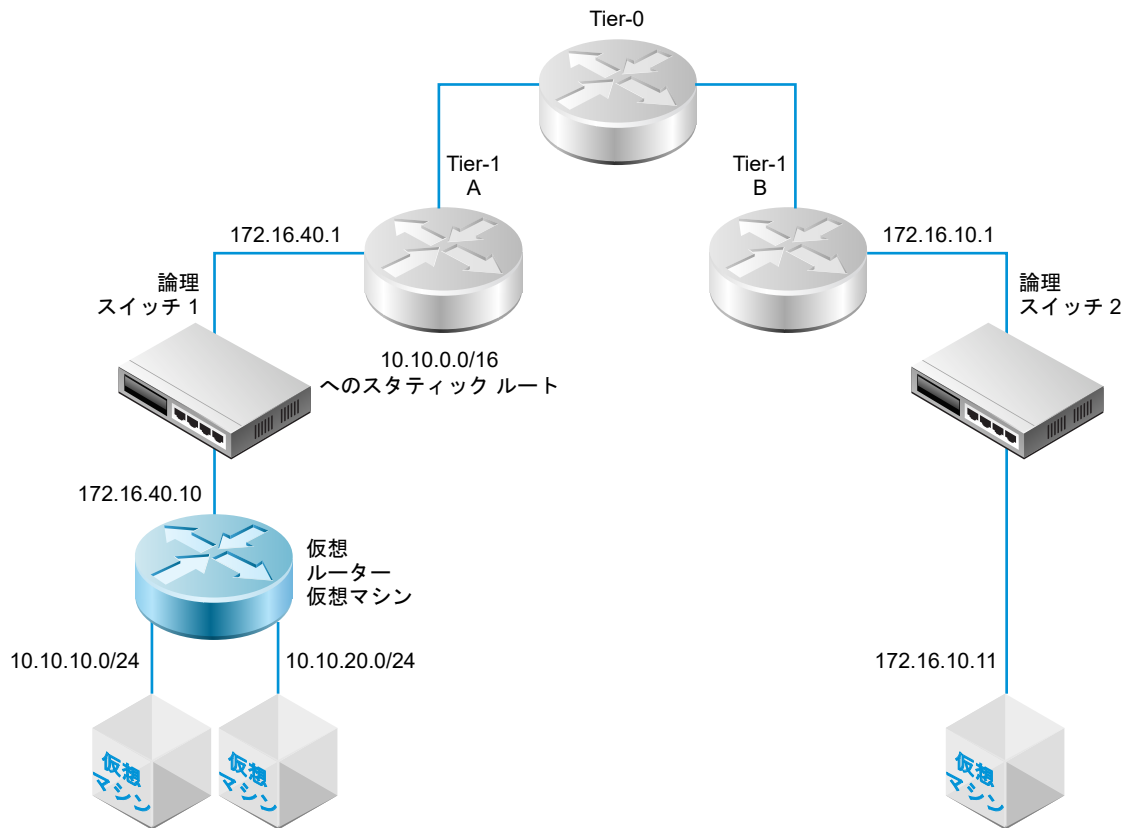
Tier-0 分散論理ルーターがすでに Tier-1 分散論理ルーターに接続されている場合は、Tier-0 ルーターが Tier-1 ルーターに接続されたルートを学習していることを確認することができます。[Tier-0 ルーターが Tier-1 ルーターからルートを学習したことの確認](#)を参照してください。

## Tier-1 論理ルーターのスタティック ルートの設定

Tier-1 論理ルーターのスタティック ルートを設定すると、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 セットとの接続が可能になります。

たとえば、次の図では、Tier-1 A 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 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示しています。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 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 論理ルーターを選択します。
- 4 [ルーティング (Routing)] タブをクリックして、ドロップダウン メニューから [スタティック ルート (Static Routes)] を選択します。
- 5 [追加 (Add)] をクリックします。
- 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 [追加 (Add)] 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 を入力します。鉛筆のアイコンをクリックして、ドロップダウン から [NULL] を選択すると、null ルートを指定できます。別のネクスト ホップ アドレスを追加するには、もう一度 [追加 (Add)] をクリックします。



- 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 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 論理ルーター

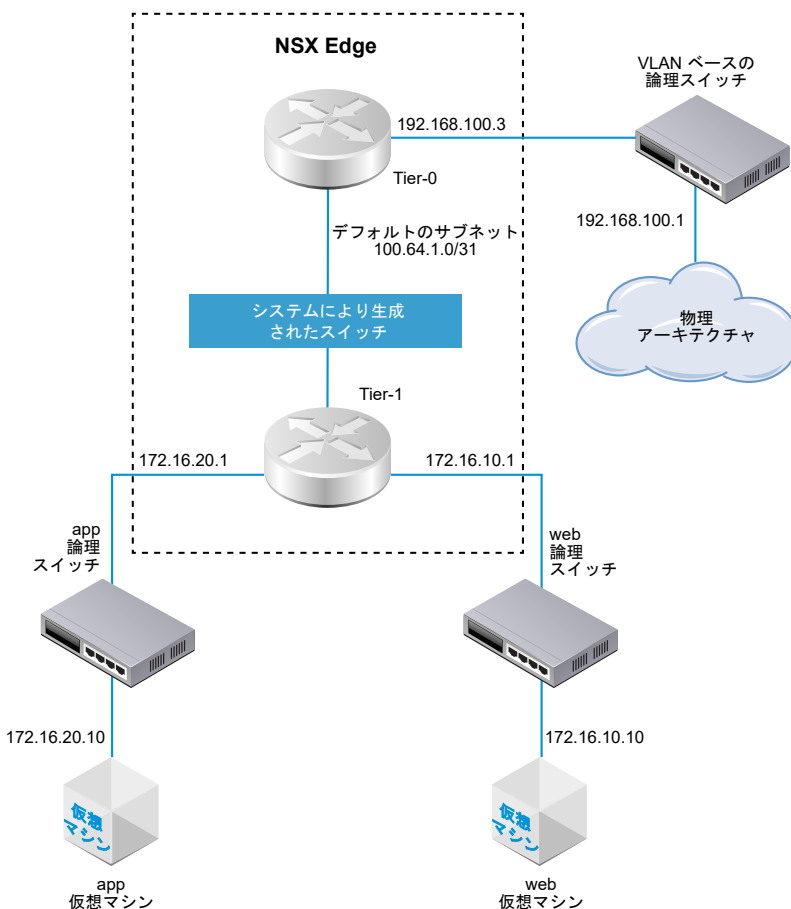
# 5

NSX-T 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 論理ルーターは、論理ネットワークと物理ネットワーク間のゲートウェイ サービスを有効または無効にします。

1 つの NSX Edge クラスターが複数の Tier-0 論理ルーターをバックアップできます。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 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プランニングが重要です。

図 5-1. Tier-0 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、単一の Tier-0 論理ルーターに接続された、単一の Tier-1 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。論理ルーターの設計を十分に活用するには、最低でも 2 台の NSX Edge ノードが必要です。

Tier-1 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、それぞれに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 論理ルーターの接続
- ループバック ルーター ポートの追加
- 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
- 転送タイマーの設定

## 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。「5 章 Tier-0 論理ルーター」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。

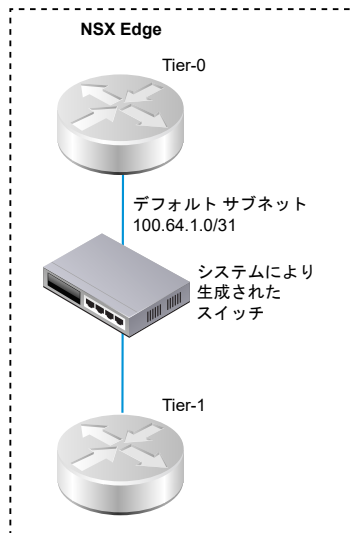
Tier-0 分散論理ルーターを VLAN 論理スイッチに接続するように設定し、外部ネットワークへのアップリンクを作成します。[「VLAN 論理スイッチへの Tier-0 論理ルーターの接続」](#)を参照してください。

## 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 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。
- 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。

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バ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バタイズすると、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

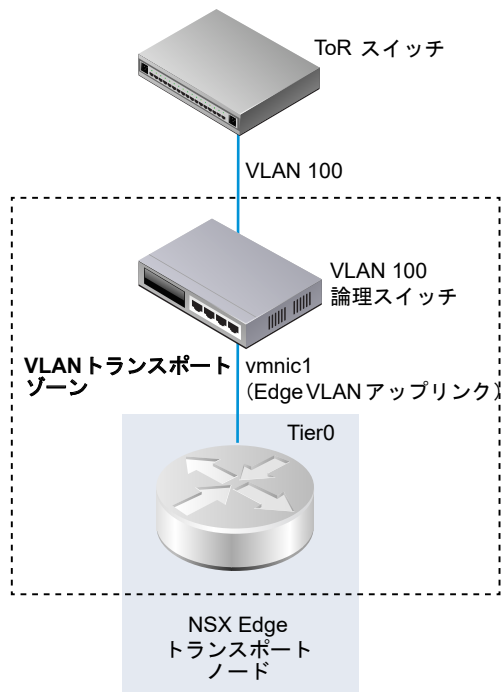
Total number of routes: 7

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 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 論理ルーターを選択します。
- 4 [設定] タブから、新しい論理ルーター 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] 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witch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。

#### 結果

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 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
```

## 結果

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 論理ルーター上の BGP の設定](#)を参照してください。

# ループバック ルーター ポートの追加

ループバック ポートを Tier-0 論理ルーターに追加できます。

ループバック ポートは次の目的で使用できます。

- ルーティング プロトコルのルーター ID
- NAT
- BFD
- ルーティング プロトコルの送信元のアドレス

## 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 論理ルーターを選択します。
- 4 [設定] - [ルーター ポート] の順に選択します。
- 5 [追加] をクリックします。
- 6 名前を入力します。必要に応じて説明も入力します。
- 7 [ループバック] タイプを選択します。
- 8 Edge トランスポート ノードを選択します。
- 9 IP アドレスを CIDR 形式で入力します。

## 結果

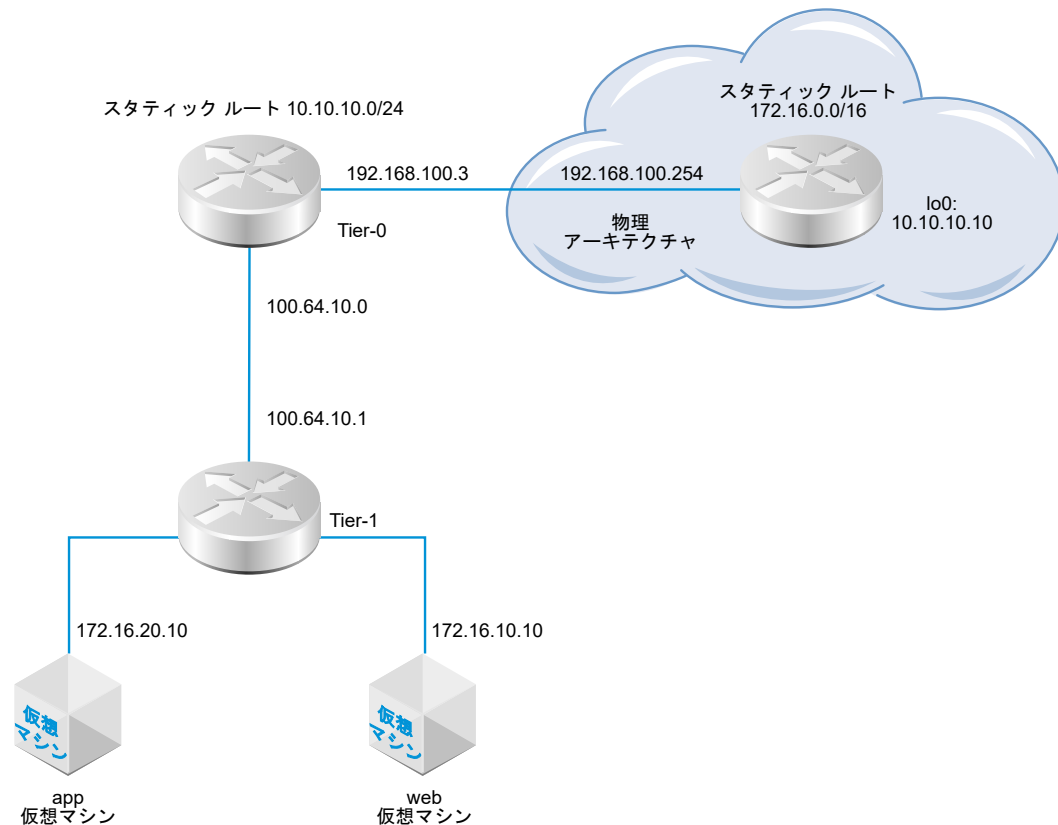
Tier-0 ルーターに新しいアップリンク ポートが追加されます。

## 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 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、10.10.10.0/32 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 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 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 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 [追加 (Add)] 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、192.168.100.254 を入力します。鉛筆のアイコンをクリックして、ドロップダウンから [NULL] を選択すると、null ルートを指定できます。別のネクスト ホップ アドレスを追加するには、もう一度 [追加 (Add)] をクリックします。
- 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。

#### 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。

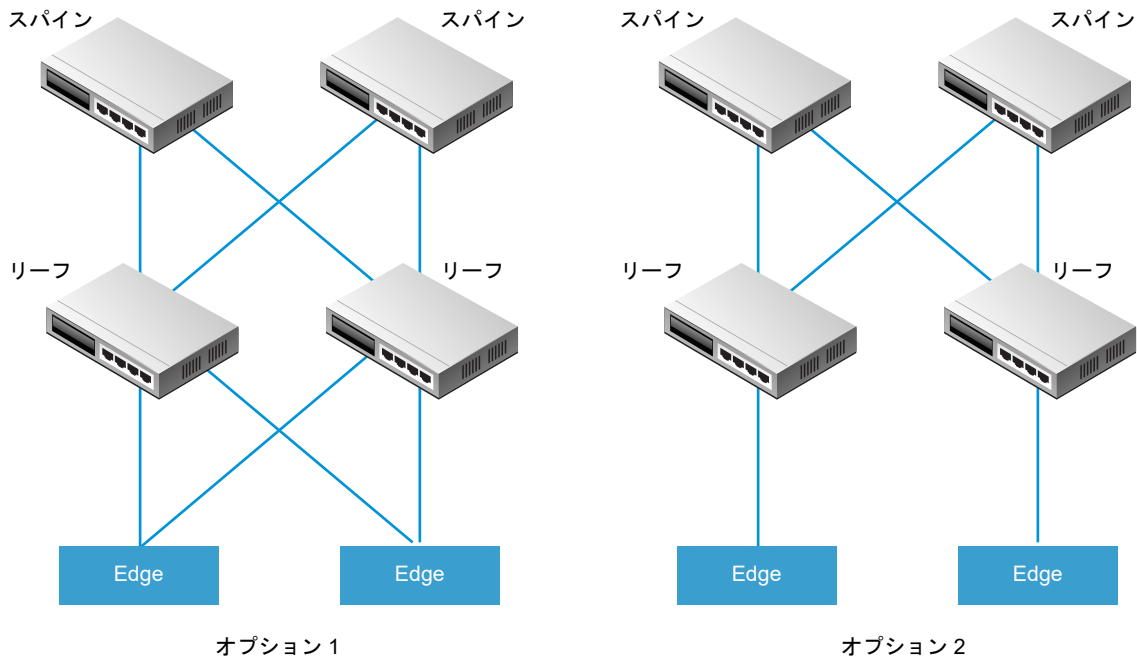
```
ping 10.10.10.10
```

```
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 論理ルーター上の BGP の設定

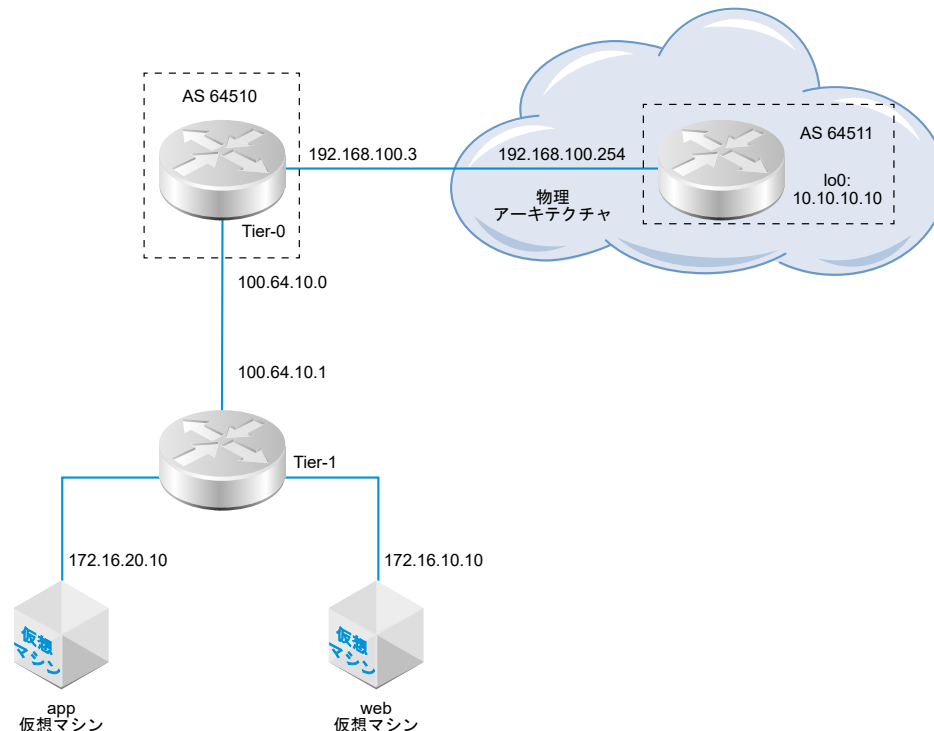
仮想マシンと外部とのアクセスを有効にするには、Tier-0 論理ルーターと物理インフラストラクチャ内のルーター間に外部 BGP (eBGP) 接続を設定します。

BGP を設定する場合は、Tier-0 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があります。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 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。

**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 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 論理ルーターが Tier-1 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 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 [BGP] を選択します。
- 5 [編集] をクリックします。
  - a ローカルの AS 番号を設定します。  
例 : 64510。
  - b [ステータス] 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。
  - c (オプション) [ECMP] 切り替えボタンをクリックして ECMP を有効にします。
  - d (オプション) [グレースフル リスタート] 切り替えボタンをクリックして、グレースフル リスタートを有効にします。
  - e (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。
  - f [保存] をクリックします。
- 6 [追加] をクリックして、BGP ネイバーを追加します。
- 7 ネイバー IP アドレスを入力します。  
例 : 192.168.100.254。
- 8 (オプション) ホップの上限を指定します。  
デフォルトは 1 です。
- 9 リモートの AS 番号を入力します。  
例 : 64511
- 10 (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。
- 11 (オプション) [ローカル アドレス] タブをクリックして、ローカル アドレスを選択します。
  - a (オプション) [すべてのアップリンク] を選択解除して、アップリンク ポートとループバック ポートを表示します。
- 12 (オプション) [アドレス ファミリー] タブをクリックして、アドレス ファミリーを追加します。
- 13 (オプション) [BFD 設定] タブをクリックして、BFD を有効にします。
- 14 [保存] をクリックします。

## 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 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 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 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 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。

```
traceroute 172.16.10.10
```

```
traceroute 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

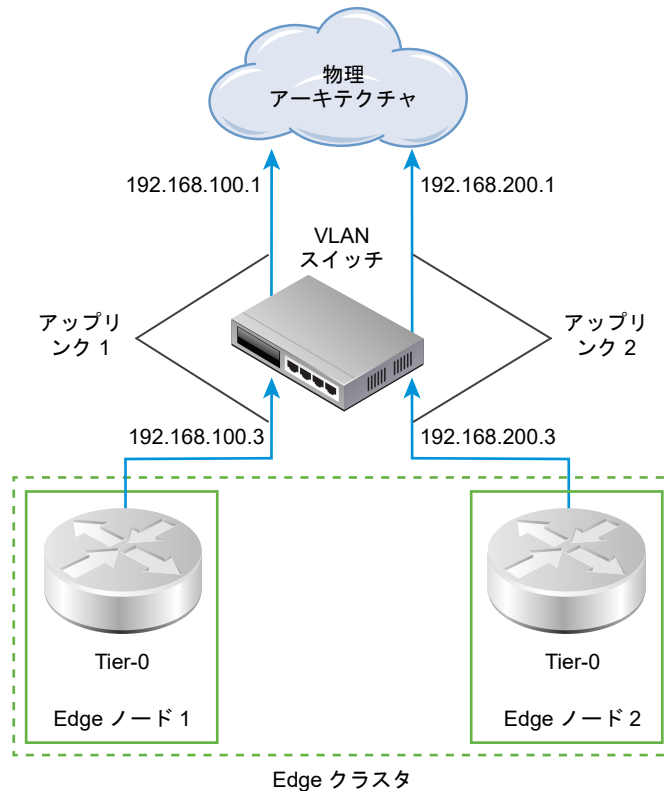
ECMP など、その他のルーティング機能を設定します。

## 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 の論理ルーターを 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 論理ルーターを選択します。
- 4 [設定] 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] 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] 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。

- 7 [保存] をクリックします。

## 結果

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 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 [BGP] を選択します。
- 5 [ネイバー] セクションの [追加] 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 (オプション) ホップの上限を指定します。  
デフォルトは 1 です。
- 8 リモート AS の番号を入力します。  
例: 64511
- 9 (オプション) [ローカル アドレス] タブをクリックして、ローカル アドレスを選択します。
  - a (オプション) [すべてのアップリンク] を選択解除して、アップリンク ポートとループバック ポートを表示します。
- 10 (オプション) [アドレス ファミリ] タブをクリックして、アドレス ファミリを追加します。
- 11 (オプション) [BFD 設定] タブをクリックして、BFD を有効にします。
- 12 [保存] 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。
- 13 [BGP 設定] セクションの横にある [編集] をクリックします。
- 14 [ECMP] 切り替えボタンをクリックして ECMP を有効にします。  
[状態] ボタンには [有効] と表示される必要があります。
- 15 [保存] をクリックします。

### 結果

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
```

- 3 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
```

- 4 Tier-0 分散ルーターの VRF を入力します。

```
vrf 5
```

- 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。

- 6 **exit** と入力して vrf コンテキストを終了します。

- 7 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。

- 8 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。

- 9 2 つの Edge ノードで SSH セッションを開始します。

- 10 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>
```

- 11 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。

- 12 キャプチャ セッションを終了します。

```
del capture session 0
```

- 13 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、ノースバウンド 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 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。

### 結果

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 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。

## 転送タイマーの設定

Tier-0 論理ルーターに転送タイマーを設定できます。

転送タイマーは、最初の BGP セッションが確立してからルーターが通知を送信するまでの時間を秒単位で定義します。このタイマー（以前の転送遅延）により、動的ルーティング (BGP) を使用する NSX Edge でアクティブ/アクティブ構成またはアクティブ/スタンバイ構成の論理ルーターがフェイルオーバーした場合に、ダウンタイムを最小限に抑えることができます。ここには、最初の BGP/BFD セッション後に外部ルーター (TOR) がすべてのルートを通知するまでの秒数を設定する必要があります。タイマー値は、ルーターが学習するノースバウンドの動的ルートの数に比例します。Edge ノードが 1 台の場合には、このタイマーは 0 に設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 [ルーティング (Routing)] を選択します。
- 3 Tier-0 論理ルーターを選択します。
- 4 [ルーティング] - [グローバル設定] の順に選択します。
- 5 [編集] をクリックします。

- 6 転送タイマーの値を入力します。
- 7 [保存] をクリックします。

# ネットワーク アドレス変換

## 6

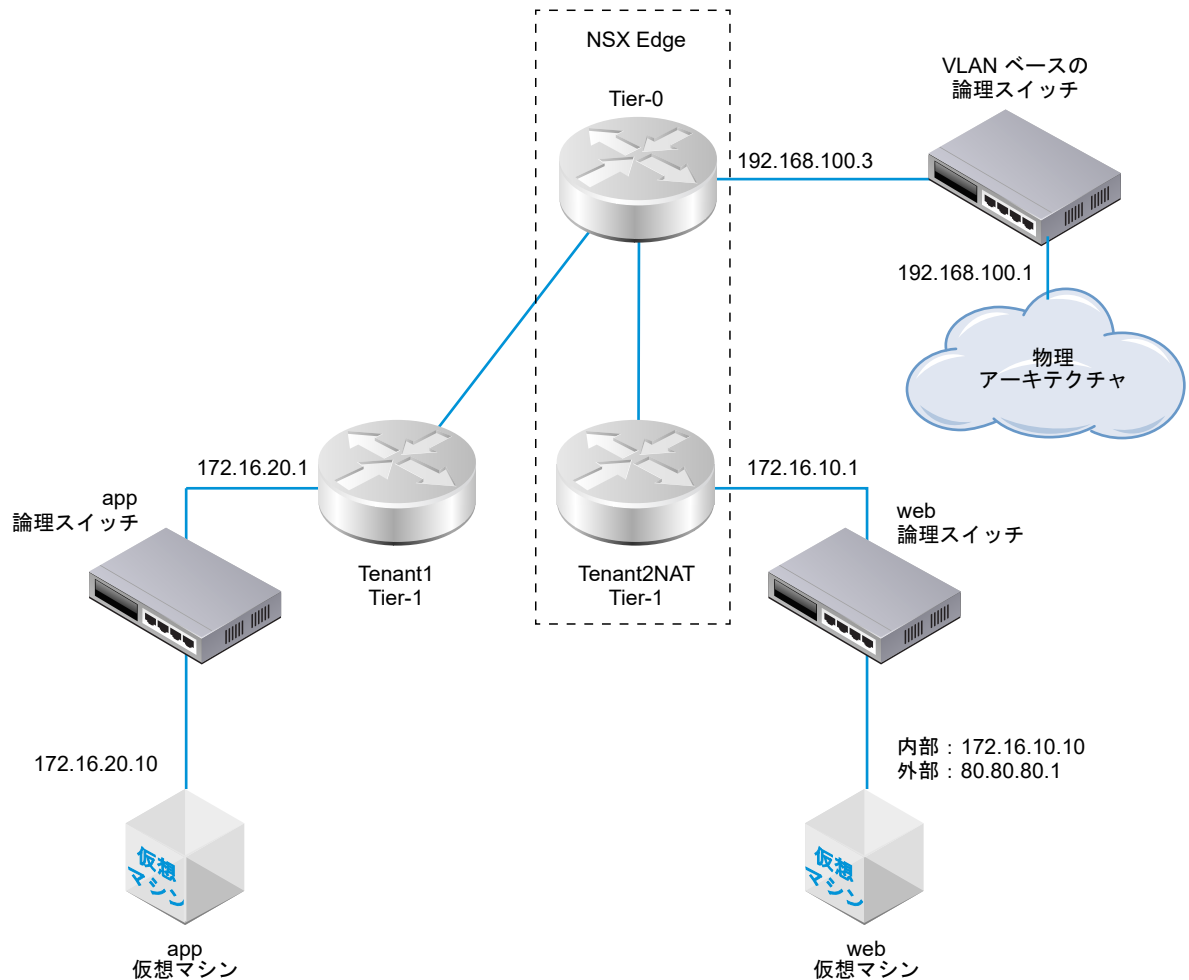
NSX-T のネットワークアドレス変換 (NAT) は、Tier-0 および Tier-1 分散論理ルーター上で設定することができます。

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 ルーター上の送信元 NAT の設定

送信元 NAT (SNAT) は、パケットの IP アドレス ヘッダー内の送信元アドレスを変更します。また、TCP/UDP ヘッダー内の送信元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宛先は送信元に戻ることができます。



## 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 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 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 論理ルーターをクリックします。
- 4 [サービス (Services)] - [NAT] の順に選択します。
- 5 [ADD] をクリックします。
- 6 優先順位を指定します。  
小さい値であるほど、このルールの優先順位は高くなります。
- 7 [アクション] には、[SNAT] を選択します。
- 8 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。
- 9 [送信元 IP アドレス] 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。  
送信元 IP アドレスを空白のままにすると、ルーターのダウンリンク ポート上の送信元がすべて変換されます。  
この例では、送信元 IP アドレスは 172.16.10.10 です。
- 10 [変換された 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。  
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。
- 11 [宛先 IP アドレス] 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。  
宛先 IP アドレス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宛先に適用されます。
- 12 ルールを有効にします。

### 13 (オプション) ログを有効にします。

#### 結果

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										
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。

## Tier-1 ルーター上での宛先 NAT の設定

宛先 NAT は、パケットの IP アドレス ヘッダー内の宛先アドレスを変更します。また、TCP/UDP ヘッダー内の宛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、受信パケットの宛先のパブリック 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、パケットの宛先ポートを 172.16.10.10 から 80.80.80.1 に変更します。パブリック宛先アドレスを使用することで、プライベート ネットワーク内の宛先にプライベート 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 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 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 論理ルーターをクリックします。

4 [サービス (Services)] - [NAT] の順に選択します。

5 [ADD] をクリックします。

6 優先順位を指定します。

小さい値であるほど、このルールの優先順位は高くなります。

7 アクションとして DNAT を選択します。

8 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。

9 宛先 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。

この例の宛先 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。

10 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。

11 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送信元に適用されます。

12 ルールを有効にします。

13 (オプション) ログを有効にします。

## 結果

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。

### 結果



## 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 ルートのアダプタイズのルールを編集して、Tier-1 NAT ルートのアダプタイズを有効にします。

結果

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。

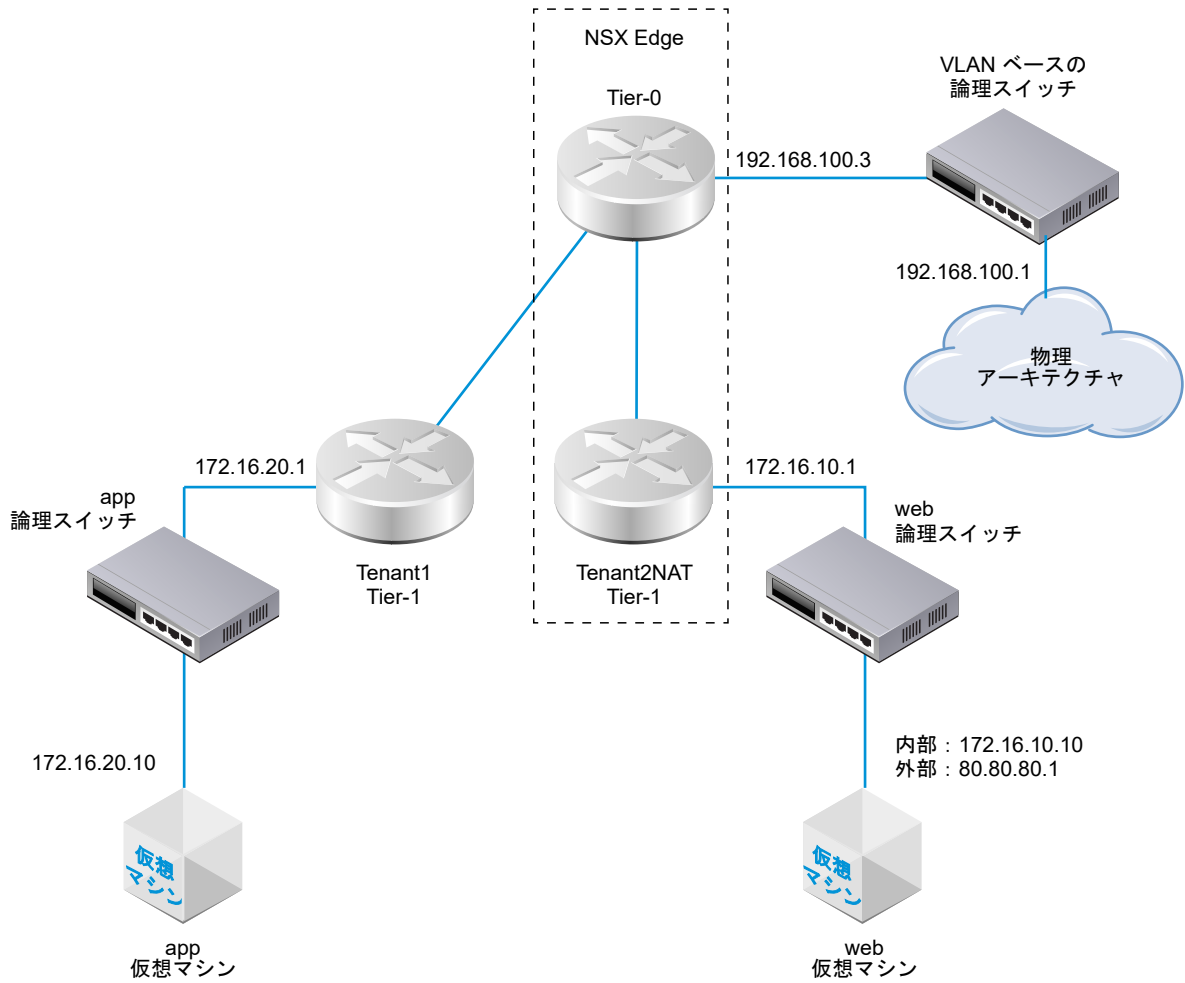
## Tier-0 NAT

Tier-0 分散論理ルーターは再帰 NAT をサポートします。

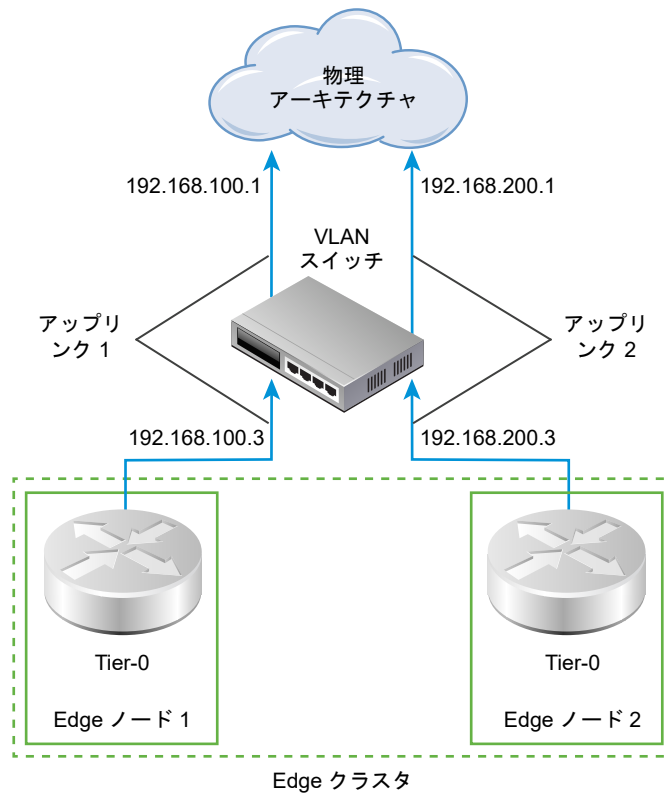
### 再帰 NAT

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 論理ルーター上の再帰 NAT の設定

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。

### 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 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 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 再帰 NAT を設定する Tier-0 論理ルーターをクリックします。
- 4 [サービス (Services)] - [NAT] の順に選択します。
- 5 [ADD] をクリックします。
- 6 優先順位を指定します。  
小さい値であるほど、このルールの優先順位は高くなります。
- 7 [アクション] には、[再帰] を選択します。
- 8 [送信元 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、送信元 IP アドレスは 80.80.80.1 です。
- 9 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。
- 10 [宛先 IP アドレス] 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。  
宛先 IP アドレス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宛先に適用されます。
- 11 ルールを有効にします。
- 12 (オプション) ログを有効にします。

## 結果

新しいルールが NAT の下に表示されます。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

o

アクティブセッション

o

パケットの数

o

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										
<div><div></div>1030</div>	再帰	任意	80.80.80.1	任意	任意	任意	172.16.10.10	任意	<div></div>	

## 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。

# 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 ログの有効化または無効化](#)
- [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](#)
- [デフォルトの分散ファイアウォール 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](#)

- [ファイアウォール除外リストの設定](#)
- [ファイアウォールの有効化と無効化](#)
- [論理ルーターへのファイアウォール ルールの追加または削除](#)

## 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。
- 2 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 既存のセクションまたはルールをクリックします。
- 4 メニュー バーで [セクションの追加 (Add Section)] をクリックするか、セクションの最初の列のメニュー アイコンをクリックして、[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)] 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。

---

- 5 セクション名およびオプションの説明を入力します。
- 6 [ステートフル (Stateful)] または [ステートレス (Stateless)] 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。

- 7 セクションを適用する 1 つまたは複数のオブジェクトを選択します。

オブジェクトのタイプは、論理ポート、論理スイッチ、NSGroup です。NSGroup を選択する場合、1 台以上の論理スイッチまたは論理ポートが含まれている必要があります。NSGroup に IP セットまたは MAC セットのみが含まれている場合は、無視されます。

---

**注：** セクション内の [適用先 (Applied To)] は、そのセクションのルールのすべての [適用先 (Applied To)] 設定を上書きします。

---

- 8 [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 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 セクションの最初の列のメニュー アイコンをクリックして、[削除 (Delete)] を選択します。
- 4 [削除 (Delete)] をクリックしてセクションを削除します。  
セクションとその中の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 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 セクションの最初の列のメニュー アイコンをクリックして、[すべてのルールを有効にする (Enable all rules)] または [すべてのルールを無効にする (Disable all rules)] を選択します。
- 4 [保存 (Save)] をクリックします。

## セクション ログの有効化または無効化

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 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 セクションの最初の列のメニュー アイコンをクリックして、[すべてのログを有効にする (Enable all logs)] または [すべてのログを無効にする (Disable all logs)] を選択します。
- 4 [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。ファイアウォールの適用から除外する論理スイッチ、論理ポート、またはグループが含まれる、除外リストを設定できます。

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。

**注：** TCP プロトコルの場合、ステートフル ルールに対する TCP Strict チェックが自動的に有効になります。これは、ネットワーク接続が SYN パケットで開始した場合のみ、パケットが TCP ルールに一致することを意味します。

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

列の名前	定義
名前	ファイアウォール ルールの名前。
ID	各ルールに対してシステムが生成した一意の ID。

表 7-1. ファイアウォール ルール画面の列 (続き)

列の名前	定義
方向	オプションは、 <b>受信</b> 、 <b>送信</b> 、および <b>受信/送信</b> です。デフォルトは <b>受信/送信</b> です。このフィールドは、宛先オブジェクトから見たトラフィックの方向を示します。 <b>受信</b> はオブジェクトへのトラフィックのみ、 <b>送信</b> はオブジェクトからのトラフィックのみ、 <b>受信/送信</b> は両方のトラフィックがチェックされることを意味します。
IP プロトコル	オプションは、 <b>IPv4</b> 、 <b>IPv6</b> 、および <b>IPv4_IPv6</b> です。デフォルトは <b>IPv4_IPv6</b> です。
送信先	ルールの送信元は、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、すべての送信先と一致します。送信元または宛先の範囲には IPv6 はサポートされません。
宛先	ルールの影響を受ける接続の宛先の 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、すべての宛先と一致します。送信元または宛先の範囲には 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。
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、 <b>許可</b> 、 <b>ドロップ</b> 、または <b>却下</b> があります。デフォルトは <b>許可</b> です。
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	ログへの記録を有効または無効にすることができます。ログは ESX および KVM ホストの /var/log/dfwptlogs.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取り専用フィールド。

**注：** SpoofGuard が有効になっていない場合は、悪意のある仮想マシンが別の仮想マシンのアドレスを要求する可能性があるため、自動検出されたアドレスのバインドの信頼性は保証されません。SpoofGuard が有効な場合、検出されたバインドがすべて検証され、承認されたバインドのみが表示されます。

## 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。各ルールの送信元と宛先に複数のオブジェクトを追加することで、追加す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、ルールは任意の送信元、宛先およびサービス 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。

- 2 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 既存のセクションまたはルールをクリックします。
- 4 メニュー バーで [ルールの追加 (Add Rule)] をクリックして、[ルールを上追加 (Add Rule Above)] または [ルールを下追加 (Add Rule Below)] を選択するか、ルールの最初の列のメニュー アイコンをクリックして [ルールを上追加 (Add Rule Above)] または [ルールを下追加 (Add 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。

**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。

- 5 [名前 (Name)] 列で、鉛筆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。

- 6 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。定義しない場合は、すべての送信元と一致します。[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	矢印をクリックして、オブジェクトを選択します。
ト	<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>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>2 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>3 オブジェクトが [選択済み] 列に移動します。</li> <li>4 [OK] をクリックします。</li> </ol>

- 7 新しいルールの [ターゲット (Destinations)] セルをポイントします。定義しない場合は、すべての宛先と一致します。[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	矢印をクリックして、オブジェクトを選択します。
ト	<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>

- 8 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。

- 9 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。
- 10 新しいサービスを定義するには、[新しい NSService の作成 (Create New NSService)] 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 アドレス</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。
送信元ポート	送信元ポートを入力します。
宛先ポート	宛先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。



- 11 [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、送信元のシステムまたは宛先の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、送信者に対して宛先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。

- 12 [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。

- 13 1 つ以上のオブジェクトを選択します。

オブジェクトのタイプは、論理ポート、論理スイッチ、NSGroup です。NSGroup を選択する場合、1 台以上の論理スイッチまたは論理ポートが含まれている必要があります。NSGroup に IP セットまたは MAC セットのみが含まれている場合は、無視されます。

- 14 [OK] をクリックします。

- 15 [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。ログの記録はデフォルトで無効になっています。[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。ログの記録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。

- 16 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

- 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 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 ルールを選択して、メニュー バーの [ルールの削除 (Delete Rule)] をクリックするか、最初の列のメニュー アイコンをクリックして、[削除 (Delete)] を選択します。
- 4 [保存 (Save)] をクリックして、削除を有効にします。

## 結果

ルールが削除されます。

## デフォルトの分散ファイアウォール 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 ルールは、どのユーザー定義のファイアウォール ルールにも一致しないトラフィックに適用されます。デフォルトのレイヤー 3 ルールは [全般 (General)] 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 (Ethernet)] タブに表示されます。

デフォルトのファイアウォール 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内の全ての準備済み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、削除することはできません。ただし、ルールの [アクション (Action)] 要素を [許可 (Allow)] から [ドロップ (Drop)] または [却下 (Reject)] (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に記録するかどうかを指定することはできます。

デフォルトのレイヤー 3 ファイアウォール ルールは、DHCP を含め、すべてのトラフィックに適用されます。[アクション (Action)] を [ドロップ (Drop)] または [却下 (Reject)] に変更すると、DHCP トラフィックがブロックされます。その場合は、DHCP トラフィックを許可するルールを作成する必要があります。

## 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 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 ルールの [名前 (Name)] 列で鉛筆のアイコンをクリックして、変更を行います。
- 4 ルールの [アクション (Action)] 列で、鉛筆のアイコンをクリックします。
- 5 ダイアログ ボックスで、次のいずれかのオプションを選択します。
  - 許可: 指定された送信元、宛先、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: 指定された送信元、宛先、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、送信元のシステムまたは宛先の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：指定された送信元、宛先、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、送信者に対して宛先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] を使用するメリットの 1 つは、一度接続を試行するのみで、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。

---

- 6 [ログ (Log)] 列で、鉛筆のアイコンをクリックします。
- 7 ログの記録を有効にするには、[ログ (Log)] 切り替えボタンを [はい (Yes)] に設定します。ログの記録を無効にするには、[いいえ (No)] に設定します。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。ログの記録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。
- 8 [保存 (Save)] をクリックします。

## 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。
- 2 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。
- 3 ルールを選択します。メニュー バーで [上へ移動 (Move Up)] または [下へ移動 (Move Down)] をクリックするか、最初の列のメニュー アイコンをクリックして、[上へ移動 (Move Down)] または [下へ移動 (Move Up)] を選択します。
- 4 [保存 (Save)] をクリックします。

## ファイアウォール ルールのフィルタ

[ファイアウォール] セクションに移動すると、最初はすべてのルールが表示されています。フィルタを使用すると、ルールのサブセットのみを表示するように表示内容を制御できます。これにより、ルールを簡単に管理できます。

### 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 L3 ルールの場合には [全般 (General)] タブを、L2 ルールの場合には、[イーサネット (Ethernet)] タブをクリックします。

- 3 メニュー バーの右側にある検索テキスト フィールドで、虫眼鏡アイコンをクリックしてオブジェクトを選択するか、オブジェクト名の最初の数文字を入力して、選択するオブジェクトのリストを絞り込みます。

オブジェクトを選択すると、フィルタが適用され、ルールが更新されます。以下の列にオブジェクトを含むルールのみが表示されます。

- 送信元
- 宛先
- 適用先
- サービス

- 4 フィルタを削除するには、テキスト フィールドからオブジェクト名を削除します。

## ファイアウォール除外リストの設定

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。
- 2 [除外リスト (Exclusion List)] タブをクリックします。  
除外リスト画面が表示されます。
- 3 オブジェクトを追加するには、メニュー バーの [追加 (Add)] をクリックします。  
ダイアログ ボックスが表示されます。
- 4 タイプとオブジェクトを選択します。  
使用可能なタイプは、[論理ポート (Logical Ports)]、[論理スイッチ (Logical Switch)]、[NSGroup] です。
- 5 [保存 (Save)] をクリックします。
- 6 除外リストからオブジェクトを削除するには、オブジェクトを選択してメニュー バーの [削除 (Delete)] をクリックします。
- 7 削除を確認します。

## ファイアウォールの有効化と無効化

分散ファイアウォール機能を有効または無効にできます。無効にすると、ルールは適用されません。

### 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。

- 2 [設定 (Settings)] タブをクリックします。
- 3 [編集 (Edit)] をクリックします。
- 4 ダイアログ ボックスで、ファイアウォールのステータスを有効または無効に設定します。
- 5 [保存 (Save)] をクリックします。

## 論理ルーターへのファイアウォール ルールの追加または削除

Tier-0 または Tier-1 論理ルーターにファイアウォール ルールを追加すると、ルーターへの通信を制御できます。

### 前提条件

ファイアウォール ルールのパラメータを確認します。[ファイアウォール ルールの追加](#)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 まだ選択していない場合は、[ルーター (Routers)] タブをクリックします。
- 4 論理ルータの名前をクリックします。
- 5 [サービス (Services)] - [Edge ファイアウォール (Edge Firewall)] の順に選択します。
- 6 既存のセクションまたはルールをクリックします。
- 7 ルールを追加するには、メニュー バーで [ルールの追加 (Add Rule)] をクリックして、[ルールを上追加 (Add Rule Above)] または [ルールを下追加 (Add Rule Below)] を選択するか、ルールの最初の列のメニュー アイコンをクリックして [ルールを上追加 (Add Rule Above)] または [ルールを下追加 (Add Rule Below)] を選択します。さらにルール パラメータを指定します。

このルールは論理ルーターにのみ適用されるため、[適用先] フィールドは表示されません。

- 8 ルールを削除するには、ルールを選択して、メニュー バーの [ルールの削除 (Delete Rule)] をクリックするか、最初の列のメニュー アイコンをクリックして、[削除 (Delete)] を選択します。

### 結果

---

**注：** Tier-0 論理ルーターにファイアウォール ルールを追加した場合、ルーターをバックアップしている NSX Edge クラスタがアクティブ/アクティブ モードで実行されていると、ファイアウォールはステートレス モードでのみ実行できます。HTTP、SSL、TCP などのステートフル サービスのファイアウォール ルールを設定すると、ファイアウォール ルールは意図したとおりに機能しません。この問題を回避するには、NSX Edge クラスタがアクティブ/スタンバイ モードで実行されるように設定します。

---

# 分散ネットワーク暗号化

## 8

分散ネットワーク暗号化 (DNE) は、同じ NSX Manager で管理されているデータセンター内の 2 つのエンドポイント（仮想マシン、VIF、セキュリティ グループなど）間で発生するデータセンター内のトラフィックを認証し、暗号化します。DNE は、NSX-T のオプション機能です。

この章には、次のトピックが含まれています。

- 分散ネットワーク暗号化について
- DNE がネットワーク パケットを処理する方法
- DNE 設定の管理
- 暗号化ルール セクションの追加、編集および削除
- セクション内のすべての暗号化ルールの有効化と無効化
- セクション内のすべての暗号化ログの有効化と無効化
- 暗号化ルールについて
- 暗号化ルールの追加、クローン作成および削除
- 暗号化ルールの編集
- 暗号化ルールの有効化と無効化
- 暗号化ルールのログの記録の有効化と無効化
- 暗号化ルールの順序の変更
- 暗号化ルールのフィルタリング
- キー ポリシーについて
- キー ポリシーの追加、編集および削除
- キー ポリシーのローテーション
- キー ポリシーの失効

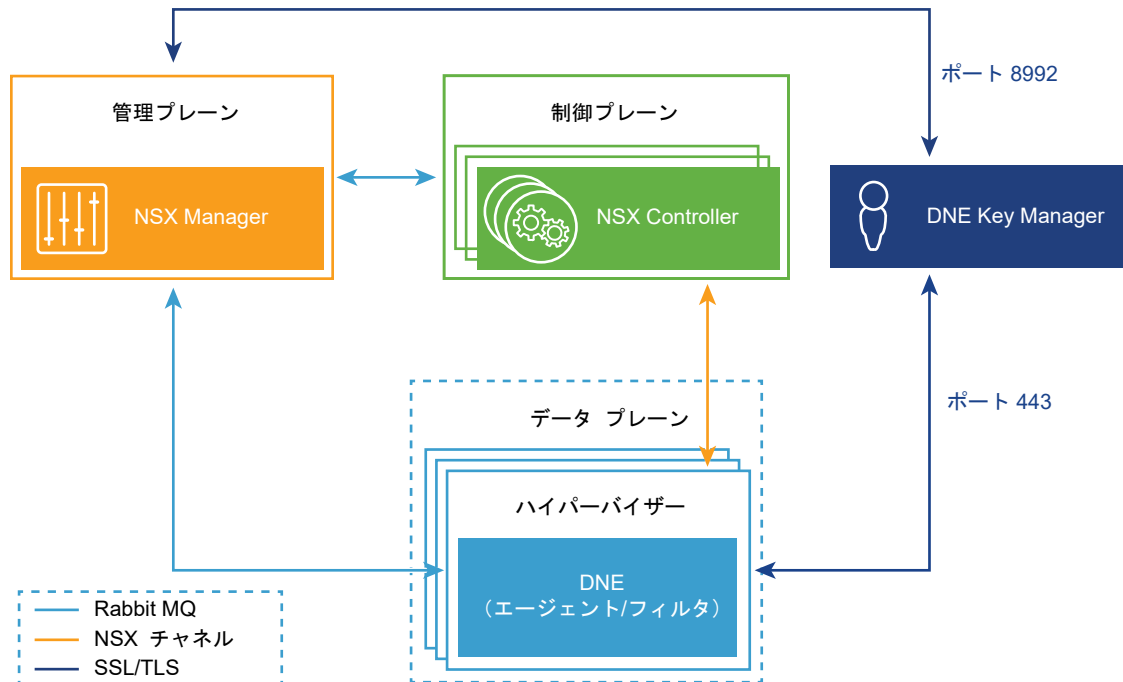
## 分散ネットワーク暗号化について

分散ネットワーク暗号化 (DNE) は、仮想マシンの一般的な機能で、グループ キーの概念に基づいてハイパーバイザーでネットワークトラフィックを暗号化します。管理者が共通の機能または要件を定義した仮想マシンは 1 つのキーを共有します。NSX Manager は、きめ細かいルールベースのグループ キー管理が可能な使用モデルを提供します。

暗号化ルールには、パケットのプロパティに基づいて個々のネットワークパケットを処理する方法が定義されています。パケットに実行される処理は、認証と暗号化または復号、または認証のみです。DNE は、VMware の DNE Key Manager アプライアンスを使用して、DNE のキー管理を行います。

次の図は、DNE と DNE Key Manager を NSX Transformers アーキテクチャ全体に適合させる方法を示しています。

図 8-1. 分散ネットワーク暗号化アーキテクチャ



次の表では、他のコンポーネントと DNE の通信について説明します。

表 8-1. 分散ネットワーク暗号化アーキテクチャのコンポーネント

プレーン	コンポーネント	説明
管理	NSX Manager	DNE サービスの設定と管理を処理する DNE Manager コンポーネント。ルールおよびポリシー管理、発行、ログの記録などを行います。管理者は、NSX Manager のグラフィカルユーザーインターフェースまたは REST API を使用して、暗号化ルール、暗号化ルールセクションおよびポリシーを定義します。
コントロール	NSX Controller	ルールの変換、発行、シャーディング、キー配布のアクセス制御を処理する DNE コントローラ コンポーネント。

表 8-1. 分散ネットワーク暗号化アーキテクチャのコンポーネント（続き）

プレーン	コンポーネント	説明
データ	DNE エージェント	ユーザー環境の DNE フィルタのエージェント。DNE フィルタと次のコンポーネント間で通信チャネルとして機能します。 <ul style="list-style-type: none"> <li>■ NSX Manager（統計）</li> <li>■ NSX Controller（構成）</li> <li>■ DNE Key Manager（キー配布）</li> </ul>
	DNE Key Manager	2 つのエンドポイント間の暗号化され、認証された接続で使用されるキーを管理します。DNE Key Manager は、ハイパーバイザーからの要求に従ってキーの生成、格納、返却を行います。NSX Controller は、どのハイパーバイザーがどのキーを取得するのかを制御します。
	DNE フィルタ	ネットワーク パケットを暗号化し、認証します。

## 主な概念

次の表では、DNE の主な概念について説明します。

表 8-2. 分散ネットワーク暗号化の主な概念

用語	定義
暗号化	送信元と目的の受信者のみが内容を読み取ることができるように、データの機密性を維持したまま、メッセージをネイティブ形式からコード化された形式に変換すること。
復号	メッセージを暗号化された形式（コード化された形式）からネイティブ形式に変換すること。
認証	ネットワーク パケットが改ざんされているかどうかを確認するため、パケットの整合性を検証するプロセス。
暗号化ルール	保護するデータ フロー（送信元と宛先）、条件に一致した場合に実行するアクション（暗号化と認証、認証のみ、プレーンテキストで許可）、ポリシー適用ポイントを定義したルール。
暗号化ルール セクション	グループとして管理される暗号化ルールのセット。
キー	認証と暗号化で使用する暗号化トークン。キーがペアになり、対称型になります（パブリック キーとプライベート キーのペアではありません）。各キーには、キー ID という一意の識別子が付きます。強度は 128 ビットです。
キー ポリシー	ルールでキーが必要な場合、ネットワーク パケットに使用するキー インスタンスを決定するためにキー ポリシー (KP) が使用されます。KP には、一連のキーのパラメータとメタデータ、DNE Key Manager インスタンスの仕様が定義されています。
キーのローテーション	DNE Key Manager から新しいキーを取得し、既存のキーの置き換えたり、新しいキーを追加するプロセス。キーのローテーションは、頻度または有効期限の設定に基づいて自動的に行われます。また、必要なときに手動で行うこともできます。キーのローテーションは、キーの失効よりも安全に行われます。
キーの失効	暗号化/復号に使用されているキーを無効にするプロセス。キーの失効は通常、データ漏えいなど、何らかの理由で 1 つ以上のキーが信頼できなくなったときに行います。キーの失効では、キーの使用を停止し、DNE Key Manager に新しいキーを要求します。ホストが新しいキーを待っている間、一部のパケットがドロップされる可能性があるため、失効はトラフィックに影響を及ぼします。

**注：** キーが失効し、DNE Key Manager または集中制御プレーンにアクセスできないなどの理由で新しいキーを使用できない場合は、古いキーが引き続き使用されます。このイベントについてのログ メッセージは、システム ログに記録されます。



## DNE がネットワーク パケットを処理する方法

DNE を設定する前に、NSX-T 環境の 2 つのエンドポイント間で転送されるネットワーク パケットを DNE でどのように処理されるのか理解しておく必要があります。

### ルールに一致するパケット

各パケットは、設定された暗号化ルールに従って暗号化されます。暗号化ルールは、最初のセクションにある最初のルールから順番に適用されます。最初のルールの条件にパケットが一致しない場合、次のルールが適用されます。

- 暗号化ルールがパケットと一致すると、この暗号ルールに設定されているアクションがパケットに実行されます。それ以降の暗号化ルールは適用されません。
- すべてのルールが適用され、一致するものが確認されなかった場合、このパケットに対しては何も実行されません。そのまま通過を許可できます。

ルールの順序は重要です。パケットが複数の暗号化ルールに一致すると、最初に一致した暗号化ルールのアクションがパケットに実行されます。他の暗号化ルールはすべて無視されます。このため、セクションとルールの順序は慎重に検討してください。

### パケットの整合性チェック

パケットが暗号化ルールに一致したときに、ルール アクションが整合性チェックのみの場合、DNE はパケットの整合性を確認し、パケットが改ざんされているかどうかを判断します。パケットの整合性が確認された場合にのみ、パケットの通過が許可されます。それ以外の場合には、パケットがドロップされます。

### パケットの認証と暗号化

パケットがルールに一致した場合、ルール アクションは暗号化との整合性チェックになります。

- 転送側では、DNE が暗号化ルールのキー ポリシーのキーを使用し、パケットを暗号化します。
- 受信側では、DNE がパケットを復号化し、整合性チェックを実行します。暗号化と復号に成功し、パケットの整合性が確認されている場合にのみ、パケットが通過します。それ以外の場合は、パケットがドロップされます。

### パケットの通過を許可する

パケットがルールに一致したときに、ルール アクションが許可してクリアに設定されている場合、パケットにアクションが実行されず、そのまま通過します。

### パケットのドロップ

パケットは、次の場合にドロップされます。

- ホストにキーがない場合
- アクションに矛盾がある場合。たとえば、テキスト形式でパケットを受信したときに、ルール アクションに「暗号化」を設定します。

## DNE 設定の管理

デフォルトでは、DNE が無効になっています。DNE 暗号化パケットのポート ミラーリングも無効になっています。両方とも、NSX Manager のグラフィカル ユーザー インターフェイスから有効にすることができます。

パケットは影響を受けやすく、ポート ミラーリングを行う場合には特別な配慮が必要になるため、デフォルトでは、DNE 暗号化パケットのポート ミラーリングは無効になっています。この設定は、DNE で暗号化されていないパケットには影響しません。

### 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 [暗号化 (Encryption)] を選択します。
- 3 [設定 (Settings)] タブをクリックします。
- 4 DNE を有効または無効にするには、[DNE の有効化] の横にある [編集 (EDIT)] をクリックします。
  - a [DNE の有効化 (DNE Enablement)] 切り替えボタンをクリックします。
- 5 ポート ミラーリングを有効または無効にするには、[ポート ミラーリングの有効化] の横にある [編集 (EDIT)] をクリックします。
  - a [ポート ミラーリングの有効化 (Port Mirroring Enablement)] 切り替えボタンをクリックします。
- 6 [保存 (Save)] をクリックします。

### 結果

無効にすると、DNE はすべてのポリシー適用操作 (認証と暗号化) をすぐにサスペンドします。無効にしても既存のポリシー設定は削除されません。ポリシーが適用されないだけです。

## 暗号化ルール セクションの追加、編集および削除

暗号化ルール セクションを使用すると、暗号化ルール セットを編成したり、ルールを個別に管理しできます。また、ルールをグループとして適用することもできます。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を定義するなど、マルチテナントに使用されます。

暗号化ルール セクションは、1 つ以上の暗号化ルールから構成されます。それぞれの暗号化ルールは 1 つセクションにのみ属しています。セクションが親になり、暗号化ルールが子になります。暗号化ルールは、ルールに一致するネットワーク パケットの処理方法を定める手順から構成されます。

セクションの順序は、暗号化ルールの処理手順に影響します。[DNE がネットワーク パケットを処理する方法](#)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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。

- 4 セクションを追加するには、メニュー バーで、[セクションの追加 (Add Section)] 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)] を選択します。
  - a セクション名およびオプションの説明を入力します。
  - b セクションの位置を選択します。既存のセクションの上または下を選択します。

デフォルトのレイヤー 3 セクションの上にセクションを追加する場合、この選択はできません。
  - c [保存 (Save)] をクリックします。
- 5 セクションを編集するには、セクションの最初の列のメニュー アイコンをクリックするか、セクションを右クリックして、ポップアップ メニューから [編集 (Edit)] を選択します。
  - a 必要に応じて名前と説明を編集します。
  - b [保存 (Save)] をクリックします。
- 6 セクションを削除するには、セクションの最初の列のメニュー アイコンをクリックするか、セクションを右クリックして、ポップアップ メニューから [削除 (Delete)] を選択します。
  - a 確認のため、[削除 (Delete)] をクリックします。

#### 結果

NSX Manager のユーザー インターフェイスでは、追加したセクションの位置は変更できません。ただし、削除したり、別の場所に作成し直すことはできます。セクションの位置は、POST `/api/v1/network-encryption/sections/<section-id>?action=revise` API で変更することもできます。詳細については、『NSX-T API リファレンス』を参照してください。

## セクション内のすべての暗号化ルールの有効化と無効化

セクション内のすべての暗号化ルールを有効または無効にできます。無効にすると、ルールの処理中にそのセクションのすべての暗号化ルールが無視されます。

#### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。
- 4 セクション内のすべてのルールを有効にするには、セクションの最初の列のメニュー アイコンをクリックするか、セクションを右クリックして、ポップアップ メニューから [すべてのルールを有効にする (Enable all rules)] を選択します。
- 5 セクション内のすべてのルールを無効にするには、セクションの最初の列のメニュー アイコンをクリックするか、セクションを右クリックして、ポップアップ メニューから [すべてのルールを無効にする (Disable all rules)] を選択します。
- 6 [保存 (Save)] をクリックします。
- 7 確認のため、[保存 (Save)] をもう一度クリックします。

## セクション内のすべての暗号化ログの有効化と無効化

パケット処理に関する情報を記録するには、セクション内のすべての暗号化ルールログを有効にします。暗号化ログには、セクション内のルールに一致するパケットとトラフィックの情報が記録されます。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。
- 4 セクション内のすべてのルールでログの記録を有効または無効にするには、セクションの最初の列のメニュー アイコンをクリックするか、セクションを右クリックして、ポップアップ メニューから [すべてのログを有効にする (Enable all logs)] または [すべてのログを無効にする (Disable all logs)] を選択します。
- 5 [保存 (Save)] をクリックします。
- 6 確認のため、[保存 (Save)] をもう一度クリックします。

## 暗号化ルールについて

暗号化ルールでは、保護するデータ フロー（送信元と宛先）、パケットがルールの条件に一致した場合に実行するアクション、ポリシー適用ポイントを定義します。

暗号化ルールには、パケットのプロパティに基づいてネットワーク パケットを処理する方法が定義されています。

- パケットの暗号化/復号と整合性チェックを実行する。
- 整合性チェックを実行するが、パケットは暗号化しない。
- パケットをそのまま通過させる（プレーンで許可する）。

各ネットワーク パケットに対して、優先順序に従って暗号化ルールが処理されます。最初のセクションの最初のルールから順番に処理されます。ルールの順序によって結果が異なります。[DNE がネットワーク パケットを処理する方法](#)を参照してください。

次の表では、暗号化ルール セクションの列について説明します。

カラム名	説明
#	この暗号化ルールのセクション内の位置を定義する一意の番号。リストの最初の暗号化ルールが 1 になります。この位置により、ルールの評価順序が決まります。リストでルールを上または下に移動すると、番号が自動的に更新されます。
名前	このルールの名前。
ID	暗号化ルールに対してシステムが生成した一意の ID。読み取り専用。
送信元	これらのフィールドは、パケットの送信元アドレスと比較されます。次の論理構造の個々または同種のコレクション (NS グループ/コンテナ) から構成されます。 <ul style="list-style-type: none"> <li>■ 論理ポート</li> <li>■ 論理スイッチ</li> <li>■ NSGroup</li> </ul>

カラム名	説明
宛先	<p>パケットの宛先アドレスと比較されます。次の論理構造の個々または同種のコレクション（NS グループ/コンテナ）から構成されます。</p> <ul style="list-style-type: none"> <li>■ 論理ポート</li> <li>■ 論理スイッチ</li> <li>■ NSGroup</li> </ul>
サービス	宛先ポートとプロトコル（HTTP など）を表します。ポートの範囲とポート セットもサポートします。ポート セットは、1 ルールあたり 15 個に制限されます。サービスのポート/プロトコルは無効にできません。
アクション	<p>このルールのアクションを指定します。次のいずれかの値：</p> <ul style="list-style-type: none"> <li>■ 暗号化と整合性チェック</li> <li>■ 整合性チェックのみ</li> <li>■ 許可</li> </ul>
キー ポリシー	このルールに使用するキー ポリシー。
適用先	<p>ポリシー適用ポイントを指定します。次の 1 つ以上のオプション：</p> <ul style="list-style-type: none"> <li>■ 論理ポート</li> <li>■ 論理スイッチ</li> <li>■ 論理スイッチ ポートの NSGroup（コンテナ）</li> </ul>
ログを記録	このセクションの暗号化ルールのログの記録をハイパーバイザーでオンにするには、この設定を有効にします。暗号化ルールのログの記録は、デフォルトで無効になっています。
統計	実行時の処理の統計情報（ルール ID、送受信されたパケット数、バイト数など）と統計が最後に更新された日時のタイムスタンプ。これらの値は、すべてのホストの集計値を表します。統計の集計は暗号化ルールの作成時から開始し、デフォルトでは 5 分間隔で更新されます。画面の更新は手動でも実行できます。
メモ	このルールに関連付けられているメモ。

デフォルトでは、[ID]、[ログ (Log)]、[メモ (Notes)] は表示されません。左下にある [列 (Columns)] をクリックすると、表示する列を選択できます。

暗号化ルールを定義する場合の考慮事項：

- Edge ノードでは DNE がサポートされていないため、DNE で暗号化されたトラフィックはドロップされます。したがって、Edge ノードを通過するトラフィックのルールは作成しないでください。
- ESXi 上の仮想マシンは、KVM 上の仮想マシンに暗号化されたトラフィックを送信できません。
- 送信元または宛先に「ANY」を使用すると、問題が発生する場合があります。トポロジによっては、この設定を行うと、Edge ノードを通過するトラフィックが誤って含まれる可能性があります。
- 重要：暗号化ルールがハイパーバイザーに適用される場合は、VTEP インターフェイスの MTU サイズを 1,700 以上にする必要があります（2,000 以上を推奨）。

## 暗号化ルールの追加、クローン作成および削除

暗号化ルールは 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。各ルールの送信元と宛先に複数のオブジェクトを追加することで、追加する暗号化ルールの総数を減らすことができます。

**注：** ルールを設定し、論理ポート、論理スイッチ、または論理ポートや論理スイッチを含む NSGroups を使用して、Sources または Destinations フィールドを指定した場合、有効な IP アドレスで解決できないスイッチまたはポートにはルールが適用されません。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。
- 4 ルールを追加するには、ルールを追加するセクションを選択します。
  - a [ルールの追加 (Add Rule)] をクリックして、[ルールを上追加 (Add Rule Above)] または [ルールを下追加 (Add Rule Below)] を選択します。
  - b (オプション) ルールの設定を編集します。
- 5 ルールのクローンを作成するには、クローンを作成するルールを選択します。
  - a [アクション (Actions)] をクリックして、[ルールのクローン作成 (Clone Rule)] を選択します。  
暗号化ルールのクローンは同じ設定で作成されますが、名前は異なります ([Copy of ...] が付きます)。
  - b (オプション) ルールの設定を編集します。
- 6 ルールを削除するには、削除するルールを選択します。
  - a [ルールの削除 (Delete Rule)] をクリックします。
- 7 [保存 (Save)] をクリックします。
- 8 確認のため、[保存 (Save)] をもう一度クリックします。

## 暗号化ルールの編集

ルールを追加したり、クローンを作成した後で、ルールの設定を編集できます。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。  
ルールとルール セクションのリストが表示されます。ウィンドウの下部にある [列 (Columns)] をクリックすると、表示する列を選択できます。

- 4 編集可能な設定を編集するには、セルをダブルクリックするか、セルの右上にマウスを移動して鉛筆のアイコンをクリックします。

[#]、[ID]、[統計 (Stats)] を除くすべての列が編集可能です。[送信元 (Sources)]、[宛先 (Destinations)]、[サービス (Services)]、[適用先 (Applied To)] フィールドを編集するときに、ドラッグアンドドロップを使用できます。

- 5 ドラッグアンドドロップでフィールドを編集するには、右上隅にある [オブジェクト (Objects)] をクリックして、ポップアップ ウィンドウを開きます。
  - a [タイプ (Type)] ドロップダウン リストからオブジェクト タイプを選択して、オブジェクトのリストを表示します。
  - b 宛先フィールドにオブジェクトをドラッグアンドドロップします。
  - c [オブジェクト (Objects)] を再度クリックして、ポップアップ ウィンドウを閉じます。
- 6 [送信元 (Sources)] と [宛先 (Destinations)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。

---

**注：** 送信元に **任意** を選択することは推奨しません。

SpoofGuard が有効になっていない場合は、悪意のある仮想マシンが別の仮想マシンのアドレスを要求する可能性があるため、自動検出されたアドレスのバインドの信頼性は保証されません。このような要求が行われても警告されません。SpoofGuard が有効な場合、検出されたバインドがすべて検証され、承認されたバインドのみが表示されます。

---

- a [タイプ (Type)] ドロップダウン リストからオブジェクト タイプを選択して、オブジェクトのリストを表示します。
 

使用可能なタイプは論理ポート、論理スイッチ、NSGroup です。DNE の場合、NSGroup に MAC セットまたは IP セットを含めることはできません。
  - b [使用可能] 列で 1 つ以上のオブジェクトを選択します。
 

[使用可能] の横にあるチェックボックスをクリックして、すべてのオブジェクトを選択します。
  - c 右矢印アイコンをクリックして、選択したオブジェクトを [選択済み] 列に移動します。
  - d 必要であれば、この手順を別のオブジェクト タイプで繰り返します。
  - e [OK] をクリックします。
- 7 [サービス (Services)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。
    - a [使用可能] 列で 1 つ以上のサービスを選択します。
    - b 右矢印アイコンをクリックして、選択したサービスを [選択済み] 列に移動します。

- c (必須) [新しい NSService の作成 (Create New NSService)] をクリックすると、新しいサービスを作成できます。

サービスの詳細を設定します。

オプション	説明
名前と説明	名前を入力します。必要に応じて説明も入力します。
サービスのタイプ	使用可能なサービス タイプの 1 つを選択します。 <ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IP アドレス</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。
送信元ポート	送信元ポートを入力します。
宛先ポート	宛先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。

- d (必須) [Raw プロトコル (Raw Protocol)] タブをクリックして、[追加 (Add)] をクリックしてプロトコルを追加します。

プロトコルの詳細を設定します。

オプション	説明
サービスのタイプ	使用可能なサービス タイプの 1 つを選択します。 <ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IP アドレス</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。
送信元ポート	送信元ポートを入力します。
宛先ポート	宛先ポートを入力します。

- e [OK] をクリックします。

## 8 [アクション (Action)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。

- a [アクション (Action)] ドロップダウン リストからアクションを選択します。

オプション	説明
暗号化と整合性チェック	デフォルトです。認証と暗号化を行います。
整合性チェックのみ	認証のみを行います。
許可	認証または暗号化を行わずにパケットの通過を許可します。

- b [OK] をクリックします。



- 9 [キー ポリシー (Key Policy)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。
  - a [キー ポリシー (Key Policy)] ドロップダウン リストからポリシーを選択します。  
デフォルトは System\_Encryption\_and\_Integrity です。
  - b [OK] をクリックします。
- 10 [適用先 (Applied To)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。
  - a [タイプ (Type)] ドロップダウン リストからオブジェクト タイプを選択して、オブジェクトのリストを表示します。  
使用可能なタイプは論理ポート、論理スイッチ、NSGroup です。DNE の場合、NSGroup に MAC セットまたは IP セットを含めることはできません。
  - b [使用可能] 列で 1 つ以上のオブジェクトを選択します。  
[使用可能] の横にあるチェックボックスをクリックして、すべてのオブジェクトを選択します。
  - c 右矢印アイコンをクリックして、選択したオブジェクトを [選択済み] 列に移動します。
  - d 必要であれば、この手順を別のオブジェクト タイプで繰り返します。
  - e [OK] をクリックします。
- 11 [ログ (Log)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。
  - a [ログ (Log)] 切り替えボタンをクリックして、ログの記録を有効または無効に設定します。
  - b [OK] をクリックします。
- 12 [メモ (Notes)] を編集するには、鉛筆のアイコンをクリックしてダイアログ ボックスを開きます。
  - a [メモ (Notes)] テキスト フィールドにメモを入力します。
  - b [OK] をクリックします。

## 結果

[統計 (Stats)] フィールドは編集できません。このフィールドにマウスを移動すると、ポップアップが開き、暗号化ルールの統計が表示されます。デフォルトでは、暗号化ルールの作成時から 5 分間隔で統計が蓄積されます。これらの値は、すべてのホストの統計情報を表します。これらの値は、自動的に更新されません。この画面の値を手動で更新するには、セルを右クリックして [更新 (Refresh)] を選択します。

## 暗号化ルールの有効化と無効化

暗号化ルールを有効または無効にできます。デフォルトでは、暗号化ルールが有効になっています。無効なルールは無視され、有効なルールが適用されます。

## 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。

- 4 ルールの最初の列のメニュー アイコンをクリックして、ポップアップ メニューから [有効 (Enable)] または [無効 (Disable)] を選択します。
- 5 [保存 (Save)] をクリックします。
- 6 確認のため、[保存 (Save)] をもう一度クリックします。

## 暗号化ルールのログの記録の有効化と無効化

暗号化ルールのログの記録を有効にすると、処理されるパケットの情報を記録できます。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。

ログの記録は、デフォルトで無効になっています。ESXi ホストでは、ログは `/var/run/log/dnepktlogs.log` ファイルに記録されます。ルール数にもよりますが、標準的な暗号化ルール セクションの場合、大量のログ情報が生成され、パフォーマンスに影響を及ぼす場合があります。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。
- 4 ログの記録を有効または無効にするルールをクリックします。
- 5 [アクション (Actions)] メニューをクリックして、[有効 (Enable)] - [ルールの有効化のログ (Enable Rule Logs)] の順にクリックするか、[無効 (Disable)] - [ルールの無効化のログ (Disable Rule Logs)] の順に選択します。
- 6 [保存 (Save)] をクリックします。
- 7 確認のため、[保存 (Save)] をもう一度クリックします。

## 暗号化ルールの順序の変更

エンドポイントを通過するトラフィックの場合、パケット情報にルールが適用されます。セクション内でリストの先頭から順番にルールが処理されます。リストの先頭は、最も優先順位の高いルールです。

リスト内で順序を変更すると、優先順位が変わります。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。たとえば、セキュリティ グループ A と B 間で FTP トラフィックの暗号化と認証を行い、セキュリティ グループ A と B 間の他のトラフィックには認証のみを行う場合、FTP ルール（アクションに暗号化と整合性チェックを設定）は、他のトラフィックを処理するルール（アクションに整合性チェックを設定）よりも優先的に処理される必要があります。そうしないと、FTP トラフィックに整合性チェックのみが実行されます。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。

- 4 ルールを選択します。
- 5 メニュー バーで [上へ移動 (Move Up)] または [下へ移動 (Move Down)] をクリックするか、最初の列のメニュー アイコンをクリックして、[上へ移動 (Move Down)] または [下へ移動 (Move Up)] を選択します。
- 6 [保存 (Save)] をクリックします。
- 7 確認のため、[保存 (Save)] をもう一度クリックします。

## 暗号化ルールのフィルタリング

[暗号化] セクションに移動すると、最初はすべてのルールが表示されています。フィルタを使用すると、ルールのサブセットのみを表示するように表示内容を制御できます。これにより、ルールを簡単に管理できます。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[ルール (Rules)] タブをクリックします。
- 4 メニュー バーの右側にある検索テキスト フィールドで、虫眼鏡アイコンをクリックしてオブジェクトを選択するか、オブジェクト名の最初の数文字を入力して、選択するオブジェクトのリストを絞り込みます。

オブジェクトを選択すると、フィルタが適用され、ルールのリストが更新されます。以下の列にオブジェクトを含むルールのみが表示されます。

- 送信元
- 宛先
- 適用先
- サービス
- キー ポリシー

- 5 フィルタを削除するには、テキスト フィールドからオブジェクト名を削除します。

## キー ポリシーについて

ルールでキーが必要な場合、キー ポリシーを使用して、ネットワーク パケットに使用するキー インスタンスを決定します。

キーは、DNE が暗号化と整合性チェックに使用する暗号化トークンです。DNE は 128 ビットの AES-GCM をサポートします。

2 つのシステム デフォルト キー ポリシーがあります。

- System\_Encryption\_and\_Integrity は暗号化と整合性チェックを行います。
- System\_Integrity\_Only は整合性チェックのみを行います。

[暗号化 (Encryption)] - [キー (Keys)] タブの順に移動すると、キー ポリシーのプロパティを表示できます。

表 8-3. [キー (Keys)] タブの列

列の名前	説明
名前	キー ポリシーの名前。
ID	システム生成のキー ポリシー固有の ID 読み取り専用。暗号化ルールと暗号化ルールのセクションで参照されます。
アクション	キー ポリシーの目的。可能な値： <ul style="list-style-type: none"> <li>■ 暗号化と整合性チェック</li> <li>■ 整合性チェックのみ</li> </ul>
アルゴリズム	暗号化アルゴリズム。AES GCM のみがサポートされます。
MAC アルゴリズム	MAC アルゴリズム。AES GCM のみがサポートされます。
キーの長さ	128 ビットのみがサポートされます。
デフォルト	ポリシーがシステムのデフォルトかどうかを示します。
ローテーションの頻度	ローテーションの頻度（日数）。最小値は 1 です。
メモ	このキーの説明。
作成時間	このポリシーが作成された日時。
最終更新	このポリシーの最終更新日時。
統計	実行時の処理の統計情報（送受信されたパケット数、バイト数など）と統計が最後に更新された日時のタイムスタンプ。これらの値は、すべてのホストの集計値を表します。統計の集計は暗号化ルールの作成時から開始し、デフォルトでは 5 分間隔で更新されます。画面の更新は手動でも実行できます。
次のローテーション時間	キーのローテーションを次に行う日時。

デフォルトでは、一部の列しか表示されません。左下にある [列 (Columns)] をクリックすると、表示する列を選択できます。

## キー ポリシーの追加、編集および削除

キー ポリシーを追加または編集できます。追加したポリシーを削除できますが、事前定義の 2 つのシステム デフォルト ポリシーは削除できません。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[キー (Keys)] タブをクリックします。

- 4 ポリシーを追加するには、[追加 (Add)] をクリックします。ポリシーを編集するには、ポリシーを選択して [編集 (Edit)] をクリックします。
  - a ポリシーの詳細をすべて設定します。

オプション	説明
名前	ポリシーの名前。
デフォルトとして設定	ポリシーがシステムのデフォルトかどうかを設定します。
アクション	[暗号化と整合性チェック (Encrypt and Check Integrity)] または [整合性チェックのみ (Check Integrity Only)] を選択します。
ローテーションの頻度	日数を入力します。
メモ	このポリシーの説明。

**注：** [MAC アルゴリズム (MAC Algorithm)]、[アルゴリズム (Algorithm)]、[キーの長さ (Key Strength)] プロパティには事前に値が選択されています。これらの値は変更できません。

- b [保存 (Save)] をクリックします。
- 5 ポリシーを削除するには、ポリシーを選択して [削除 (Delete)] をクリックします。
  - a 確認のため、[削除 (Delete)] をクリックします。

## キー ポリシーのローテーション

キー ローテーションは、DNE Key Manager から新しいキーを取得するプロセスです。ローテーションは、頻度と有効期限の設定に基づいて自動的に行われます。キーのローテーションは手動でも実行できます。

### 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[キー (Keys)] タブをクリックします。
- 4 ローテーションするポリシーを選択します。
- 5 [アクション (Actions)] をクリックして、[ローテーション (Rotate)] を選択します。
- 6 [OK] をクリックします。

## キー ポリシーの失効

キーの失効は、キーを無効にして使用不能にするプロセスです。失効は通常、データ漏えいなど、何らかの理由で 1 つ以上のキーが信頼できなくなったときに行います。キーの失効では、キーの使用を停止し、DNE Key Manager に新しいキーを要求します。ホストが新しいキーを待っている間、一部のパケットがドロップされる可能性があるため、失効はトラフィックに影響を及ぼします。

## 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 [暗号化 (Encryption)] を選択します。
- 3 まだ選択していない場合は、[キー (Keys)] タブをクリックします。
- 4 失効するポリシーを選択します。
- 5 [アクション (Actions)] をクリックして、[失効 (Revoke)] を選択します。
- 6 [OK] をクリックします。

# オブジェクト、グループ、サービス、仮想マシンの管理

## 9

IP セット、IP アドレス プール、MAC セット、NSGroups、NSServices を作成できます。仮想マシンのタグを管理することもできます。

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
- 仮想マシンのタグの管理

## 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 ルールまたは DNE（分散ネットワーク暗号化）ルールで、送信元、宛先、Applied To フィールドに NSGroup を指定できます。

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、論理ポートまたは仮想マシンに適用するにはメンバーシップ基準を 5 つまで指定できます。論理スイッチ、論理ポートまたは仮想マシンに適用される条件には、タグと範囲を指定できます（範囲はオプションです）。さらに、仮想マシンに適用される条件の場合、文字列の先頭、最後、途中に特定の文字がある名前を指定できます。
- 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。
- サポートされる仮想マシンの最大数は 10,000 です。

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、仮想マシンおよび 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 まだ選択していない場合は、[グループ (GROUPS)] タブをクリックします。
- 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。

条件は、論理スイッチ、論理ポートまたは仮想マシンに適用できます。論理スイッチ、論理ポートまたは仮想マシンに適用される条件には、タグと範囲を指定できます (範囲はオプションです)。仮想マシンに適用される条件の場合、文字列の先頭、最後、途中に特定の文字がある名前を指定できます。

- 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 を使用すると、ファイアウォール ルールと DNE (分散ネットワーク暗号化) ルールで特定のタイプのトラフィックを許可またはブロックできます。

NSService には、次のようなタイプがあります。

- Ether
- IP アドレス
- IGMP
- ICMP
- ALG
- L4 ポート セット

L4 ポート セットは、送信先ポートおよび宛先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 ルールや DNE（分散ネットワーク暗号化）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] 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] 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] 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]、[IGMP]、[ICMP]、[ALG]、および [L4 ポート セット] 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] および [レイヤー 3 以上] です。
- 9 [保存] をクリックします。

## 仮想マシンのタグの管理

インベントリ内の仮想マシンのリストを表示できます。仮想マシンにタグを追加することで、検索が容易になります。

### 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、[インベントリ] - [仮想マシン] の順に選択します。

仮想マシンのリストは、[仮想マシン]、[外部 ID]、[ソース]、および [タグ] の 4 つの列で表示されます。最初の 3 つの列の見出しのフィルタ アイコンをクリックすると、リストをフィルタできます。文字列を入力すると、部分一致検索が行われます。列内の文字列に、入力した文字列が含まれている場合、そのエントリが表示されます。文字列を二重引用符で囲んで入力すると、完全一致検索が行われます。列内の文字列が、入力した文字列と完全に一致する場合、そのエントリが表示されます。

## 3 仮想マシンを選択します。

## 4 [タグの管理] をクリックします。

## 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] 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] をクリックします。

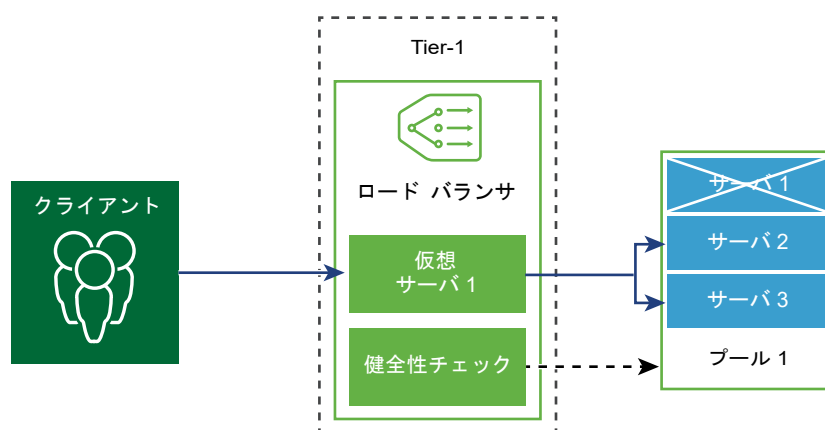
1 台の仮想マシンに、最大で 15 個のタグを指定できます。

## 6 [保存] をクリックします。

# 論理ロード バランサ

# 10

NSX-T 論理ロード バランサは、アプリケーションの高可用性サービスを提供し、複数のサーバ間でネットワーク トラフィックの負荷を分散します。



ロード バランサは、受信サービス リクエストを複数のサーバ間で均等に配分します。負荷の配分は、ユーザーに透過的に行われます。ロード バランシングは、最適なリソース使用率の実現、スループットの最大化、応答時間の最小化、過負荷の回避に役立ちます。

ロード バランシング用に、1 つの仮想 IP アドレスを一連のプール サーバにマッピングできます。ロード バランサは仮想 IP アドレスに対する TCP、UDP、HTTP、または HTTPS リクエストを受け入れ、どのプール サーバを使用するかを決定します。

環境によっては、仮想サーバとプール メンバーを増やし、負荷の高いネットワーク トラフィックを処理することによって、ロード バランサのパフォーマンスを高めることができます。

**注：** 論理ロード バランサは、Tier-1 論理ルーターでのみサポートされます。1 つのロード バランサは、1 つの Tier-1 論理ルーターにのみ接続できます。

この章には、次のトピックが含まれています。

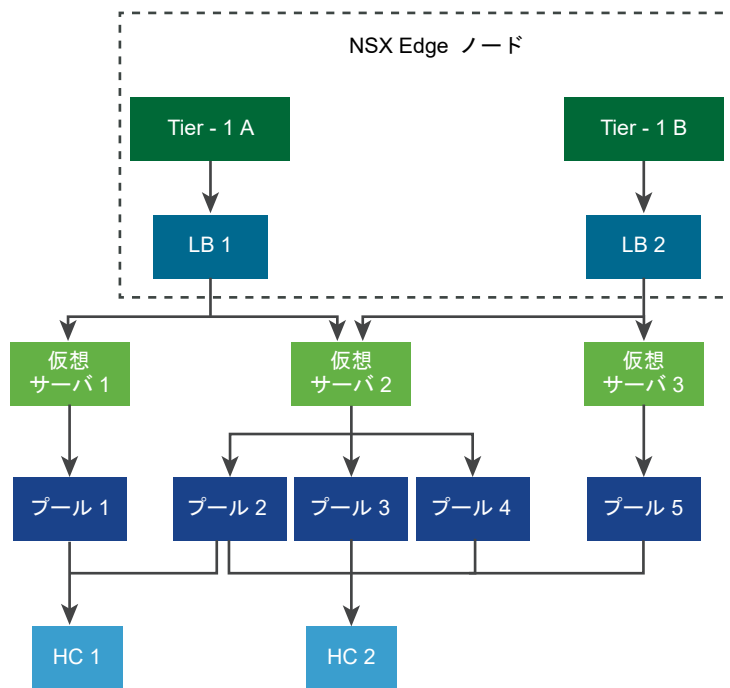
- [キー ロード バランサの概念](#)
- [ロード バランサ コンポーネントの構成](#)

## キー ロード バランサの概念

ロード バランサには、仮想サーバ、サーバ プール、健全性チェック モニターが含まれます。

ロード バランサは Tier-1 論理ルーターに接続されています。ロード バランサは 1 台または複数の仮想サーバをホストします。仮想サーバはアプリケーション サービスを抽象化したものであり、IP アドレス、ポート、プロトコルの一意の組み合わせによって表されます。仮想サーバは 1 つまたは複数のサーバ プールに関連付けられます。サーバ プールは、サーバのグループで構成されます。サーバ プールには、個々のサーバ プール メンバーが含まれます。

サーバの健全性を確認する健全性チェック モニターを追加すると、各サーバでアプリケーションが正しく実行されているかどうかを確認できます。



## ロード バランサ リソースの拡張

ロード バランサは、小規模、中規模、および大規模に利用できます。ロード バランサの規模に基づいて、ロード バランサは異なる仮想サーバとプール メンバーをホストすることができます。

ロード バランサは 1 つの Tier-1 論理ルーターに接続されています。この Tier-1 論理ルーターは、Tier-0 論理ルーターを使用して既存の NSX Edge ノードの 1 つに接続されています。NSX Edge は、フォーム ファクタとして、ベア メタル、小規模、中規模、および大規模の仮想マシン アプライアンスを備えています。フォーム ファクタに基づいて、NSX Edge ノードは異なる数のロード バランサをホストすることができます。

ロード バランサ (LB) の規模とパフォーマンス

	小規模 LB	中規模 LB	大規模 LB
仮想サーバの数	10	100	1000
プール メンバーの数	30	300	3000

NSX Edge あたりのロードバランサ (LB)

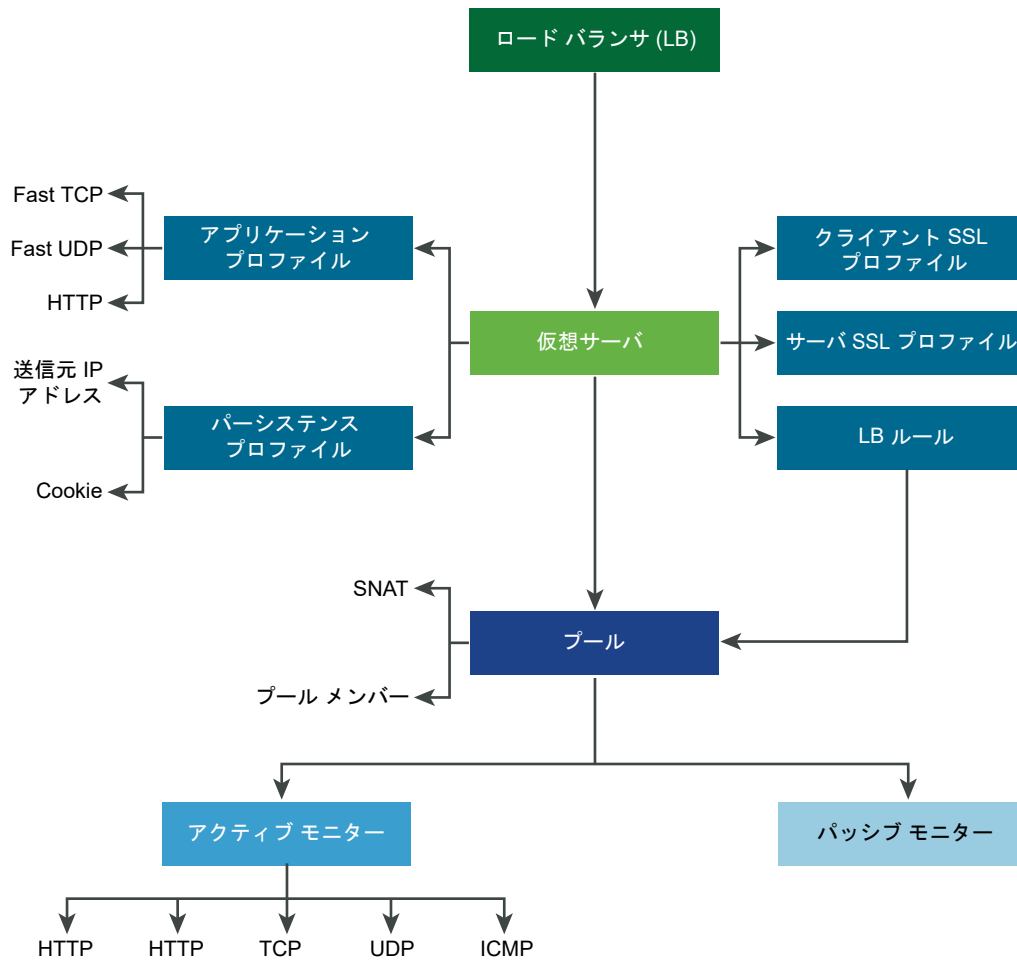
	小規模 LB	中規模 LB	大規模 LB
NSX Edge 仮想マシン – 小規模	該当なし	該当なし	該当なし
NSX Edge 仮想マシン – 中規模	1	該当なし	該当なし
NSX Edge 仮想マシン – 大規模	4	1	該当なし
NSX Edge – ペア メタル	100	10	1

## サポートされているロード バランサの機能

NSX-T ロード バランサは、次の機能をサポートしています。

- レイヤー 4 - TCP および UDP
- レイヤー 7 - ロード バランサ ルールがサポートされている HTTP および HTTPS
- サーバ プール：静的および動的（NSGroup を使用）
- パーシステンス：送信元 IP および Cookie のパーシステンス モード
- 健全性チェック モニター：HTTP、HTTPS、TCP、UDP、ICMP を含むアクティブ モニターおよびパッシブ モニター
- SNAT：透過的、自動マップ、IP アドレス リスト

注：SSL - NSX-T 2.1 リリースでは、終了モードとプロキシ モードはサポートされていません。



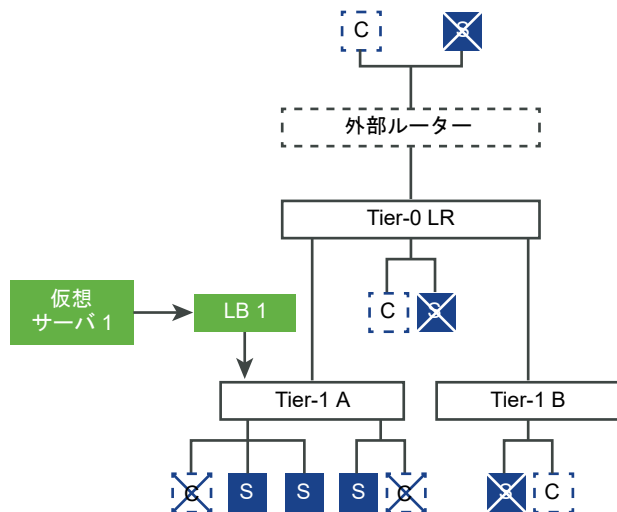
## ロード バランサ トポロジ

通常、ロード バランサはインライン モードまたはワンアーム モードのいずれかで展開されます。

### インライン トポロジ

インライン モードでは、ロード バランサはクライアントとサーバ間のトラフィック パスに配置します。クライアントとサーバを同じ Tier-1 論理ルーターに接続することはできません。このトポロジでは、仮想サーバで SNAT は必要ありません。

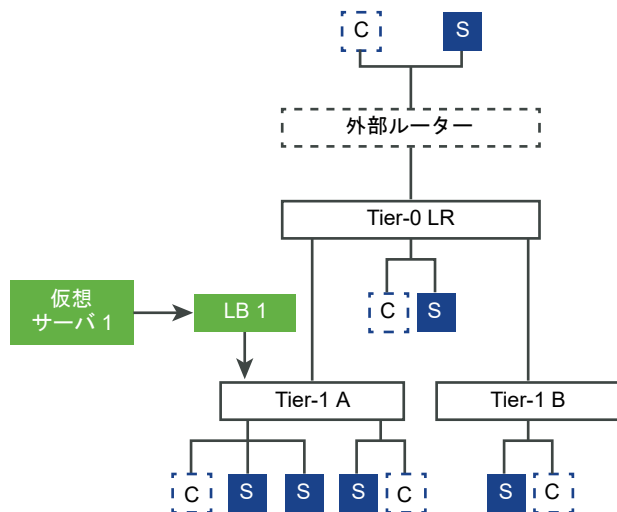




## ワンアーム トポロジ

ワンアーム モードでは、ロード バランサはクライアントとサーバ間のトラフィック パスに配置しません。このモードでは、クライアントとサーバは任意の場所に配置できます。ロード バランサは、送信元の NAT (SNAT) を実行して、サーバからクライアントへのリターン トラフィックがロード バランサを通過するように強制します。このトポロジでは、仮想サーバで SNAT を有効にする必要があります。

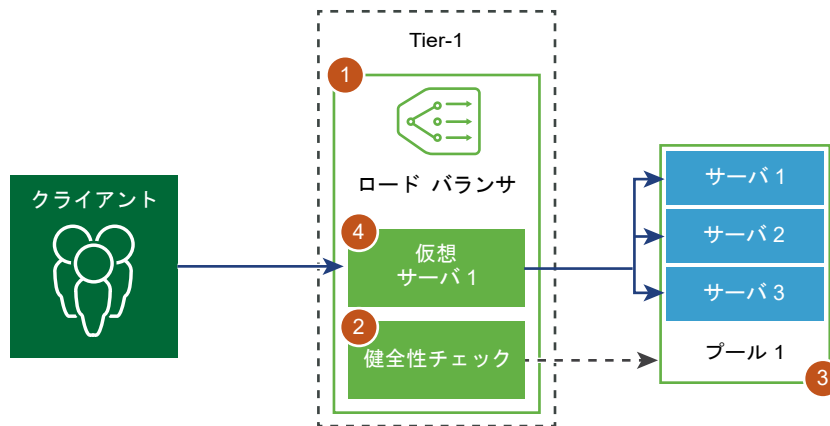
ロード バランサは仮想 IP アドレスに送信されるクライアント トラフィックを受信すると、サーバ プール メンバーを選択してクライアント トラフィックを転送します。ワンアーム モードでは、ロード バランサはクライアントの IP アドレスをロード バランサの IP アドレスで置き換えることで、サーバの応答が常にロード バランサに送信され、ロード バランサがその応答をクライアントに転送できるようになります。



## ロード バランサ コンポーネントの構成

論理ロード バランサを使用するには、最初にロード バランサを構成して、Tier-1 論理ルーターに接続する必要があります。

次に、サーバに対する健全性チェック監視を設定できます。その次に、ロード バランサのサーバ プールを構成する必要があります。最後に、ロード バランサ用のレイヤー 4 またはレイヤー 7 仮想サーバを作成する必要があります。

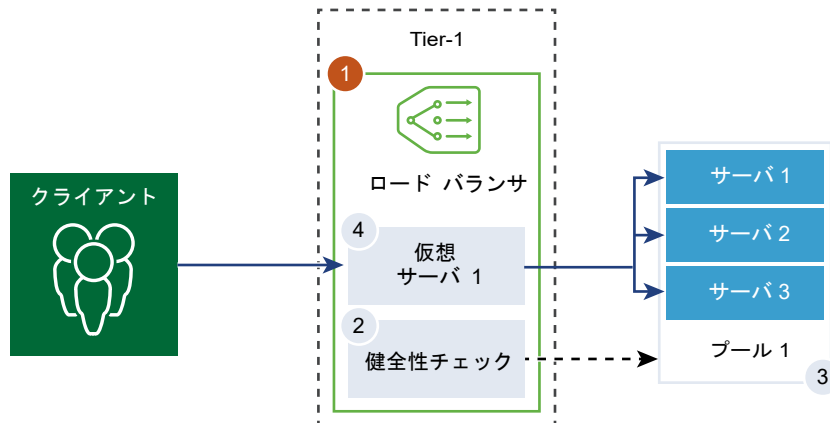


## ロード バランサの作成

ロード バランサが作成され、Tier-1 論理ルーターに接続されています。

ロード バランサのエラー ログに追加するエラー メッセージのレベルを設定できます。

**注：** トラフィックが多い場合は、ロード バランサのログ レベルをデバッグに設定しないでください。ログに出力されるメッセージ数が増えて、パフォーマンスが低下します。



### 前提条件

Tier-1 論理ルーターが設定されていることを確認します。[Tier-1 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 [ロード バランサ (Load Balancer)] - [追加 (Add)] の順に選択します。
- 3 ロード バランサの名前および説明を入力します。

- 4 使用可能なリソースに基づいて、ロード バランサの仮想サーバのサイズおよびプール メンバーの数を選択します。
- 5 ドロップダウン メニューで、エラー ログの重要度を定義します。

ロード バランサは、発生したさまざまな重要度の問題に関する情報を収集して、エラー ログに記録します。
- 6 [OK] をクリックします。
- 7 新たに作成されたロード バランサを仮想サーバに関連付けます。
  - a ロード バランサを選択し、[アクション (Actions)] - [仮想サーバに接続 (Attach to a Virtual Server)] の順にクリックします。
  - b ドロップダウン メニューから既存の仮想サーバを選択します。
  - c [OK] をクリックします。
- 8 新たに作成されたロード バランサを、Tier-1 論理ルーターに接続します。
  - a ロード バランサを選択し、[アクション (Actions)] - [論理ルーターに接続 (Attach to a Logical Router)] の順にクリックします。
  - b ドロップダウン メニューから既存の Tier-1 論理ルーターを選択します。

Tier-1 ルーターはアクティブ/スタンバイ モードにする必要があります。
  - c [OK] をクリックします。
- 9 (オプション) ロード バランサを削除します。

このロード バランサの使用を停止する場合は、まずロード バランサを仮想サーバおよび Tier-1 論理ルーターから切断する必要があります。

## アクティブ健全性モニターの構成

アクティブ健全性モニターは、サーバが使用可能かどうかをテストする際に使用します。アクティブ健全性モニターでは、基本的なサーバへの ping 送信や高度な HTTP の要求などのさまざまなタイプのテストを使用してアプリケーションの健全性を監視します。

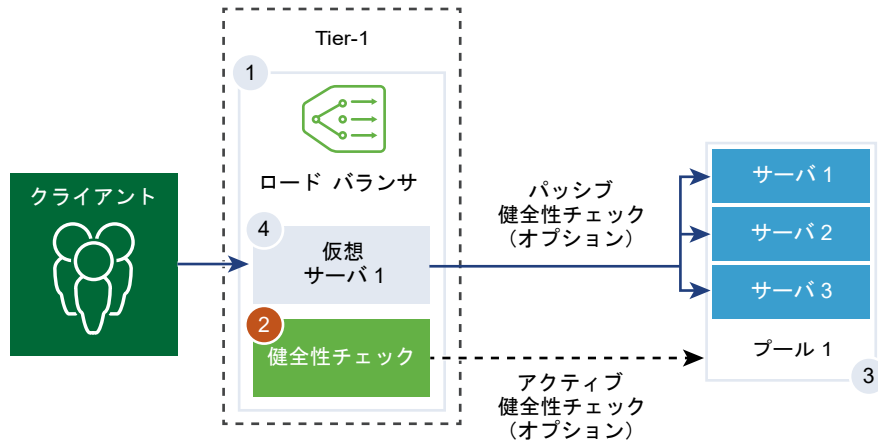
一定期間内に応答しなかったサーバまたは応答時にエラーが発生したサーバは、以降の定期的な健全性チェックでこれらのサーバが良好であることがわかるまで、この後の接続処理から除外されます。

アクティブ健全性チェックは、プール メンバーが仮想サーバに接続され、このサーバが Tier-1 論理ルーターに接続された後に、サーバ プールのメンバーに対して実行されます。健全性チェックには Tier-1 アップリンク IP アドレスが使用されます。

---

**注：** サーバ プールごとにアクティブ健全性モニターを 1 つ構成できます。

---



## 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 [ロード バランサ (Load Balancer)] - [サーバ プール (Server Pools)] - [アクティブ健全性モニタ (Active Health Monitors)] - [追加 (Add)] の順に選択します。
- 3 アクティブ健全性モニターの名前および説明を入力します。
- 4 ドロップダウン メニューでサーバの健全性チェック プロトコルを選択します。

NSX Manager で事前定義されたプロトコル (nsx-default-http-monitor、nsx-default-https-monitor、nsx-default-icmp-monitor、および nsx-default-tcp-monitor) を使用することもできます。

- 5 監視ポートの値を設定します。
- 6 サービス プールの監視に関連する値を設定します。

アクティブな健全性モニターのデフォルト値をそのまま使用することもできます。

オプション	説明
監視間隔	監視がサーバに別の接続要求を送信するまでの間隔を秒単位で設定します。
失敗カウント	障害の連続発生回数がこの値に達すると、そのサーバは一時的に使用不可能であると見なされます。
接続試行数	ここで設定したタイムアウト時間が経過すると、サーバに新しい接続がないかを調べ、アクセス可能かどうかを確認します。
タイムアウト期間	サーバはダウンしているものと見なされるまでのサーバのテスト回数を設定します。

たとえば、監視間隔が 5 秒、タイムアウトが 15 秒に設定されている場合、ロード バランサは 5 秒おきにサーバに要求を送信します。それぞれの検証で、15 秒以内に予期した応答がサーバから返された場合、健全性チェックの結果は [OK] になります。そうでない場合、結果は [重大] になります。最近実行した 3 回の健全性チェックの結果がすべて [稼動中] の場合、サーバは稼動していると思なされます。

## 7 健全性チェック プロトコルとして HTTP を選択した場合は、次の詳細を入力します。

オプション	説明
HTTP メソッド	ドロップダウン メニューで、サーバのステータスの検出方法を選択します (GET、OPTIONS、POST、HEAD、および PUT)。
HTTP 要求の URL	メソッドに使用する HTTP 要求の URI を入力します。
HTTP 要求バージョン	ドロップダウン メニューで、サポートされている要求のバージョンを選択します。 デフォルト バージョンの HTTP_VERSION_1_1 を受け入れることもできます。
HTTP 要求の本文	HTTP 要求の本文を入力します。 POST および PUT メソッドで有効です。
HTTP 応答コード	HTTP 応答本文のステータス行で一致すると予測される文字列を入力します。 応答コードは、カンマ区切りリストです。 たとえば、200,301,302,401 と指定します。
HTTP 応答の本文	HTTP 応答の本文の文字列と HTTP 健全性チェックの応答の本文が一致する場合、サーバは良好であると見なされます。

## 8 健全性チェック プロトコルとして HTTPS を選択した場合は、次の詳細を入力します。

### a SSL プロトコル リストを選択します。

TLS バージョンとして TLS1.1 および TLS1.2 がサポートされていて、デフォルトで有効になっています。  
TLS 1.0 はサポートされていますが、デフォルトで無効になっています。

### b 矢印をクリックし、選択済みセクションにプロトコルを移動します。

## 9 健全性チェック プロトコルとして ICMP を選択した場合は、ICMP 健全性チェックのパケット データ サイズをバイト単位で割り当てます。

## 10 健全性チェック プロトコルとして TCP を選択した場合は、パラメータを空白のままにします。

送信済みデータと予測データがどちらも表示されない場合は、サーバの健全性を検証するために 3 方向ハンドシェイク TCP 接続が確立されます。データは送信されません。予測データが表示されている場合、予測データは文字列でなければなりません。また、応答内の任意の場所に表示されることがあります。正規表現はサポートされません。

## 11 健全性チェック プロトコルとして UDP を選択した場合は、次の詳細を入力します。

必須オプション	説明
送信	接続が確立された後でサーバに送信する文字列を入力します。
受信	サーバから受信すると予測される文字列を入力します。 受信した文字列がこの定義と一致する場合にのみ、サーバが稼働状態と見なされます。

## 12 [終了 (Finish)] をクリックします。

### 次のステップ

アクティブ健全性モニターにサーバ プールを関連付けます。[ロード バランシング用サーバ プールの追加](#)を参照してください。

## パッシブ健全性モニターの設定

ロード バランサはパッシブ健全性チェックを実行してクライアント接続中の障害を監視し、連続して障害が発生しているサーバはダウンしているものとしてマークします。

パッシブ健全性チェックでは、ロード バランサを通過するクライアント トラフィックが監視され、障害が発生していないかどうかを確認されます。たとえば、プール メンバーがクライアント接続への応答で TCP リセット (RST) を送信すると、ロード バランサがその障害を検出します。特定のサーバ プール メンバーで複数の障害が連続して発生した場合、ロード バランサはそのプール メンバーが一時的に使用不可能であると見なし、しばらくの間、そのプール メンバーへの接続要求の送信を停止します。しばらく時間を置いてから、ロード バランサはそのプール メンバーが回復したかどうかを確認するために接続要求を送信します。接続に成功した場合、そのプール メンバーの状態は良好と見なされます。接続に失敗した場合、ロード バランサはしばらく待機してから接続を再度試みます。

パッシブ健全性チェックで次の状況が検出されると、クライアント トラフィックで障害が発生しているものと見なされます。

- サーバ プールがレイヤー 7 仮想サーバに関連付けられていて、プール メンバーへの接続に失敗した場合。たとえば、ロード バランサがプール メンバーへの接続や SSL ハンドシェイクを試みて失敗し、プール メンバーが TCP RST を送信した場合。
- サーバ プールがレイヤー 4 TCP 仮想サーバに関連付けられていて、プール メンバーがクライアントからの TCP SYN への応答として TCP RST を送信した場合、またはまったく応答しない場合。
- サーバ プールがレイヤー 4 UDP 仮想サーバに関連付けられていて、ポートに到達できない場合、またはクライアントの UDP パケットへの応答として宛先に到達できないことを示す ICMP エラー メッセージを受信した場合。

サーバ プールがレイヤー 7 仮想サーバに関連付けられている場合、TCP 接続エラー（データ送信時や SSL ハンドシェイク時の TCP RST エラーなど）が発生するたびに接続失敗のカウントが増加します。

サーバ プールがレイヤー 4 仮想サーバに関連付けられている場合、サーバ プール メンバーに送信された TCP SYN への応答がなかったり、TCP SYN への応答として TCP RST が送信されたりすると、そのサーバ プール メンバーはダウンしているものと見なされます。その場合、接続失敗のカウントが増加します。

レイヤー 4 UDP 仮想サーバの場合、クライアント トラフィックへの応答として ICMP エラー（ポートまたは宛先に到達できないことを示すメッセージなど）を受信すると、そのサーバはダウンしているものと見なされます。

---

**注：** パッシブ健全性モニターはサーバ プールごとに 1 つ設定できます。

---

### 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 [ロード バランサ (Load Balancer)] - [サーバ プール (Server Pools)] - [パッシブ健全性モニタ (Passive Health Monitors)] - [追加 (Add)] の順に選択します。
- 3 パッシブ健全性モニターの名前と説明を入力します。

#### 4 サービス プールの監視に関連する値を設定します。

アクティブな健全性モニターのデフォルト値をそのまま使用することもできます。

オプション	説明
失敗回数	障害の連続発生回数がこの値に達すると、そのサーバは一時的に使用不可能であると見なされます。
タイムアウト期間	サーバはダウンしているものと見なされるまでのサーバのテスト回数を設定します。

たとえば、この値が 5 に設定されている場合、特定のメンバーで障害が連続して 5 回発生すると、そのメンバーは 5 秒間、一時的に使用不可能であると見なされます。この期間が過ぎると、そのメンバーへの接続が新たに試みられ、使用可能であるかどうかを確認されます。接続が成功した場合、そのメンバーは使用可能と見なされ、失敗回数はゼロに設定されます。接続に失敗した場合、そのメンバーは新たに 5 秒のタイムアウト期間が過ぎるまで使用されません。

#### 5 [OK] をクリックします。

##### 次のステップ

パッシブ健全性モニターをサーバ プールに関連付けます。[ロード バランシング用サーバ プールの追加](#) を参照してください。

## ロード バランシング用サーバ プールの追加

サーバ プールは、同じアプリケーションを実行する構成済みの 1 台以上のサーバで構成されています。レイヤー 4 およびレイヤー 7 の両方の仮想サーバに 1 つのプールを関連付けることができます。

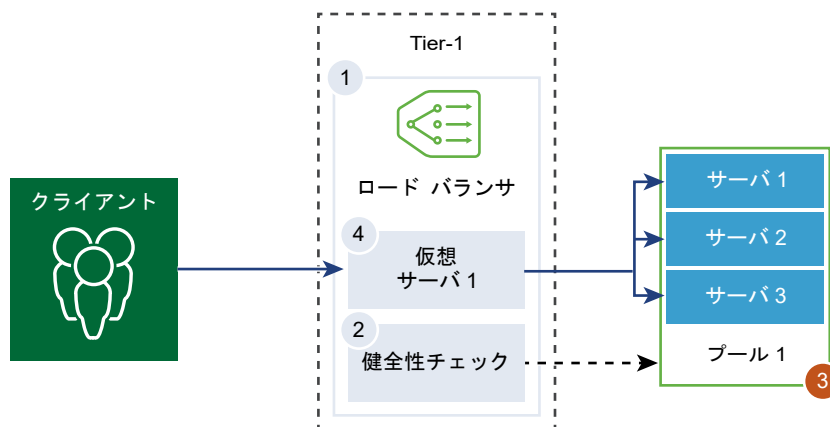
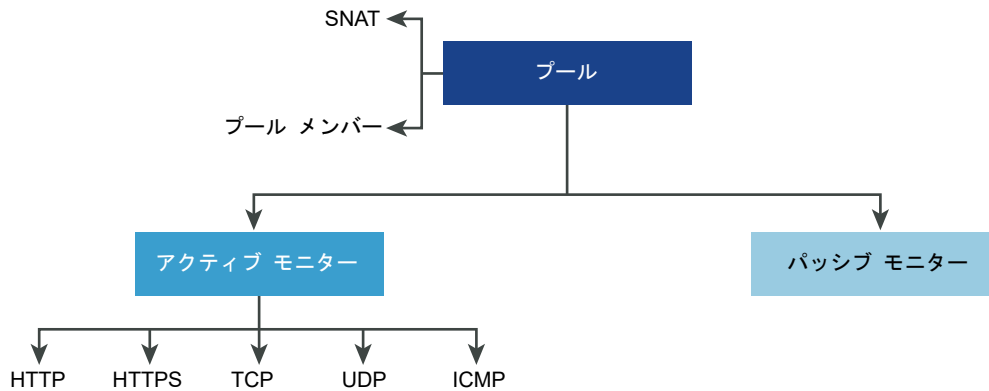


図 10-1. サーバ プール パラメータの設定



## 前提条件

- 動的プールのメンバーを使用する場合は、NSGroup を設定する必要があります。[NSGroup の作成](#)を参照してください。
- 使用するモニターに応じて、アクティブまたはパッシブ健全性モニターが設定されていることを確認します。[アクティブ健全性モニターの構成](#)または[パッシブ健全性モニターの設定](#)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 [ロード バランサ (Load Balancer)] - [サーバ プール (Server Pools)] - [パッシブ健全性モニタ (Passive Health Monitors)] - [追加 (Add)] の順に選択します。
- 3 ロード バランサ プールの名前と説明を入力します。  
必要に応じて、サーバ プールで管理される接続を記述できます。
- 4 アルゴリズムでサーバ プールのロード バランシング方法を選択します。  
ロード バランシングのアルゴリズムは、メンバー間における受信接続の分散方法を制御します。アルゴリズムはサーバ プールで使用することも、サーバで直接使用することもできます。  
次の条件のいずれかを満たすサーバは、すべてのロード バランシング アルゴリズムでスキップされます。
  - 管理状態が「無効」に設定されている
  - 管理状態が「GRACEFUL\_DISABLED」に設定されていて、一致するパーシステンス エントリがない
  - アクティブまたはパッシブ健全性チェックの状態が「切断」になっている



## ■ サーバ プールの最大同時接続の上限に達した

オプション	説明
ROUND_ROBIN	受信クライアント要求は、要求を処理できる使用可能なサーバのリスト内で順番に振り分けられます。 サーバ プール メンバーに重みが設定されている場合でも、重みは無視されます。
WEIGHTED_ROUND_ROBIN	各サーバには、サーバの動作を、プール内の他のサーバに対して相対的に示す重み値が割り当てられています。この値により、サーバに送信されるクライアント要求の数が、プール内の他のサーバに対して相対的に決定されます。 このロード バランシング アルゴリズムは、使用可能なサーバ リソース間で負荷を均等に分散する処理に特化しています。
LEAST_CONNECTION	サーバの既存の接続数に基づいて、クライアント要求を複数のサーバに配信します。 新しい接続は、接続数が最も少ないサーバに送信されます。サーバ プール メンバーに重みが設定されている場合でも、重みは無視されます。
IP-HASH	送信元 IP アドレスのハッシュ、および実行されているすべてのサーバの重みの合計に基づいて、サーバを選択します。

### 5 [TCP 多重化] ボタンを切り替えて、このメニュー項目を有効にします。

TCP 多重化では、ロード バランサとサーバ間で同じ TCP 接続を使用することにより、複数のクライアント TCP 接続から複数のクライアント要求を送信することができます。

### 6 以降のクライアント要求を送信するために維持される、プールあたりの TCP 多重化接続の最大数を設定します。

## 7 送信元 NAT (SNAT) モードを選択します。

トポロジによっては、ロード バランサがサーバからクライアントに送信されるトラフィックを受信するために、SNAT が必要になることがあります。SNAT はサーバ プール単位で有効にできます。

モード	説明
透過モード	ロード バランサはサーバとの接続の確立時に、クライアントの IP アドレスおよびポート スプーフィングを使用します。 SNAT は不要です。
自動マップ モード	ロード バランサは、インターフェイスの IP アドレスおよび短期ポートを使用して、サーバ上に確立されたリスニング ポートの 1 つに元々接続されていたクライアントと引き続き通信します。 SNAT が必要です。 SNAT プロセスの実行後に 5-tuple (送信元 IP アドレス、送信元 ポート、宛先 IP アドレス、宛先ポート、および IP プロトコル) が一意である場合は、ポートのオーバーロードを有効にして、同じ SNAT IP アドレスおよびポートを複数の接続で使用できるようにします。 また、ポートのオーバーロード係数を設定して、複数の接続に対してポートを同時に使用できる最大回数を有効にすることもできます。
IP アドレス リスト モード	プール内のいずれかのサーバに接続しているときに SNAT に対して使用する 1.1.1.1-1.1.1.10 のような、単一の IP アドレス範囲を指定します。 デフォルトでは、設定されたすべての SNAT IP アドレスに 4000 ~ 64000 のポート範囲が使用されます。1000 ~ 4000 のポート範囲は、健全性チェックや、Linux アプリケーションからの接続用に予約されています。複数の IP アドレスが存在する場合は、ラウンド ロビン方式で選択されます。 SNAT プロセスの実行後に 5-tuple (送信元 IP アドレス、送信元 ポート、宛先 IP アドレス、宛先ポート、および IP プロトコル) が一意である場合は、ポートのオーバーロードを有効にして、同じ SNAT IP アドレスおよびポートを複数の接続で使用できるようにします。 また、ポートのオーバーロード係数を設定して、複数の接続に対してポートを同時に使用できる最大回数を有効にすることもできます。

## 8 サーバ プールのメンバーを選択します。

サーバ プールは、1 つまたは複数のプール メンバーで構成されています。各プール メンバーには、IP アドレスおよびポートが設定されています。

サーバ プールの各メンバーに、ロード バランシング アルゴリズムで使用される重みを設定することができます。重みは、特定のプール メンバーが処理できる負荷の量を、同じプール内の他のメンバーに対して相対的に示します。

オプション	説明
静的	[追加 (Add)] をクリックして、静的プール メンバーを追加します。 既存の静的プール メンバーのクローンを作成することもできます。
動的	ドロップダウン メニューから NSGroup を選択します。 サーバ プールのメンバーシップ基準は、このグループ内で定義されます。必要に応じて、グループの最大 IP アドレスのリストを定義することができます。

## 9 サーバ プールで常に維持する必要があるアクティブ メンバーの最小数を入力します。

## 10 ドロップダウン メニューで、サーバ プールに対してアクティブまたはパッシブ健全性モニターを選択します。

11 [終了 (Finish)] をクリックします。

## 仮想サーバ コンポーネントの設定

仮想サーバには、アプリケーション プロファイル、パーシステンス プロファイル、ロード バランサー ルールなど、設定可能なコンポーネントがあります。

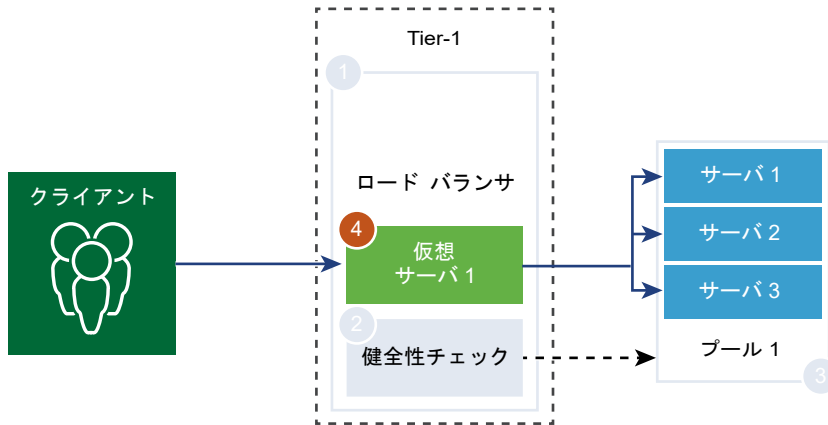
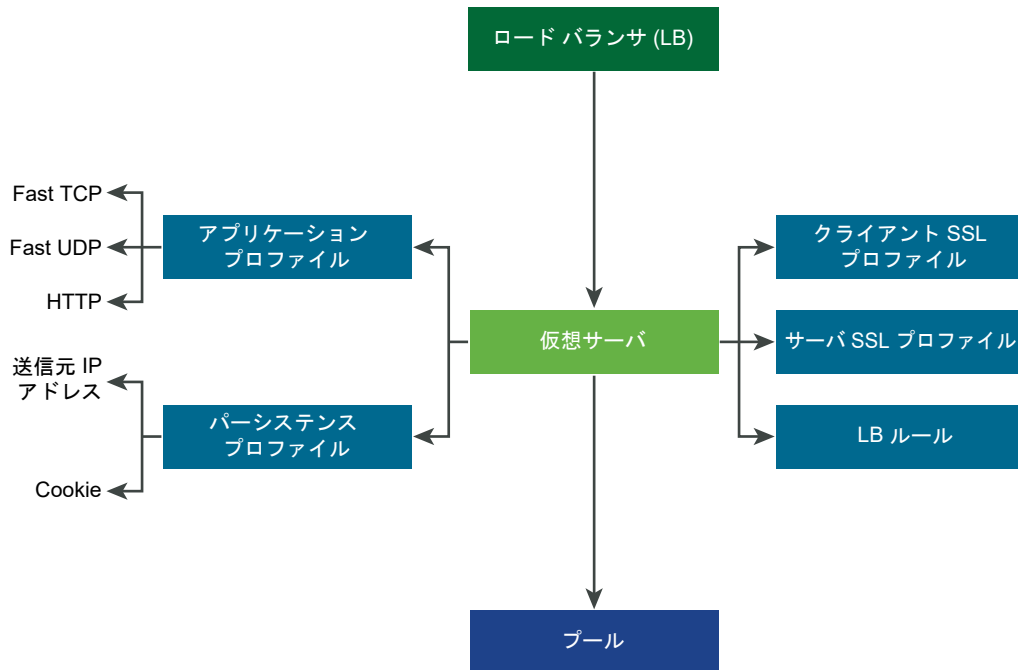


図 10-2. 仮想サーバ コンポーネント



## アプリケーション プロファイルの設定

アプリケーション プロファイルは、仮想サーバに関連付けらることで、ネットワーク トラフィックのロード バランシングを強化し、トラフィック管理タスクを簡素化します。

アプリケーション プロファイルは、それぞれ特定のタイプのネットワーク トラフィックの動作を定義します。関連付けられた仮想サーバは、アプリケーション プロファイルで指定された値に基づいてネットワーク トラフィックを処理します。Fast TCP、Fast UDP、HTTP の各アプリケーション プロファイルがサポートされています。

仮想サーバに関連付けられているアプリケーション プロファイルがない場合は、TCP アプリケーション プロファイルがデフォルトで使用されます。TCP および UDP アプリケーション プロファイルは、アプリケーションが TCP または UDP プロトコルで実行されていて、HTTP URL ロード バランシングなどのアプリケーション レベルのロード バランシングが不要な場合に使用されます。これらのプロファイルは、接続のミラーリングがサポートされる高パフォーマンスのレイヤー 4 ロード バランシングのみが必要な場合にも使用されます。

HTTP アプリケーション プロファイルは、HTTP と HTTPS の両方のアプリケーションで使用されます。これは、特定のサーバ プール メンバーに送信されたすべてのイメージ要求に対してロード バランシングを行う場合、またはプール メンバーから SSL をオフロードするために HTTPS を終了する場合など、ロード バランサがレイヤー 7 ベースでアクションを実行する際に使用されます。TCP アプリケーション プロファイルとは異なり、HTTP アプリケーション プロファイルは、サーバ プール メンバーを選択する前にクライアントの TCP 接続を終了します。

図 10-3. レイヤー 4 の TCP および UDP アプリケーション プロファイル

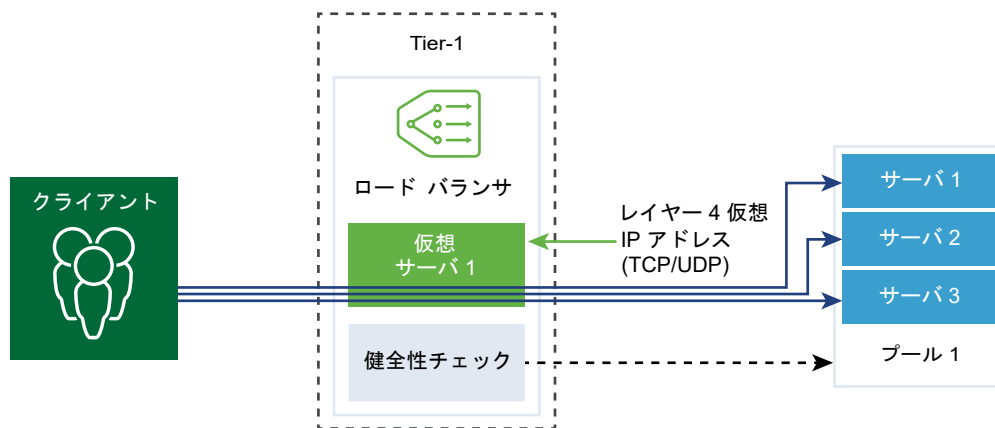
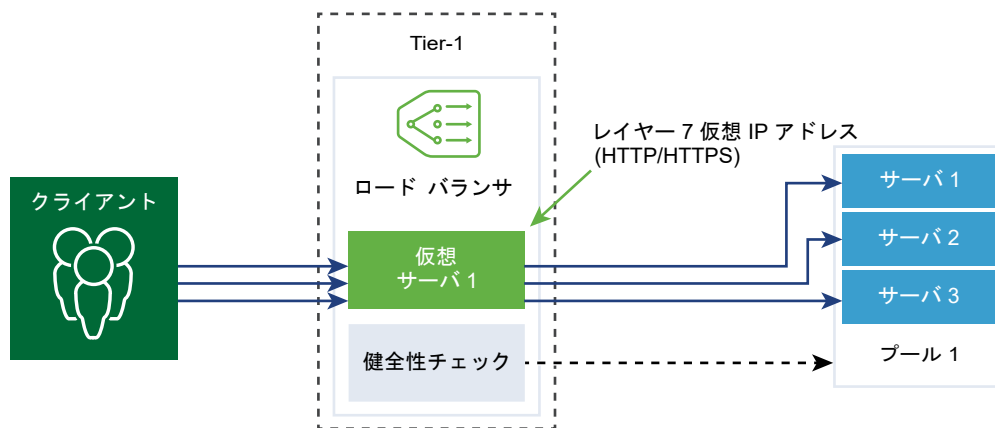


図 10-4. レイヤー 7 の HTTPS アプリケーション プロファイル



#### 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 [ロード バランサ (Load Balancer)] - [仮想サーバ (Virtual Servers)] - [アプリケーション プロファイル (Application Profiles)] の順に選択します。

### 3 Fast TCP アプリケーション プロファイルを作成します。

- a ドロップダウン メニューから [追加] - [Fast TCP プロファイル] の順に選択します。
- b Fast TCP アプリケーション プロファイルの名前と説明を入力します。
- c アプリケーション プロファイルの詳細を入力します。

FAST TCP のデフォルトのプロファイル設定を受け入れることもできます。

オプション	説明
接続アイドル タイムアウト	TCP 接続が確立された後、サーバがアイドルのまま接続が維持される時間（秒数）を入力します。  アプリケーションが接続を終了する前にロード バランサが接続を終了するのを避けるために、実際のアプリケーション アイドル時間に数秒を加算した値をアイドル時間として設定します。
接続終了タイムアウト	FIN と RST の両方を送信した TCP 接続が、アプリケーションの接続を維持する時間を入力します。  接続にかかる時間を短縮するには、終了タイムアウトを短く設定する必要があります。
HA フローのミラーリング	ボタンの切り替えにより、関連付けられている仮想サーバへのすべてのフローを HA スタンバイ ノードにミラーリングします。

- d [OK] をクリックします。

### 4 Fast UDP アプリケーション プロファイルを作成します。

UDP のデフォルトのプロファイル設定を受け入れることもできます。

- a ドロップダウン メニューから [追加] - [Fast UDP プロファイル] の順に選択します。
- b Fast UDP アプリケーション プロファイルの名前と説明を入力します。
- c アプリケーション プロファイルの詳細を入力します。

オプション	説明
アイドルタイムアウト	UDP 接続が確立された後、サーバがアイドルのまま接続が維持される時間（秒数）を入力します。  UDP は、コネクションレス プロトコルです。ロード バランシング処理では、同じフローと識別される UDP パケット、つまりアイドル タイムアウト期間内に受信された送信元と宛先の IP アドレス、またはポートと IP プロトコルなどが同じ UDP パケットは、すべて同じ接続に属すと見なされ、同じサーバに送信されます。  アイドル タイムアウト期間内にパケットが受信されなかった場合は、フロー署名と選択されたサーバ間で関連付けられた接続は切断されます。
HA フローのミラーリング	ボタンの切り替えにより、関連付けられている仮想サーバへのすべてのフローを HA スタンバイ ノードにミラーリングします。

- d [OK] をクリックします。

### 5 HTTP アプリケーション プロファイルを作成します。

HTTP のデフォルトのプロファイル設定を受け入れることもできます。

HTTP アプリケーション プロファイルは、HTTP と HTTPS の両方のアプリケーションに使用されます。

- a ドロップダウン メニューから [追加] - [Fast HTTP プロファイル] の順に選択します。
- b HTTP アプリケーション プロファイルの名前と説明を入力します。

## C アプリケーション プロファイルの詳細を入力します。

オプション	説明
リダイレクト	<ul style="list-style-type: none"> <li>■ [なし] - Web サイトが一時的に停止しているとき、ユーザーにはページが見つからないというエラー メッセージが表示されます。</li> <li>■ [HTTP リダイレクト] - Web サイトが一時的に停止しているとき、または移動した場合、その仮想サーバ宛の受信された要求は、ここで指定した URL に一時的にリダイレクトできます。静的リダイレクトのみがサポートされています。</li> </ul> <p>たとえば、[HTTP リダイレクト] を <code>http://sitedown.abc.com/sorry.html</code> に設定すると、元の Web サイトが停止しているとき、実際の要求が <code>http://original_app.site.com/home.html</code> であっても <code>http://original_app.site.com/somepage.html</code> であっても、受信された要求は指定された URL にリダイレクトされます。</p> <ul style="list-style-type: none"> <li>■ [HTTP から HTTPS にリダイレクト] - 特定のセキュアなアプリケーションでは SSL による通信が必要ですが、非 SSL 接続を拒否するのではなく、代わりにクライアント要求が SSL を使用するようにリダイレクトできます。[HTTP から HTTPS にリダイレクト] に設定すると、ホストと URI の両方のパスを保持して、クライアント要求が SSL を使用するようにリダイレクトできます。</li> </ul> <p>[HTTP から HTTPS にリダイレクト] に設定する場合、HTTPS 仮想サーバにポート 443 が必要です。また、同じロード バランサに同じ仮想サーバ IP アドレスを設定する必要があります。</p> <p>たとえば、<code>http://app.com/path/page.html</code> へのクライアント要求は <code>https://app.com/path/page.html</code> にリダイレクトされます。たとえば <code>https://secure.app.com/path/page.html</code> にリダイレクトする際にホスト名または URI を変更する必要がある場合は、ロード バランシング ルールを使用する必要があります。</p>
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> <li>■ [挿入] - 受信された要求に XFF HTTP ヘッダーがない場合は、ロード バランサがクライアントの IP アドレスを持つ新しい XFF ヘッダーを挿入します。</li> <li>■ [置き換え] - 受信された要求に XFF HTTP ヘッダーがすでに存在する場合、ロード バランサはそのヘッダーを置き換えることができます。</li> </ul> <p>Web サーバは、処理するすべての要求を要求元のクライアント IP アドレスと共に記録します。これらのログは、デバッグと分析のために使用されます。ロード バランサに SNAT が必要な展開トポロジでは、サーバはクライアントの SNAT IP アドレスを使用しますが、そうするとログ作成の目的が達成できなくなります。</p> <p>この問題を回避するには、元のクライアント IP アドレスを持つ XFF HTTP ヘッダーを挿入するようにロード バランサを設定します。接続の送信元 IP アドレスの代わりに、この IP アドレスを XFF ヘッダーに記録するようにサーバを設定します。</p>
接続アイドル タイムアウト	HTTP アプリケーションがアイドル状態を維持できる時間（秒数）を入力します。この値は、TCP アプリケーション プロファイルで設定する TCP ソケット設定の代わりに使用されます。
要求ヘッダー サイズ	HTTP 要求ヘッダーを格納するために使用されるバッファの最大サイズ（バイト数）を指定します。
NTLM 認証	<p>ボタンの切り替えにより、ロード バランサの TCP 多重化をオフにし、HTTP キープアライブを有効にします。</p> <p>NTLM は、HTTP 上で使用可能な認証プロトコルです。NTLM 認証でロード バランシングを行うには、NTLM ベースのアプリケーションをホストしているサーバ プールで TCP 多重化を無効にする必要があります。無効にしないと、特定のクライアントの資格情報で確立されたサーバ側の接続が、別のクライアントの要求を処理するために使用される可能性があります。</p>

オプション	説明
	<p>NTLM がプロファイルで有効になっており、仮想サーバに関連付けられている場合、サーバプールで TCP 多重化が有効になっていると、NTLM が優先されます。その仮想サーバに対して、TCP 多重化は実行されません。ただし、同じプールが NTLM でない別の仮想サーバに関連付けられている場合は、TCP 多重化をその仮想サーバへの接続に使用できます。</p> <p>クライアントが HTTP/1.0 を使用している場合、ロード バランサは HTTP/1.1 プロトコルにアップデートし、HTTP キープアライブが設定されます。同じクライアント側 TCP 接続で受信されたすべての HTTP 要求は、再認証が不要になるように、1 つの TCP 接続を介して同じサーバに送信されます。</p>

d [OK] をクリックします。

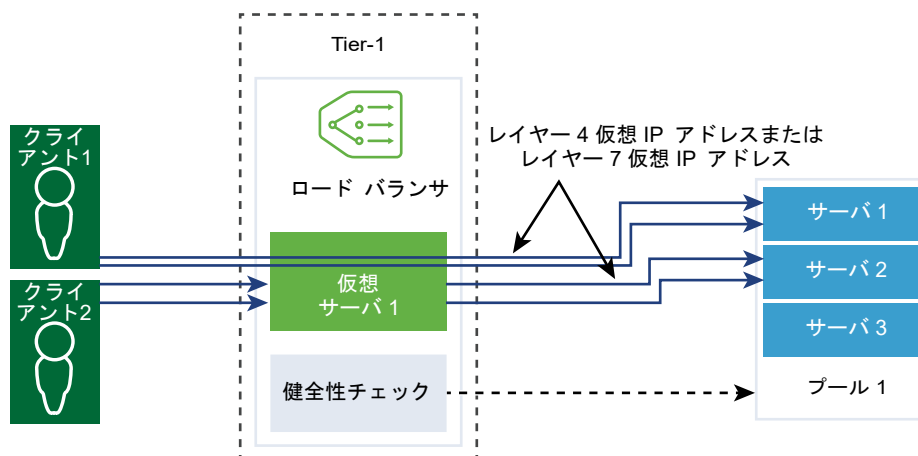
## パーシステンス プロファイルの設定

ステートフル アプリケーションの安定性を確保するため、ロード バランサには、関連するすべての接続を同じサーバに転送するパーシステンス機能が実装されています。アプリケーションによるさまざまな種類のニーズに対応できるように、さまざまな種類のパーシステンス機能がサポートされています。

一部のアプリケーションでは、サーバの状態（ショッピング カートなど）が維持されます。これらの状態はクライアントごとに、IP アドレス ベースか、HTTP セッション ベースで維持されます。アプリケーションは、同じクライアントや HTTP セッションからの接続を処理する際に、この状態を参照または変更する場合があります。

送信元 IP アドレス パーシステンス プロファイルは、送信元の IP アドレスに基づいてセッションを追跡します。送信元アドレス ベースのパーシステンス が有効になっている仮想サーバへクライアントが接続を要求すると、ロード バランサは、そのクライアントに以前接続したかどうかを確認し、接続したことがあれば、そのクライアントを同じサーバに返します。以前に接続したことがない場合は、プールのロード バランシング アルゴリズムに基づいてサーバプール メンバーを選択できます。送信元 IP アドレス パーシステンス プロファイルは、レイヤー 4 およびレイヤー 7 の仮想サーバによって使用されます。

Cookie によるパーシステンス プロファイルは、クライアントが特定のサイトに初めてアクセスする際に、一意の Cookie を挿入してセッションを識別します。以降の要求では、クライアントから HTTP Cookie が転送され、ロード バランサはその情報を使用して Cookie によるパーシステンスを行います。Cookie パーシステンス プロファイルを使用できるのはレイヤー 7 の仮想サーバのみです。





## 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 [ロード バランサ (Load Balancer)] - [仮想サーバ (Virtual Servers)] - [パーシステンス プロファイル (Persistence Profiles)] の順に選択します。
- 3 送信元 IP アドレス パーシステンス プロファイルを作成します。
  - a ドロップダウン メニューから [追加 (Add)] - [送信元 IP アドレス パーシステンス (Source IP Persistence)] の順に選択します。
  - b 送信元 IP アドレス パーシステンス プロファイルの名前と説明を入力します。
  - c パーシステンス プロファイルの詳細を設定します。

送信元 IP アドレス プロファイルのデフォルト設定をそのまま使用することもできます。

オプション	説明
パーシステンスを共有	<p>切り替えボタンを使用して、このプロファイルに関連付けられているすべての仮想サーバでパーシステンス テーブルを共有するかどうかを指定します。</p> <p>送信元 IP アドレス パーシステンス プロファイルが特定の仮想サーバに関連付けられていて、そのプロファイルでパーシステンスの共有が有効になっていない場合、そのプロファイルに関連付けられている各仮想サーバでは、プライベートなパーシステンス テーブルが保持されます。</p>
パーシステンス エントリのタイムアウト	<p>パーシステンス期間を秒単位で入力します。</p> <p>ロード バランサのパーシステンス テーブルには、同じサーバにクライアント要求が転送されたことを記録したエントリが維持されます。</p> <ul style="list-style-type: none"> <li>■ タイムアウト期間内に同じクライアントから新しい接続要求を受信しなかった場合、パーシステンスのエントリは期限切れになり、削除されます。</li> <li>■ タイムアウト期間内に同じクライアントからの新しい接続要求を受信した場合、タイマーがリセットされ、クライアント要求がスティッキー プール メンバーに送信されます。</li> </ul> <p>タイムアウト期間が経過すると、ロード バランシング アルゴリズムで割り当てられたサーバに新しい接続要求が送信されます。L7 ロード バランシングの TCP で、送信元 IP アドレス パーシステンスを使用するシナリオでは、一定期間に新規の TCP 接続がない場合、接続が継続中であってもパーシステンス エントリがタイムアウトします。</p>
HA パーシステンス ミラーリング	<p>切り替えボタンを使用して、パーシステンス エントリを HA ピアに同期するかどうかを指定します。</p>
テーブルがフルになるとエントリを消去	<p>パーシステンス テーブルがいっぱいになったときにエントリを消去します。</p> <p>タイムアウト値が大きい場合、トラフィックが大量に発生すると、パーシステンス テーブルがすぐにいっぱいになる可能性があります。パーシステンス テーブルがいっぱいになると、新しいエントリを受け入れるため、最も古いエントリが削除されます。</p>

- d [OK] をクリックします。
- 4 Cookie パーシステンス プロファイルを作成します。
  - a ドロップダウン メニューから [追加 (Add)] - [Cookie パーシステンス (Cookie Persistence)] の順に選択します。
  - b Cookie パーシステンス プロファイルの名前と説明を入力します。

- c [パーシステンスを共有 (Share Persistence)] 切り替えボタンを使用して、同じプール メンバーに関連付けられている複数の仮想サーバの間でパーシステンスを共有するかどうかを指定します。

Cookie パーシステンス プロファイルでは、`<name>.<profile-id>.<pool-id>` という形式を持つ Cookie が挿入されます。

Cookie パーシステンス プロファイルが特定の仮想サーバに関連付けられていて、そのプロファイルでパーシステンスの共有が有効になっていない場合は、仮想サーバごとに Cookie パーシステンスがプライベートに使用され、プール メンバーによって修飾されます。ロード バランサによって、`<name>.<virtual_server_id>.<pool_id>` という形式を持つ Cookie が挿入されます。

- d [次へ (Next)] をクリックします。
- e パーシステンス プロファイルの詳細を設定します。

オプション	説明
Cookie モード	ドロップダウン メニューからモードを選択します。 <ul style="list-style-type: none"> <li>■ [挿入] - セッションを識別する一意の Cookie を追加します。</li> <li>■ [ブリフィックス] - 既存の HTTP Cookie 情報に新しい情報を追加します。</li> <li>■ [書き換え] - 既存の HTTP Cookie 情報を書き換えます。</li> </ul>
Cookie 名	Cookie 名を入力します。
Cookie ドメイン	ドメイン名を入力します。 HTTP Cookie ドメインは、挿入モードの場合にのみ設定できます。
Cookie のパス	Cookie の URL パスを入力します。 HTTP Cookie のパスは、挿入モードの場合にのみ設定できます。
Cookie の暗号化	Cookie サーバの IP アドレスとポート情報を暗号化します。 暗号化を無効にするには、この切り替えボタンをオフにします。暗号化を無効にすると、Cookie サーバの IP アドレスとポート情報はプレーン テキストになります。
Cookie のフォールバック	Cookie で無効状態またはダウン状態のサーバが参照されている場合、クライアントの要求を処理する新しいサーバを選択します。 Cookie で無効状態またはダウン状態のサーバが参照されている場合、クライアントの要求を却下するには、この切り替えボタンをオフにします。

- f Cookie の有効期限の詳細を設定します。

オプション	説明
Cookie の時間タイプ	ドロップダウン メニューから Cookie の時間タイプを選択します。 セッション Cookie タイプを選択した場合も、パーシステンス Cookie タイプを選択した場合も、ブラウザが閉じられると Cookie は期限切れになります。
最大アイドル時間	Cookie を期限切れにするまでの最大アイドル時間を秒単位で入力します。
Cookie の最大維持期間	セッション Cookie タイプを選択した場合に、Cookie を維持する期間を秒単位で入力します。

- g [終了 (Finish)] をクリックします。

## SSL プロファイルの設定

SSL プロファイルは、暗号リストなど、アプリケーションに依存しない SSL プロパティを設定し、それらのリストを複数のアプリケーション間で再利用します。ロード バランサがクライアントとサーバの両方として動作している場合は SSL プロパティが異なるため、クライアント側とサーバ側で異なる SSL プロファイルがサポートされます。

**注：** SSL プロファイルは NSX-T 2.1 リリースではサポートされていません。

クライアント側 SSL プロファイルは、SSL サーバとして動作し、クライアント SSL 接続を終端するロード バランサを参照します。サーバ側 SSL プロファイルは、クライアントとして動作し、サーバへの接続を確立するロード バランサを参照します。

暗号リストは、クライアント側 SSL プロファイルでも、サーバ側 SSL プロファイルでも指定できます。

SSL セッションのキャッシュを有効にすると、以前にネゴシエートされたセキュリティ パラメータを SSL クライアントとサーバで再利用できるようになり、負荷の高いパブリック キー処理を SSL ハンドシェイク中に回避できるようになります。デフォルトでは、SSL セッションのキャッシュはクライアント側とサーバ側の両方で無効になっています。

以前にネゴシエートされたセッション パラメータを SSL クライアントとサーバで再利用する別のメカニズムとしては、SSL セッション チケットがあります。SSL セッション チケットの場合、クライアントとサーバはハンドシェイクの交換中にお互いが SSL セッション チケットをサポートしているかどうかをネゴシエートします。チケットが両方でサポートされている場合、サーバはクライアントに SSL チケットを送信することができます。この SSL チケットには暗号化された SSL セッション パラメータが含まれています。クライアントは後続の接続でそのチケットを使用することによって、セッションを再利用します。SSL セッション チケットはクライアント側で有効になり、サーバ側では無効になります。

図 10-5. SSL オフロード

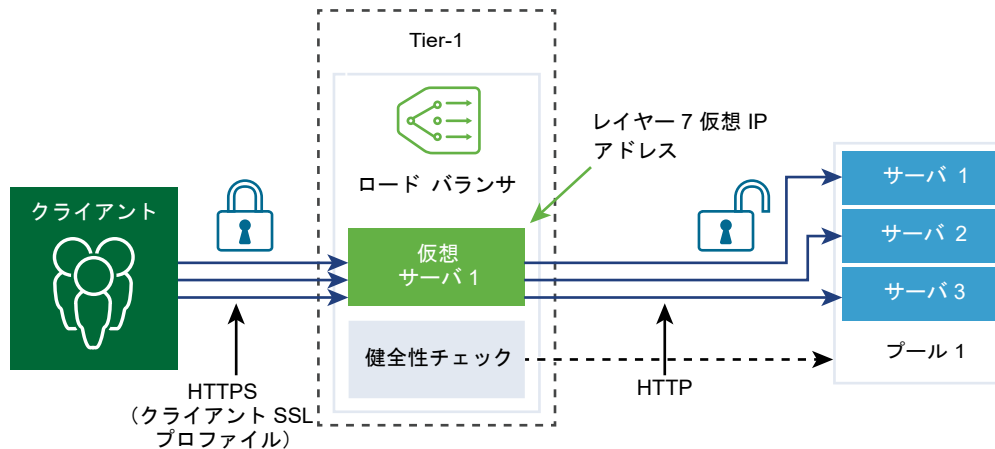
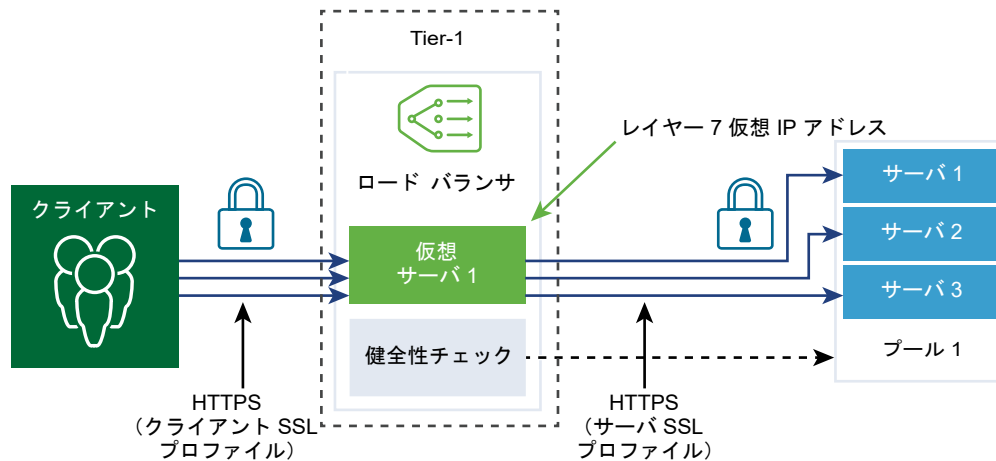


図 10-6. エンド ツー エンドの SSL



## 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 [ロード バランサ (Load Balancer)] - [仮想サーバ (Virtual Servers)] - [SSL プロファイル (SSL Profiles)] の順に選択します。
- 3 クライアント SSL プロファイルを作成します。
  - a ドロップダウン メニューから [追加 (Add)] - [クライアント側 SSL (Client Side SSL)] の順に選択します。
  - b クライアント SSL プロファイルの名前と説明を入力します。
  - c クライアント SSL プロファイルに含める SSL 暗号を選択します。
  - d 矢印をクリックして [選択済み] セクションに暗号を移動します。
  - e [プロトコルとセッション (Protocols and Sessions)] タブをクリックします。
  - f クライアント SSL プロファイルに含める SSL プロトコルを選択します。

SSL プロトコルバージョン TLS1.1 と TLS1.2 はデフォルトで有効になっています。TLS1.0 もサポートされていますが、デフォルトでは無効になっています。

  - g 矢印をクリックして [選択済み] セクションにプロトコルを移動します。

- h SSL プロトコルの詳細を設定します。

SSL プロファイルのデフォルト設定をそのまま使用することもできます。

オプション	説明
セッションのキャッシュ	SSL セッションのキャッシュを有効にすると、以前にネゴシエートされたセキュリティ パラメータを SSL クライアントとサーバで再利用できるようになり、負荷の高いパブリック キー処理を SSL ハンドシェイク中に回避できるようになります。
セッション キャッシュ エントリのタイムアウト	キャッシュのタイムアウトを秒単位で入力します。このキャッシュ期間が過ぎるまでは、SSL セッション パラメータを再利用できます。
サーバの暗号を優先	切り替えボタンを使用して、サーバでサポートできる暗号のリストの中で最初にある暗号を使用するかどうかを指定します。  SSL ハンドシェイクの際、クライアントは、サポートされている暗号の順序付きリストをサーバに送信します。

- i [OK] をクリックします。

#### 4 サーバ SSL プロファイルを作成します。

- ドロップダウン メニューから [追加 (Add)] - [サーバ側 SSL (Server Side SSL)] の順に選択します。
- サーバ SSL プロファイルの名前と説明を入力します。
- サーバ SSL プロファイルに含める SSL 暗号を選択します。
- 矢印をクリックして [選択済み] セクションに暗号を移動します。
- [プロトコルとセッション (Protocols and Sessions)] タブをクリックします。
- サーバ SSL プロファイルに含める SSL プロトコルを選択します。

SSL プロトコル バージョン TLS1.1 と TLS1.2 はデフォルトで有効になっています。TLS1.0 もサポートされていますが、デフォルトでは無効になっています。

- 矢印をクリックして [選択済み] セクションにプロトコルを移動します。
- デフォルトのセッション キャッシュ設定をそのまま受け入れます。

SSL セッションのキャッシュを有効にすると、以前にネゴシエートされたセキュリティ パラメータを SSL クライアントとサーバで再利用できるようになり、負荷の高いパブリック キー処理を SSL ハンドシェイク中に回避できるようになります。

- i [OK] をクリックします。

## レイヤー 4 仮想サーバの設定

仮想サーバは、すべてのクライアント接続を受信し、複数のサーバに分散します。仮想サーバには、IP アドレス、ポート、およびプロトコルが 1 つずつ設定されます。レイヤー 4 仮想サーバの場合は、1 つの TCP または UDP ポートでなくポート範囲のリストを指定できるため、動的ポートによって複雑なプロトコルをサポートできます。

レイヤー 4 仮想サーバは、デフォルト プールとも呼ばれるプライマリ サーバ プールに関連付ける必要があります。

仮想サーバのステータスが無効になっている場合、仮想サーバに新規接続を試みると、TCP 接続では TCP RST の送信、UDP では ICMP エラー メッセージの送信によってすべて拒否されます。新しい接続に対応するパーシステンス エントリがある場合でも拒否されます。アクティブな接続は、引き続き処理されます。仮想サーバが削除されるか、仮想サーバとロード バランサの関連付けが解除されると、その仮想サーバへのアクティブな接続に失敗します。

#### 前提条件

- アプリケーション プロファイルが使用できることを確認します。[アプリケーション プロファイルの設定](#)を参照してください。
- パーシステンス プロファイルが使用できることを確認します。[パーシステンス プロファイルの設定](#)を参照してください。
- クライアントとサーバの SSL プロファイルが使用できることを確認します。[SSL プロファイルの設定](#)を参照してください。
- サーバ プールが使用できることを確認します。[ロード バランシング用サーバ プールの追加](#)を参照してください。

#### 手順

##### 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 [ロード バランサ (Load Balancer)] - [仮想サーバ (Virtual Servers)] - [追加 (Add)] の順に選択します。
- 3 レイヤー 4 仮想サーバの名前と説明を入力します。
- 4 ドロップダウン メニューからレイヤー 4 のプロトコルを選択します。

レイヤー 4 仮想サーバは、Fast TCP と Fast UDP のいずれかのプロトコルをサポートしますが、その両方をサポートすることはできません。DNS などの場合に、同じ IP アドレスとポートで Fast TCP プロトコルと Fast UDP プロトコルをサポートするには、各プロトコルに対応する仮想サーバをそれぞれ作成する必要があります。

プロトコル タイプに基づいて、既存のアプリケーション プロファイルが自動的に適用されます。

- 5 [次へ (Next)] をクリックします。
- 6 仮想サーバの IP アドレスとポート番号を入力します。  
仮想サーバのポート番号またはポートの範囲を入力できます。

## 7 詳細プロパティの詳細を入力します。

オプション	説明
最大同時接続数	同じロード バランサでホストされている他のアプリケーションのリソースをすべて消費することがないように、仮想サーバに許される同時接続の最大数を設定します。
新規接続の最大速度	仮想サーバがリソースをすべて消費することがないように、サーバ プール メンバーに対して新規接続の最大速度を設定します。
デフォルトのプール メンバー ポート	仮想サーバのプール メンバー ポートが定義されていない場合は、デフォルトのプール メンバー ポートを入力します。  たとえば、仮想サーバに 2000～2999 のポート範囲を定義し、デフォルトのプール メンバー ポート範囲を 8000～8999 と設定した場合、仮想サーバのポート 2500 への受信クライアント 接続は、ターゲット ポートが 8500 に設定された状態でプール メンバーに送信されます。

## 8 ドロップダウン メニューから既存のサーバ プールを選択します。

サーバ プールは、プール メンバーとも呼ばれる 1 台または複数のサーバで構成されます。これらは同じように設定され、同じアプリケーションを実行します。

## 9 [次へ (Next)] をクリックします。

## 10 ドロップダウン メニューから既存のパースিসテンス プロファイルを選択します。

仮想サーバでパースিসテンス プロファイルを有効にすると、関連する複数のクライアント接続を同じサーバに送信できます。

## 11 [終了 (Finish)] をクリックします。

## レイヤー 7 仮想サーバの設定

仮想サーバは、すべてのクライアント接続を受信し、複数のサーバに分散します。仮想サーバには、IP アドレス、ポート、および TCP プロトコルが設定されます。

ロード バランサ ルールは、レイヤー 7 仮想サーバと HTTP アプリケーション プロファイルの組み合わせでのみサポートされます。ロード バランサ サービスが異なれば、異なるロード バランサ ルールを使用できます。

各ロード バランサ ルールは、1 つまたは複数の一致条件と 1 つまたは複数のアクションで構成されます。一致条件が指定されないロード バランサ ルールは常に一致するため、デフォルトのルールを定義するために使用されます。複数の一致条件が指定された場合、ロード バランサ ルールに一致したとみなすのは、すべての条件に一致させる場合か、いずれか 1 つの条件に一致させる場合かは、一致条件に関する指針に従って決定されます。

各ロード バランサ ルールは、HTTP 要求の書き換え、HTTP 要求の転送、HTTP 応答の書き換えというロード バランシング処理の特定のフェーズに実装されます。すべての一致条件とアクションが各フェーズに適用されるわけではありません。

仮想サーバのステータスが無効になっている場合、仮想サーバに新規接続を試みると、TCP 接続では TCP RST の送信、UDP では ICMP エラー メッセージの送信によってすべて拒否されます。新しい接続に対応するパースিসテンス エントリがある場合でも拒否されます。アクティブな接続は、引き続き処理されます。仮想サーバが削除されるか、仮想サーバとロード バランサの関連付けが解除されると、その仮想サーバへのアクティブな接続に失敗します。

## 前提条件

- アプリケーション プロファイルが使用できることを確認します。[アプリケーション プロファイルの設定](#)を参照してください。
- パーシステンス プロファイルが使用できることを確認します。[パーシステンス プロファイルの設定](#)を参照してください。
- クライアントとサーバの SSL プロファイルが使用できることを確認します。[SSL プロファイルの設定](#)を参照してください。
- サーバ プールが使用できることを確認します。[ロード バランシング用サーバ プールの追加](#)を参照してください。
- 認証局とクライアントの証明書が使用できることを確認します。[証明書署名要求ファイルの作成](#)を参照してください。
- 証明書失効リスト (CRL) が使用できることを確認します。[証明書失効リストのインポート](#)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 [ロード バランサ (Load Balancer)] - [仮想サーバ (Virtual Servers)] - [追加 (Add)] の順に選択します。
- 3 レイヤー 7 仮想サーバの名前と説明を入力します。
- 4 レイヤー 7 のメニュー項目を選択します。  
レイヤー 7 仮想サーバは、HTTP プロトコルと HTTPS プロトコルをサポートします。  
既存の HTTP アプリケーション プロファイルが自動的に取り込まれます。
- 5 (オプション) [次へ (Next)] をクリックして、サーバ プールとロード バランシング プロファイルを設定します。
- 6 [終了 (Finish)] をクリックします。

## レイヤー 7 仮想サーバ プールおよびルールの設定

レイヤー 7 仮想サーバでは、ロード バランサ ルールを設定し、一致またはアクションのルールを使用してロード バランシングの動作をカスタマイズすることもできます。

## 前提条件

レイヤー 7 仮想サーバが使用できることを確認します。[レイヤー 7 仮想サーバの設定](#)を参照してください。

## 手順

- 1 レイヤー 7 仮想サーバを開きます。
- 2 [サーバ プールとルール] ページに進みます。
- 3 仮想サーバの IP アドレスとポート番号を入力します。  
仮想サーバのポート番号またはポートの範囲を入力できます。



#### 4 詳細プロパティの詳細を入力します。

オプション	説明
最大同時接続数	同じロード バランサでホストされている他のアプリケーションのリソースをすべて消費することがないように、仮想サーバに許される同時接続の最大数を設定します。
新規接続の最大速度	仮想サーバがリソースをすべて消費することがないように、サーバ プール メンバーに対して新規接続の最大速度を設定します。
デフォルトのプール メンバー ポート	仮想サーバのプール メンバー ポートが定義されていない場合は、デフォルトのプール メンバー ポートを入力します。  たとえば、仮想サーバに 2000～2999 のポート範囲を定義し、デフォルトのプール メンバー ポート範囲を 8000～8999 と設定した場合、仮想サーバのポート 2500 への受信クライアント 接続は、ターゲット ポートが 8500 に設定された状態でプール メンバーに送信されます。

#### 5 (オプション) ドロップダウン メニューから既存のデフォルト サーバ プールを選択します。

サーバ プールは、プール メンバーと呼ばれる 1 台または複数のサーバで構成されます。これらは同じように設定され、同じアプリケーションを実行します。

#### 6 [追加 (Add)] をクリックして、HTTP 要求の書き換えフェーズにロード バランサ ルールを設定します。

サポートされている一致のタイプは、REGEX、STARTS\_WITH、ENDS\_WITH などと、反転オプションです。

サポートされている一致条件	説明
HTTP 要求メソッド	HTTP 要求メソッドに一致します。 http_request.method : 一致する値
HTTP 要求 URI	クエリの引数を除いて、HTTP 要求 URI と一致します。 http_request.uri : 一致する値
HTTP 要求の URI 引数	HTTP 要求の URI クエリ引数と一致します。 http_request.uri_arguments : 一致する値
HTTP 要求バージョン	HTTP 要求のバージョンと一致します。 http_request.version : 一致する値
HTTP 要求ヘッダー	任意の HTTP 要求ヘッダーと一致します。 http_request.header_name : 一致するヘッダー名 http_request.header_value : 一致する値
HTTP 要求ペイロード	HTTP 要求の本文の内容に一致します。 http_request.body_value : 一致する値

サポートされている一致条件	説明
TCP ヘッダー フィールド	TCP の送信元ポートまたは宛先ポートと一致します。 tcp_header.source_port : 一致する送信元ポート tcp_header.destination_port : 一致する宛先ポート
IP ヘッダー フィールド	送信元またはターゲットの IP アドレスに一致します。 ip_header.source_address : 一致する送信元の IP アドレス ip_header.destination_address : 一致する宛先の IP アドレス

アクション	説明
HTTP 要求 URI の書き換え	URI を変更します。 http_request.uri : 書き込む URI (クエリ引数なし) http_request.uri_args : 書き込む URI クエリ引数
HTTP 要求ヘッダーの書き換え	HTTP ヘッダーの値を変更します。 http_request.header_name : ヘッダー名 http_request.header_value : 書き込む値

## 7 [追加 (Add)] をクリックして、HTTP 要求の転送にロード バランサ ルールを設定します。

一致するすべての値には、正規表現を使用できます。

サポートされている一致条件	説明
HTTP 要求メソッド	HTTP 要求メソッドに一致します。 http_request.method : 一致する値
HTTP 要求 URI	HTTP 要求 URI と一致します。 http_request.uri : 一致する値
HTTP 要求の URI 引数	HTTP 要求の URI クエリ引数と一致します。 http_request.uri_args : 一致する値
HTTP 要求バージョン	HTTP 要求のバージョンと一致します。 http_request.version : 一致する値
HTTP 要求ヘッダー	任意の HTTP 要求ヘッダーと一致します。 http_request.header_name : 一致するヘッダー名 http_request.header_value : 一致する値
HTTP 要求ペイロード	HTTP 要求の本文の内容に一致します。 http_request.body_value : 一致する値

サポートされている一致条件	説明
TCP ヘッダー フィールド	TCP の送信元ポートまたは宛先ポートと一致します。 tcp_header.source_port : 一致する送信元ポート tcp_header.destination_port : 一致する宛先ポート
IP ヘッダー フィールド	送信元の IP アドレスと一致します。 ip_header.source_address : 一致する送信元の IP アドレス
アクション	説明
却下	たとえば、ステータスを 5xx に設定することによって要求を却下します。 http_forward.reply_status - 却下するために使用する HTTP ステータス コード http_forward.reply_message - HTTP 却下メッセージ
リダイレクト	要求をリダイレクトします。ステータス コードは、3xx に設定する必要があります。 http_forward.redirect_status : リダイレクトの HTTP ステータス コード http_forward.redirect_url : HTTP リダイレクト URL
プールの選択	要求に特定のサーバ プールを適用します。指定されたプール メンバーの設定済みアルゴリズム（予測）を使用して、サーバ プール内のサーバを選択します。 http_forward.select_pool : サーバ プールの UUID

- 8 [追加 (Add)] をクリックして、HTTP 応答の書き換えにロード バランサ ルールを設定します。

一致するすべての値には、正規表現を使用できます。

サポートされている一致条件	説明
HTTP 応答ヘッダー	任意の HTTP 応答ヘッダーに一致します。 http_response.header_name : 一致するヘッダー名 http_response.header_value : 一致する値
アクション	説明
HTTP 応答ヘッダーの書き換え	HTTP 応答ヘッダーの値を変更します。 http_response.header_name : ヘッダー名 http_response.header_value : 書き込む値

- 9 [次へ (Next)] をクリックします。

- 10 [パーシステンス] ボタンを切り替えてプロファイルを有効にします。

パーシステンス プロファイルでは、関連する複数のクライアント接続を同じサーバに送信できます。

- 11 送信元 IP アドレスによるパーシステンス プロファイルまたは Cookie によるパーシステンス プロファイルを選択します。
- 12 ドロップダウン メニューから既存のパーシステンス プロファイルを選択します。
- 13 (オプション) [次へ (Next)] をクリックして、ロード バランシング プロファイルを設定します。
- 14 [終了 (Finish)] をクリックします。

## レイヤー 7 仮想サーバのロード バランシング プロファイルの設定

レイヤー 7 仮想サーバでは、ロード バランサのパーシステンス、クライアント側 SSL、サーバ側 SSL の各プロファイルも設定できます。

仮想サーバでクライアント側 SSL プロファイル バインドが設定されており、サーバ側 SSL プロファイル バインドは設定されていない場合、仮想サーバは SSL 終了モードで動作し、クライアントとは暗号化を使用した接続、サーバとの接続はプレーン テキスト接続となります。クライアント側とサーバ側の両方の SSL プロファイル バインドが設定されている場合、仮想サーバは SSL プロキシ モードで動作し、クライアントとサーバの両方に暗号化を使用して接続されます。

現時点では、クライアント側 SSL プロファイル バインドを関連付けずにサーバ側 SSL プロファイル バインドを関連付けることはサポートされません。クライアント側とサーバ側の SSL プロファイル バインドが仮想サーバに関連付けられておらず、アプリケーションが SSL ベースの場合、仮想サーバは SSL 非対応モードで動作します。この場合、仮想サーバはレイヤー 4 で設定する必要があります。たとえば、仮想サーバを Fast TCP プロファイルに関連付けることができます。

### 前提条件

レイヤー 7 仮想サーバが使用できることを確認します。 [レイヤー 7 仮想サーバの設定](#)を参照してください。

### 手順

- 1 レイヤー 7 仮想サーバを開きます。
- 2 [ロード バランシング プロファイル] ページに進みます。
- 3 [パーシステンス] ボタンを切り替えてプロファイルを有効にします。  
パーシステンス プロファイルでは、関連する複数のクライアント接続を同じサーバに送信できます。
- 4 送信元 IP アドレスによるパーシステンス プロファイルまたは Cookie によるパーシステンス プロファイルを選択します。
- 5 ドロップダウン メニューから既存のパーシステンス プロファイルを選択します。
- 6 [次へ (Next)] をクリックします。
- 7 [クライアント側 SSL] ボタンを切り替えてプロファイルを有効にします。  
クライアント側で SSL プロファイル バインドを行うと、複数のホスト名に対応する複数の証明書を同一の仮想サーバに関連付けることができます。  
関連付けられたクライアント側 SSL のプロファイルが自動的に適用されます。
- 8 ドロップダウン メニューからデフォルトの証明書を選択します。  
この証明書は、サーバが同じ IP アドレスの複数のホスト名に対応しない場合、またはクライアントが SNI (Server Name Indication) 拡張機能をサポートしていない場合に使用されます。
- 9 使用可能な SNI 証明書を選択し、矢印をクリックして証明書を [選択済み] セクションに移動します。
- 10 (オプション) [必須のクライアント認証] を切り替えて、このメニュー項目を有効にします。
- 11 使用可能な CA 証明書を選択し、矢印をクリックして証明書を [選択済み] セクションに移動します。
- 12 サーバ証明書チェーンの階層の深さを確認するための [証明書チェーンの深さ] を設定します。

- 13 使用可能な CRL を選択し、矢印をクリックして証明書を [選択済み] セクションに移動します。

CRL を設定することで、不正なサーバ証明書を禁止することができます。

- 14 [次へ (Next)] をクリックします。

- 15 [サーバ側 SSL] ボタンを切り替えてプロファイルを有効にします。

関連付けられたサーバ側 SSL のプロファイルが自動的に適用されます。

- 16 ドロップダウン メニューからクライアントの証明書を選択します。

このクライアント証明書は、サーバが同じ IP アドレスの複数のホスト名に対応しない場合、またはクライアントがサーバ名インディケーション SNI (Server Name Indication) 拡張機能をサポートしていない場合に使用されます。

- 17 使用可能な SNI 証明書を選択し、矢印をクリックして証明書を [選択済み] セクションに移動します。

- 18 (オプション) [サーバ認証] を切り替えて、このメニュー項目を有効にします。

サーバ側 SSL プロファイル バインドによって、SSL ハンドシェイク中にロード バランサに提示されるサーバ証明書を検証する必要があるかどうかを指定します。検証を有効にする場合、サーバ証明書は、同じサーバ側 SSL プロファイル バインドで自己署名証明書が指定されている、信頼された CA の 1 つによって署名されている必要があります。

- 19 使用可能な CA 証明書を選択し、矢印をクリックして証明書を [選択済み] セクションに移動します。

- 20 サーバ証明書チェーンの階層の深さを確認するための [証明書チェーンの深さ] を設定します。

- 21 使用可能な CRL を選択し、矢印をクリックして証明書を [選択済み] セクションに移動します。

CRL を設定することで、不正なサーバ証明書を禁止することができます。サーバ側では、OCSP および OCSP Stapling はサポートされていません。

- 22 [終了 (Finish)] をクリックします。

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 サーバを作成し、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。ただし、論理スイッチ上に DHCP サーバを設定したり、同じ論理スイッチが接続されているルーター ポート上で DHCP リレー サービスを設定することは避けてください。このようなシナリオでは、DHCP リクエストは DHCP リレー サービスにのみ送信されます。

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分散ファイアウォール ルールを設定します。

---

**注：** Logical Switch/Logical Port/NSGroup を宛先、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 分散ファイアウォール 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、送信元と宛先の両方を 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、[DDI] - [DHCP] の順に選択します。
- 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。
- 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 NSX Edge クラスタを選択します。
- 6 (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

- 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、[DDI] - [DHCP] の順に選択します。
- 3 [サーバ] 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 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。
- 6 (必須) 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。
- 7 (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。
- 8 (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。
- 9 (オプション) 他のオプションを入力します。
- 10 [保存] をクリックします。
- 11 新しく作成した DHCP サーバを選択します。
- 12 IP アドレス プールのセクションを展開します。
- 13 [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。
- 14 静的バインドのセクションを展開します。

- 15 [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、[DDI] - [DHCP] の順に選択します。
- 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、[DDI] - [DHCP] の順に選択します。
- 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

# 12

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。

#### 例

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	53293932-b4b0-11e8-8ae0-000c298761d2	×	▼

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。

## 結果

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。

## 結果

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。

IP アドレス管理 (IPAM) では、NSX-T Container Plug-in (NCP) をサポートする IP アドレス ブロックを作成できます。NCP の詳細については、『NSX-T Container Plug-in for Kubernetes - インストールおよび管理ガイド』を参照してください。

この章には、次のトピックが含まれています。

- IP アドレス ブロックの管理
- IP アドレス ブロックのサブネットの管理

## IP アドレス ブロックの管理

NSX-T Container Plug-in を設定するには、コンテナに IP アドレス ブロックを作成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、[DDI] - [IP アドレス管理 (IPAM)] の順に選択します。
- 3 IP アドレス ブロックを追加するには、[追加 (Add)] をクリックします。
  - a 名前を入力します。必要に応じて説明も入力します。
  - b IP アドレス ブロックを CIDR 形式で入力します。例 : 10.10.10.0/24。
- 4 IP アドレス ブロックを編集するには、IP アドレス ブロックの名前をクリックします。
  - a [概要 (Overview)] タブで [編集 (Edit)] をクリックします。  
名前、説明、または IP アドレス ブロックの値を変更できます。
- 5 IP アドレス ブロックのタグを管理するには、IP アドレス ブロックの名前をクリックします。
  - a [概要 (Overview)] タブで [管理 (Manage)] をクリックします。  
タグを追加または削除できます。
- 6 1 つ以上の IP アドレス ブロックを削除するには、ブロックを選択します。
  - a [削除 (Delete)] をクリックします。  
サブネットが割り当てられた IP アドレス ブロックは削除できません。

## IP アドレス ブロックのサブネットの管理

IP アドレス ブロックにサブネットを追加したり、削除できます。

### 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、[DDI] - [IP アドレス管理 (IPAM)] の順に選択します。
- 3 IP アドレス ブロックの名前をクリックします。
- 4 [サブネット (Subnets)] タブをクリックします。
- 5 サブネットを追加するには、[追加 (Add)] をクリックします。
  - a 名前を入力します。必要に応じて説明も入力します。
  - b サブネットのサイズを入力します。
- 6 1 つ以上のサブネットを削除するには、サブネットを選択します。
  - a [削除 (Delete)] をクリックします。

ポリシーとはルールとサービスの組み合わせで、ルールによってリソースへのアクセスおよび使用率の基準が定義されます。NSX ポリシーを使用すると、低レベルの詳細を気にせずにリソースへのアクセスおよび使用率を管理できます。

この章には、次のトピックが含まれています。

- [概要](#)
- [適用ポイントの追加](#)
- [通信プロファイルの追加](#)
- [サービスの追加](#)
- [ドメインの追加](#)
- [NSX Policy Manager のバックアップの設定](#)
- [NSX Policy Manager のバックアップ](#)
- [NSX Policy Manager のリストア](#)
- [vIDM ホストと NSX Policy Manager の関連付け](#)
- [ロールの割り当ての管理](#)

## 概要

NSX ポリシーを使用すると、ルールの仕組みを気にせずに、仮想マシン、論理ポート、IP アドレス、MAC アドレスなどのオブジェクトのルールを指定できます。NSX Manager ではなく、NSX Policy Manager からポリシーを管理します。

ポリシーを設定する前に、NSX Policy Manager をインストールする必要があります。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。NSX Policy Manager では、適用ポイントを追加し、ポリシーが適用される NSX Manager に関する情報を提供する必要があります。

次の例は、ポリシーを使用してアプリケーションのネットワークを管理する方法を示しています。

アプリケーションには 3 つの層（Web、アプリケーション、データベース）があり、アプリケーションの仮想マシンに次のルールを適用する必要があります。

- Web 層とアプリケーション層間のトラフィックを許可する。

- アプリケーション層とデータベース層間のトラフィックを許可する。
- 任意のシステムと Web 層間のトラフィックを許可する。

NSX Manager で、次の手順を実行します。

- Web 仮想マシンのワークロード名を、Web の後に識別文字列を続けて設定します。
- アプリケーション仮想マシンのワークロード名を、App の後に識別文字列を続けて設定します。
- データベース仮想マシンのワークロード名を、DB の後に識別文字列を続けて設定します。

NSX Policy Manager で、次の手順を実行します。

- Profile1 という通信プロファイルを作成して、Web 層とアプリケーション層間のトラフィックを許可します。
- Profile2 という通信プロファイルを作成して、アプリケーション層とデータベース層間のトラフィックを許可します。
- Profile3 という通信プロファイルを作成して、任意のシステムと Web 層間のトラフィックを許可します。
- ドメインを作成し、以下を指定します。
  - ワークロード名が Web で始まる仮想マシンで構成される WebGroup というグループを作成する。
  - ワークロード名が App で始まる仮想マシンで構成される AppGroup というグループを作成する。
  - ワークロード名が DB で始まる仮想マシンで構成される DBGroup というグループを作成する。
  - Profile1 を送信元として WebGroup に関連付け、宛先として AppGroup に関連付ける。
  - Profile2 を送信元として AppGroup に関連付け、宛先として DBGroup に関連付ける。
  - Profile3 を送信元として Any に関連付け、宛先として WebGroup に関連付ける。
- ドメインを検証して、エラーがないことを確認します。
- ドメインをデプロイします。

ドメインをデプロイすると、NSX Policy Manager は NSX Manager と通信し、ポリシーを実装します。

## ロールベースのアクセス制御

NSX Policy Manager には、**admin** と **audit** という 2 つの組み込みユーザーが用意されています。NSX Policy Manager と VMware Identity Manager (vIDM) を統合して、vIDM が管理するユーザーにロールベースのアクセス制御 (RBAC) を設定できます。

vIDM によって管理されるユーザーに適用される認証ポリシーは、vIDM 管理者によって設定されたポリシーです。**admin** および **audit** ユーザーにのみ適用される NSX Policy Manager の認証ポリシーではありません。

## 適用ポイントの追加

適用ポイントとは、ポリシーのルールを適用する場所のことです。今回のリリースでは、適用ポイントには NSX-T インストールを指定する必要があります。NSX Policy Manager がサポートする適用ポイントは 1 つのみです。



## 手順

- 1 ブラウザから <https://nsx-policy-manager-IP-address> にアクセスし、NSX Policy Manager 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] - [適用ポイント] の順に選択します。
- 3 [追加] をクリックします。
- 4 次の情報を指定します。

パラメータ	説明
名前	適用ポイントの名前。
認証情報	NSX Manager にログインするためのユーザー名およびパスワード。
適用アドレス	NSX Manager の IP アドレス。
サムプリント	NSX Manager の証明書サムプリント。

- 5 [保存] をクリックします。

## 通信プロファイルの追加

通信プロファイルとは、特定のサービスに対して実行されるアクションを指定する再利用可能なエンティティのことです。複数のドメイン内の通信エントリで参照することができます。

サービスの例としては、FTP、HTTP、Active Directory サーバ、DHCP サーバ、Oracle Database などがあります。指定したサービスへのトラフィックを許可、ドロップ、または却下することができます。

## 手順

- 1 ブラウザから <https://nsx-policy-manager-IP-address> にアクセスし、NSX Policy Manager にログインします。
- 2 ナビゲーション パネルから、[インフラストラクチャ (Infra)] - [プロファイル (Profiles)] の順に選択します。
- 3 [追加 (Add)] をクリックします。
- 4 プロファイルの名前を指定します。
- 5 [追加 (Add)] をクリックしてプロファイル エントリを追加します。

a プロファイル エントリの名前を指定します。

b [サービス (Services)] フィールドをクリックして、HTTP、Oracle Database などのサービスを 1 つ以上選択します。

c [アクション (Action)] フィールドをクリックして、アクションを選択します。

使用可能なアクションは [許可 (Allow)]、[ドロップ (Drop)]、[却下 (Reject)] です。

エントリは追加できます。また、[削除 (Delete)] をクリックしてエントリを削除したり、[アクション (Action)] をクリックしてエントリの順序を変更したりできます。

- 6 [保存 (Save)] をクリックします。

## サービスの追加

サービスとは、環境内のプロトコルまたはソフトウェア コンポーネントのことです。ポリシーには、サービスに適用されるルールが含まれています。

サービスの例は FTP、HTTP、Active Directory サーバ、DHCP サーバ、Oracle データベースなどです。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-ip-address> にアクセスし、NSX Policy Manager にログインします。
- 2 ナビゲーション パネルから、[インフラストラクチャ (Infra)] - [サービス (Services)] の順に選択します。
- 3 [追加 (Add)] をクリックして、サービスを追加します。
- 4 サービスの名前を指定します。
- 5 [追加 (Add)] をクリックして、サービスのエントリを追加します。
  - a サービス エントリの名前を指定します。
  - b [タイプ (Type)] フィールドをクリックして、タイプを指定します。

使用可能なタイプは、[Ether]、[IP]、[IGMP]、[ICMP]、[ALG]、および [L4 ポート セット (L4 Port Set)] です。
  - c [プロパティ (Properties)] フィールドをクリックして、プロパティを設定します。

エントリを追加するか、または [削除 (Delete)] をクリックしてエントリを削除することができます。
- 6 [保存 (Save)] をクリックします。

## ドメインの追加

ドメインは、共通のビジネス目的に使用されるワークロードの論理的な集合体です。ドメインにはポリシーを適用する必要があります。ドメインにはグループおよび対応する通信要件が 1 セット含まれています。

それぞれに 200 個以上のルールがある複数の大規模なドメインを作成する場合は、必ず各ドメインの実行結果を確認してから次に進み、適用ポイントに順番に展開していきます。API を使用してこれらのドメインを展開する場合は、ドメインが適用ポイントに展開される前に通信のエントリを作成することをお勧めします。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-ip-address> にアクセスし、NSX Policy Manager にログインします。
- 2 ナビゲーション パネルから、[インフラストラクチャ (Infra)] - [ドメイン (Domains)] の順に選択します。
- 3 [追加 (Add)] をクリックしてドメインを追加します。
- 4 ドメインの名前と、必要に応じて説明を指定します。
- 5 [次へ (Next)] をクリックして、ワークロード グループの手順に進みます。

6 [追加 (Add)] をクリックして、ワークロード グループを追加します。

- a ワークロード グループの名前を指定します。
- b [メンバー (Members)] フィールドをクリックして、メンバーを選択します。
- c メンバーシップのタイプを選択します。

使用可能なタイプは、[仮想マシン (Virtual Machine)]、[論理ポート (Logical Port)]、[IP アドレス (IP Address)]、および [MAC アドレス (MAC Address)] です。

- d メンバーの選択方法を指定するには、[条件を追加 (Add Criteria)] または [追加 (Add)] をクリックします。

仮想マシンの基準は、タグまたはワークロード グループ名の値に基づいて設定できます。タグでサポートされている演算子は [が次と等しい (Equals)] です。ワークロード グループ名でサポートされている演算子は、[が次と等しい (Equals)]、[が次を含む (Contains)]、[が次で始まる (Starts With)] です。論理ポートの基準には、タグの値を指定する必要があります。IP アドレスには、実際のアドレスまたはアドレス範囲を指定します。MAC アドレスには、実際のアドレスを指定します。

ワークロード グループを追加するか、または [削除 (Delete)] をクリックしてグループを削除することができます。

7 [次へ (Next)] をクリックして、通信の手順に進みます。

8 [追加 (Add)] をクリックして、通信のエントリを追加します。

- a 通信の名前を指定します。
- b [通信プロファイル (Communication Profile)] フィールドをクリックして、通信プロファイルを選択します。
- c [送信元 (Sources)] フィールドをクリックして、ワークロード グループを選択します。
- d [ターゲット (Destinations)] フィールドをクリックして、ワークロード グループを選択します。

通信エントリを追加する、[削除 (Delete)] をクリックしてエントリを削除する、または [アクション (Actions)] をクリックしてエントリの順序を変更することができます。

9 [次へ (Next)] をクリックして、ドメインの検証手順に進みます。

ドメインがグラフで表示されます。

10 [次へ (Next)] をクリックして、ドメインのデプロイ手順に進みます。

11 適用ポイントを選択します。

12 [終了 (Finish)] をクリックして、ドメインをデプロイします。

## 結果

---

**注：** ドメインを編集して、通信エントリの名前を変更しても、元の名前は通信エントリを追跡するために引き続き内部で使用されます。新しい通信エントリを作成する場合は、元の名前を使用しないでください。競合が発生し、新しいエントリが作成されなくなります。

---

## NSX Policy Manager のバックアップの設定

NSX Policy Manager をバックアップすることで、Policy Manager が保存するデータを保護できます。バックアップを実行する前に、バックアップのプロパティを設定する必要があります。

### 前提条件

バックアップ ファイル サーバの SSH フィンガープリントを入手します。フィンガープリントとして使用できるのは、SHA256 ハッシュの ECDSA キーだけです。「[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。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-ip-address> にアクセスし、NSX Policy Manager 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] - [ユーティリティ] の順に選択します。
- 3 [設定] をクリックします。
- 4 [自動バックアップ] 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または無効にします。
- 5 バックアップ ファイル 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 バックアップ ファイル 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 [宛先ディレクトリ] 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。  
存在するディレクトリを使用してください。
- 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 [スケジュール] タブをクリックします。
- 12 頻度を選択します。  
[毎週] を選択した場合は、曜日と時刻を指定します。[間隔] を選択した場合は、間隔を指定します。
- 13 [保存] をクリックします。

## NSX Policy Manager のバックアップ

NSX Policy Manager は自動または手動でバックアップできます。

自動バックアップが設定されている場合は、バックアップが自動的に行われます。この手順では、手動でバックアップを開始します。

### 前提条件

バックアップのプロパティが設定されていることを確認します。「[NSX Policy Manager のバックアップの設定](#)」を参照してください。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-IP-address> にアクセスし、NSX Policy Manager 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] - [ユーティリティ] の順に選択します。
- 3 [今すぐバックアップ] をクリックします。

## NSX Policy Manager のリストア

NSX Policy Manager をバックアップから過去の状態にリストアすることができます。

### 前提条件

バックアップ ファイル サーバの SSH フィンガープリントを入手します。フィンガープリントとして使用できるのは、SHA256 ハッシュの ECDSA キーだけです。[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。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-IP-address> にアクセスし、NSX Policy Manager 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 [今すぐリストア (Restore Now)] をクリックします。
- 4 前提条件とリスクに関するメッセージを確認し、[次へ (Next)] をクリックします。
- 5 バックアップ サーバの IP アドレスまたはホスト名を入力します。
- 6 必要に応じてポート番号を変更します。  
デフォルトは 22 です。
- 7 サーバへのログインで使用するユーザー名とパスワードを入力します。
- 8 [バックアップ ディレクトリ (Backup Directory)] フィールドに、バックアップの保存先ディレクトリの絶対パスを入力します。
- 9 バックアップ データの暗号化で使ったパスフレーズを入力します。
- 10 バックアップ サーバの SSH フィンガープリントを入力します。
- 11 [次へ (Next)] をクリックします。
- 12 バックアップを選択します。

### 13 [リストア (Restore)] をクリックします。

リストア操作のステータスが表示されます。バックアップの作成後にファブリック ノードまたはトランスポート ノードを削除または追加した場合には、ノードへのログインやスクリプトの実行など、特定の操作を実行するように指示されます。

リストア操作の完了後、リストアの完了画面が開き、復元の結果、バックアップ ファイルのタイムスタンプ、リストア操作の開始時間と終了時間が表示されます。リストアに失敗すると、エラーが発生した手順が画面に表示されます。

## vIDM ホストと NSX Policy Manager の関連付け

NSX Policy Manager と vIDM の統合を有効にするには、vIDM ホストの情報を指定する必要があります。

### 前提条件

- vIDM ホストの証明書サムプリントがあることを確認します。[vIDM ホストからの証明書サムプリントの取得](#)を参照してください。
- vIDM ホストに NSX Policy Manager が OAuth クライアントとして登録されていることを確認します。登録時に、クライアント ID とクライアント シークレットをメモしてください。詳細については、<https://www.vmware.com/support/pubs/identitymanager-pubs.html> で VMware Identity Manager のドキュメントを参照してください。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-ip-address> にアクセスし、NSX Policy Manager 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)] - [ユーザー (Users)] の順に選択します。
- 3 [設定 (Configuration)] タブをクリックします。
- 4 [編集 (Edit)] をクリックします。
- 5 [VMware Identity Manager の統合 (VMware Identity Manager Integration)] をクリックして、[有効 (Enabled)] に切り替えます。
- 6 次の情報を指定します。

パラメータ	説明
VMware Identity Manager アプライアンス	vIDM ホストの完全修飾ドメイン名 (FQDN)。
OAuth クライアント ID	vIDM ホストに NSX Policy Manager を登録するときに作成される ID。
OAuth クライアント シークレット	vIDM ホストに NSX Policy Manager を登録するときに作成されるシークレット。

パラメータ	説明
SHA-256 サムプリント	vIDM ホストの証明書のサムプリント。
NSX ポリシー アプライアンス	NSX Policy Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN)。FQDN を指定する場合は、URL で VMware Identity Manager の FQDN を使用してブラウザから NSX Policy Manager にアクセスする必要があります。また、IP アドレスを指定する場合は、URL に IP アドレスを使用する必要があります。あるいは、vIDM 管理者が、FQDN または IP アドレスのいずれかを使用して接続できるように NSX Policy Manager クライアントを設定します。

7 [保存 (Save)] をクリックします。

## ロールの割り当ての管理

VMware Identity Manager が NSX Policy Manager と統合されている場合には、ユーザーまたはユーザー グループにロールを割り当てたり、割り当ての変更や削除を行うことができます。

Admin と Auditor という 2 つの組み込みロールが用意されています。新しいロールは追加できません。

### 前提条件

- vIDM ホストが NSX Policy Manager に関連付けられていることを確認します。詳細については、[vIDM ホストと NSX Policy Manager の関連付け](#)を参照してください。

### 手順

- 1 ブラウザから <https://nsx-policy-manager-IP-address> にアクセスし、NSX Policy Manager 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)] - [ユーザー (Users)] の順に選択します。
- 3 まだ選択していない場合は、[キーの割り当て (Role Assignments)] タブをクリックします。
- 4 ロールの割り当てを追加、変更、または削除します。

オプション	操作
ロールの割り当てを追加する	[追加 (Add)] をクリックしてユーザーまたはユーザー グループを選択し、ロールを選択します。
ロール割り当てを変更する	ユーザーまたはユーザー グループを選択して、[編集 (Edit)] をクリックします。
ロールの割り当てを削除する	ユーザーまたはユーザー グループを選択して、[削除 (Delete)] をクリックします。

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 アカウントとロールベースのアクセス コントロールの管理](#)
- [証明書の設定](#)
- [アプライアンスの設定](#)
- [コンピュート マネージャの追加](#)
- [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](#)
- [DNE Key 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](#)
- [ログ収集システム 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](#)



- [仮想マシンで実行中のアプリケーションのデータの表示](#)
- [プリンシパル ID の表示](#)
- [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 アカウントとロールベースのアクセス コントロールの管理

NSX-T アプライアンスには、admin と audit という 2 つのユーザーが事前に設定されています。NSX-T と VMware Identity Manager (vIDM) を統合して、vIDM が管理するユーザーにロールベースのアクセス コントロール (RBAC) を設定できます。

vIDM によって管理されるユーザーに適用される認証ポリシーは、vIDM 管理者によって設定されたポリシーです。admin または audit ユーザーにのみ適用される NSX-T の認証ポリシーではありません。

## CLI ユーザーのパスワードの変更

各アプライアンスには admin と audit の 2 つの組み込みユーザーが用意されています。これらのユーザーを使用して CLI にログインしてコマンドを実行できます。これらのユーザーのパスワードは変更できますが、ユーザーを追加したり、削除することはできません。

### 手順

- 1 アプライアンスの CLI にログインします。
- 2 `set user` コマンドを実行します。次はその例です。

```
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

## 認証ポリシーの設定

CLI を使用すると、認証ポリシーの設定を表示したり、変更することができます。

次のコマンドを使用して、パスワードの最小長を表示または設定できます。

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

次のコマンドは、NSX Manager ユーザー インターフェイスへのログインまたは、API 呼び出しに適用されます。

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

次のコマンドは、NSX Manager、NSX Controller または NSX Edge ノードで CLI にログインする場合に適用されます。

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

CLI コマンドの詳細については、『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。

デフォルトでは、NSX Manager ユーザー インターフェイスへのログインに 5 回連続して失敗すると、管理者アカウントが 15 分間ロックされます。次のコマンドを使用すると、アカウントのロックアウトを無効にできます。

```
set auth-policy api lockout-period 0
```

同様に、次のコマンドでも CLI のアカウント ロックアウトを無効にできます。

```
set auth-policy cli lockout-period 0
```

## vIDM ホストからの証明書サムプリントの取得

vIDM と NSX-T の統合を設定する前に、vIDM ホストから証明書サムプリントを取得する必要があります。

### 手順

- 1 SSH で vIDM ホストに接続し、**sshuser** としてログインします。
- 2 次のコマンドを実行して、**root** ユーザーになります。

```
su root
```

- 3 /etc/ssh/sshd\_config ファイルを編集し、PermitRootLogin の値を yes に、StrictModes の値を no にそれぞれ変更します。

```
PermitRootLogin yes
StrictModes no
```

- 4 次のコマンドを実行して、sshd サービスを再起動します。

```
service sshd restart
```

- 5 ログアウトして **root** としてログインします。
- 6 次のコマンドを実行して、Director に変更します。

```
cd /usr/local/horizon/conf
```

- 7 次のコマンドを実行して、サムプリントを取得します。

```
openssl x509 -in <FQDN of vIDM host>_cert.pem -noout -sha256 -fingerprint
```

次はその例です。

```
openssl x509 -in vidm.corp.local_cert.pem -noout -sha256 -fingerprint
```

## vIDM ホストと NSX-T の関連付け

NSX-T と vIDM の統合を有効にするには、vIDM ホストの情報を指定する必要があります。

### 前提条件

- vIDM ホストの証明書サムプリントがあることを確認します。[vIDM ホストからの証明書サムプリントの取得](#)を参照してください。
- vIDM ホストに NSX Manager が OAuth クライアントとして登録されていることを確認します。登録時に、クライアント ID とクライアント シークレットをメモしてください。詳細については、<https://www.vmware.com/support/pubs/identitymanager-pubs.html> で VMware Identity Manager のドキュメント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)] - [ユーザー (Users)] の順に選択します。
- 3 [設定 (Configuration)] タブをクリックします。
- 4 [編集 (Edit)] をクリックします。
- 5 次の情報を指定します。

パラメータ	説明
VMware Identity Manager アプライアンス	vIDM ホストの完全修飾ドメイン名 (FQDN)。
クライアント ID	vIDM ホストに NSX Manager を登録するときに作成される ID。
クライアント シークレット	vIDM ホストに NSX Manager を登録するときに作成されるシークレット。
サムプリント	vIDM ホストの証明書のサムプリント。
NSX アプライアンス	NSX Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN)。FQDN を指定する場合は、URL で VMware Identity Manager の FQDN を使用してブラウザから NSX Manager にアクセスする必要があります。また、IP アドレスを指定する場合は、URL に IP アドレスを使用する必要があります。あるいは、vIDM 管理者が、FQDN または IP アドレスのいずれかを使用して接続できるように NSX Manager クライアントを設定します。

- 6 [保存 (Save)] をクリックします。

## NSX Manager、vIDM、および関連コンポーネント間の時刻の同期

認証を正しく動作させるには、NSX Manager、vIDM、および Active Directory などのサービス プロバイダのすべての時刻が同期している必要があります。このセクションでは、これらのコンポーネントの時刻を同期させる方法について説明します。

## VMware Infrastructure

ESXi ホストの同期については、次のナレッジベースの記事を参照してください。

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

仮想マシンとホストの同期方法については、[https://docs.vmware.com/jp/VMware-vSphere/6.0/com.vmware.vsphere.vm\\_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html](https://docs.vmware.com/jp/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html) を参照してください。仮想マシンは、NSX Manager、vIDM、Active Directory、またはその他のサービス プロバイダを実行している可能性があります。

### サードパーティ製インフラストラクチャ

仮想マシンとホストの同期方法については、ベンダーのドキュメントを参照してください。

### vIDM サーバでの NTP の設定（推奨されません）

ホスト間で時刻を同期できない場合は、ホストへの同期を無効にして、vIDM サーバ上で NTP を設定することができます。vIDM サーバの UDP ポート 123 を開く必要があるため、この方法は推奨されません。

- vIDM サーバの時刻を確認し、正しいかどうかを確認します。

```
# hwclock
Tue May  9 12:08:43 2017  -0.739213 seconds
```

- /etc/ntp.conf を編集し、次のエントリが見つからない場合は追加します。

```
server server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- UDP ポート 123 を開きます。

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

次のコマンドを実行して、ポートが開いていることを確認します。

```
# iptables -L -n
```

- NTP サービスを開始します。

```
/etc/init.d/ntp start
```

- 再起動後 NTP を自動的に実行するように設定します。

```
# chkconfig --add ntp
# chkconfig ntp on
```

- NTP サーバにアクセスできることを確認します。

```
# ntpq -p
```

reach 列には 0 が表示されていないことを確認します。st 列には 16 以外の数字が表示されている事を確認します。

## ロールベースのアクセス制御

ロールベースのアクセス制御 (RBAC) では、許可されたユーザーにシステムへのアクセスを制限できます。ロールはユーザーに割り当てられます。各ロールには特定の権限が設定されています。

権限には 4 つのタイプがあります。

- フル アクセス
- 実行
- 読み取り
- なし

フル アクセスは、すべての権限をユーザーに付与します。実行権限には、読み取り権限が含まれています。

NSX-T には、次のロールが事前に用意されています。新しいロールは追加できません。

- エンタープライズ管理者
- 監査者
- ネットワーク エンジニア
- ネットワーク オペレーション
- セキュリティ エンジニア
- セキュリティ オペレーション
- クラウド サービス管理者
- クラウド サービス監査者
- ロード バランサ管理者
- ロード バランサ監査者

Active Directory (AD) ユーザーにロールが割り当てられた後、Active Directory サーバ上でユーザー名が変更された場合は、新しいユーザー名を使用してロールを再度割り当てる必要があります。

## ロールと権限

表 15-1. [ロールと権限](#) に、各ロールの操作権限を示します。次の略語を使用します。

- EA - エンタープライズ管理者
- A - 監査者
- NE - ネットワーク エンジニア
- NO - ネットワーク オペレーション
- SE - セキュリティ エンジニア

- SO - セキュリティ オペレーション
- CS Adm - クラウド サービス管理者
- CS Aud - クラウド サービス監査者
- LB Adm - ロード バランサ管理者
- LB Aud - ロード バランサ監査者
- FA - フル アクセス
- E - 実行
- R - 読み取り

表 15-1. ロールと権限

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
[ツール] > [ポートの接続]	E	R	E	E	E	E	E	R	E	E
[ツール] > [トレースフロー]	E	R	E	E	E	E	E	R	E	E
[ツール] > [ポートミラーリング]	FA	R	FA	FA	FA	FA	FA	R	なし	なし
[ツール] > [IPFIX]	FA	R	FA	R	FA	R	FA	R	なし	なし
[ファイアウォール] > [全般]	FA	R	R	R	FA	R	FA	R	なし	なし
[ファイアウォール] > [設定]	FA	R	R	R	FA	R	FA	R	なし	なし
暗号化	FA	R	FA	R	FA	FA	なし	なし	なし	なし
[ルーティング] > [ルーター]	FA	R	FA	R	R	R	FA	R	R	R
[ルーティング] > [NAT]	FA	R	FA	R	FA	R	FA	R	R	R
[DDI] > [DHCP] > [サーバプロファイル]	FA	R	FA	R	FA	なし	FA	R	なし	なし
[DDI] > [DHCP] > [サーバ]	FA	R	FA	R	FA	なし	FA	R	なし	なし
[DDI] > [DHCP] > [リレープロファイル]	FA	R	FA	R	FA	なし	FA	R	なし	なし

表 15-1. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
[DDI] > [DHCP] > [リレ ー サービス]	FA	R	FA	R	FA	なし	FA	R	なし	なし
[DDI] > [DHCP] > [メタ データ プロキ シ]	FA	R	FA	R	FA	なし	なし	なし	なし	なし
[DDI] > [IP ア ドレス管理]	FA	R	FA	R	FA	なし	なし	なし	なし	なし
[スイッチング] > [スイッチ]	FA	R	FA	FA	R	R	FA	R	R	R
[スイッチング] > [ポート]	FA	R	FA	FA	R	R	FA	R	R	R
[スイッチング] > [スイッチ ング プロファイ ル]	FA	R	FA	FA	FA	FA	FA	R	R	R
[ロード バラン シング] > [ロー ド バランサ]	FA	R	なし	なし	なし	なし	FA	R	FA	R
[ロード バラン サ] > [仮想サー バ]	FA	R	なし	なし	なし	なし	FA	R	FA	R
[ロード バラン サ] > [アプリケ ーション プロフ ァイル]	FA	R	なし	なし	なし	なし	FA	R	FA	R
[ロード バラン サ] > [セッション 維持 プロファ イル]	FA	R	なし	なし	なし	なし	FA	R	FA	R
[ロード バラン サ] > [SSL プロ ファイル]	FA	R	なし	なし	FA	R	FA	R	FA	R
[ロード バラン サ] > [サーバ プ ール]	FA	R	なし	なし	なし	なし	FA	R	FA	R
[ロード バラン サ] > [アクティ ブ健全性モニタ ー]	FA	R	なし	なし	なし	なし	FA	R	FA	R
[ロード バラン サ] > [パッシブ 健全性モニター]	FA	R	なし	なし	なし	なし	FA	R	FA	R



表 15-1. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
[インベントリ] > [グループ]	FA	R	FA	R	FA	R	FA	R	R	R
[インベントリ] > [IP セット]	FA	R	FA	R	FA	R	FA	R	R	R
[インベントリ] > [IP アドレス プール]	FA	R	FA	R	なし	R	なし	なし	R	R
[インベントリ] > [MAC セッ ト]	FA	R	FA	R	FA	R	FA	R	R	R
[インベントリ] > [サービス]	FA	R	FA	R	FA	R	FA	R	R	R
[インベントリ] > [仮想マシン]	R	R	R	R	R	R	R	R	R	R
[インベントリ] > [仮想マシン] > [タグの作成 および割り当て]	FA	R	FA	FA	FA	FA	FA	R	R	R
[インベントリ] > [仮想マシン] > [タグの設定]	FA	なし	なし	なし	FA	なし	なし	なし	なし	なし
[ファブリック] > [ノード] > [ホスト]	FA	R	R	R	R	R	R	R	なし	なし
[ファブリック] > [ノード] > [ノード]	FA	R	FA	R	FA	R	R	R	なし	なし
[ファブリック] > [ノード] > [Edge]	FA	R	FA	R	R	R	R	R	なし	なし
[ファブリック] > [ノード] > [Edge クラス タ]	FA	R	FA	R	R	R	R	R	なし	なし
[ファブリック] > [ノード] > [ブリッジ]	FA	R	FA	R	R	R	なし	なし	R	R
[ファブリック] > [ノード] > [トランスポート ノード]	FA	R	R	R	R	R	R	R	R	R
[ファブリック] > [ノード] > [トンネル]	R	R	R	R	R	R	R	R	R	R

表 15-1. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
[ファブリック] > [プロファイ ル] > [アップリ ック プロファイ ル]	FA	R	R	R	R	R	R	R	R	R
[ファブリック] > [プロファイ ル] > [Edge ク ラス プロファ イル]	FA	R	FA	R	R	R	R	R	R	R
[ファブリック] > [プロファイ ル] > [設定]	FA	R	なし	なし	なし	なし	R	R	なし	なし
[ファブリック] > [トランスポ ートゾーン] > [トランスポート ゾーン]	FA	R	R	R	R	R	R	R	R	R
[ファブリック] > [トランスポ ートゾーン] > [トランスポート ゾーン プロファ イル]	FA	R	R	R	R	R	R	R	R	R
[ファブリック] > [コンピュー ト マネージャ]	FA	R	R	R	R	R	R	R	なし	なし
[システム] > [信 頼]	FA	R	なし	なし	FA	R	なし	なし	FA	R
[システム] > [設 定]	E	R	R	R	R	R	なし	なし	なし	なし
[システム] > [ユ ーティリティ] > [サポート バ ンドル]	FA	R	R	R	R	R	R	R	なし	なし
[システム] > [ユ ーティリティ] > [バックアッ プ]	FA	R	なし	なし	なし	なし	なし	なし	なし	なし
[システム] > [ユ ーティリティ] > [リストア]	FA	R	なし	なし	なし	なし	なし	なし	なし	なし
[システム] > [ユ ーティリティ] > [アップグレ ード]	FA	R	R	R	R	R	なし	なし	なし	なし

表 15-1. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
[システム] > [ユーザー] > [ロールの割り当て]	FA	R	なし	なし	なし	なし	なし	なし	なし	なし
[システム] > [ユーザー] > [設定]	FA	R	なし	なし	なし	なし	なし	なし	なし	なし

## ロールの割り当ての管理

VMware Identity Manager が NSX-T と統合されている場合には、ユーザーまたはユーザー グループにロールを割り当てたり、割り当ての変更や削除を行うことができます。

### 前提条件

- vIDM ホストが NSX-T に関連付けられていることを確認します。詳細については、[vIDM ホストと NSX-T の関連付け](#)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] - [ユーザー] の順に選択します。
- 3 まだ選択していない場合は、[ロールの割り当て] タブをクリックします。
- 4 ロールの割り当てを追加、変更、または削除します。

オプション	操作
ロールの割り当てを追加する	[追加] をクリックしてユーザーまたはユーザー グループを選択し、ロールを選択します。
ロール割り当てを変更する	ユーザーまたはユーザー グループを選択して、[編集] をクリックします。
ロールの割り当てを削除する	ユーザーまたはユーザー グループを選択して、[削除] をクリックします。

## 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] - [信頼] の順に選択します。
- 3 [CSRS] タブをクリックします。
- 4 [CSR を生成] をクリックします。
- 5 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。
コモン ネーム	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。
部門名	この証明書を扱う組織の部門を入力します。 例 : IT department。
市区町村	組織が存在する都市を入力します。 例 : Palo Alto。
都道府県	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。

- 6 [保存] 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。

- 7 証明書署名要求を選択して [アクション] をクリックします。

- 8 ドロップダウン メニューから [CSR PEM をダウンロード] 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。

- 9 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。

#### 結果

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、会社の臨時の 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] - [信頼] の順に選択します。
- 3 [証明書] タブをクリックします。
- 4 [インポート] - [認証局 (CA) 証明書をインポート] の順に選択して、証明書の詳細を入力します。

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] をクリックします。

#### 結果

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] - [信頼] の順に選択します。
- 3 [証明書] タブをクリックします。
- 4 [インポート] - [証明書をインポート] の順に選択して、証明書の詳細を入力します。

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] をクリックします。

### 結果

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

自己署名証明書は信頼される証明書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。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。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、クライアント ユーザーのセキュリティが低下します。

### 前提条件

証明書署名要求 (CSR) が使用可能かどうか確認します。「[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] - [信頼] の順に選択します。
- 3 [CSRS] タブをクリックします。
- 4 既存の証明書署名要求を選択します。
- 5 [アクション] をクリックし、ドロップダウン メニューから [CSR の自己署名証明書] を選択します。

- 自己署名証明書の有効期間を入力します。

デフォルトの期間は 10 年です。

- [保存] をクリックします。

#### 結果

[証明書] 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確認します。 [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

- 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、[システム (System)] - [信頼 (Trust)] の順に選択します。
- [証明書 (Certificates)] タブをクリックします。
- 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。
- 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
```

#### 結果

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、サブスクリバとその証明書の状態のリストです。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] - [信頼] の順に選択します。
- 3 [CRLS] タブをクリックします。
- 4 [インポート] 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	<p>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。</p> <p>例：</p> <pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTENMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEhMBk G A1UEAxMSU1NMZW51IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDB a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCsq G SIb3DQEGBBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSV05CIyyS0tYscz8o07avwBxTiMpDEQg== -----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。

- 5 [保存] をクリックします。

#### 結果

インポートされた CRL がリンクとして表示されます。

## CSR の証明書のインポート

CSR に署名付き証明書をインポートできます。

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。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。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、クライアント ユーザーのセキュリティが低下します。



## 前提条件

証明書署名要求 (CSR) が使用可能かどうか確認します。「[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] - [信頼] の順に選択します。
- 3 [CSRS] タブをクリックします。
- 4 既存の証明書署名要求を選択します。
- 5 [アクション] をクリックし、ドロップダウン メニューから [CSR の証明書をインポート] を選択します。
- 6 コンピュータで署名付き証明書ファイルを検索し、ファイルを追加します。
- 7 [保存] をクリックします。

## 結果

[証明書] 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。

# 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 15-2. 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	set timezone <timezone>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node">https://&lt;nsx-mgr&gt;/api/v1/node</a>
NTP サーバを設定	set ntp-server <ntp-server>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp">https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp</a>
DNS サーバを設定	set name-servers <dns-server>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers">https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers</a>
DNS 検索ドメインを設定	set search-domains <domain>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains">https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains</a>

# コンピュート マネージャの追加

コンピュート マネージャは、vCenter Server のように、ホストや仮想マシンなどのリソースを管理するアプリケーションです。NSX-T は、コンピュート マネージャをポーリングし、ホストまたは仮想マシンの追加や削除などの変更を検出し、インベントリを更新します。

今回のリリースでは、この機能は次のものをサポートしています。

- vCenter Server バージョン 6.5 Update 1 と 6.5 GA のみ。

- vCenter Server との IPv6 または IPv4 による通信。
- 最大 5 個のコンピュート マネージャ。

#### 手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 ナビゲーション パネルから、[ファブリック (Fabric)] - [コンピュート マネージャ (Compute Managers)] の順に選択します。
- 3 [追加 (Add)] をクリックします。
- 4 コンピュート マネージャの詳細を設定します。

オプション	説明
名前と説明	vCenter Server を識別する名前を入力します。 必要に応じて、vCenter Server のクラスタ数などの詳細を入力します。
ドメイン名/IP アドレス	vCenter Server の IP アドレスを入力します。
タイプ	デフォルトのオプションを使用します。
ユーザー名とパスワード	vCenter Server ログイン認証情報を入力します。
サムプリント	vCenter Server SHA-256 サムプリント アルゴリズムの値を入力します。

サムプリント値を空白にすると、サーバのサムプリントを使用するように指示されます。

サムプリントを受け入れてから NSX-T が vCenter Server リソースを検出して登録するまで、数秒かかります。

- 5 進行状況アイコンが [処理中 (In progress)] から [未登録 (Not registered)] に変わった場合は、次の手順を実行してエラーを解決します。
  - a エラー メッセージを選択し、[解決 (Resolve)] をクリックします。次のようなエラー メッセージが表示される可能性があります：

```
Extension already registered at CM <vCenter Server name> with id <extension ID>
```

- b vCenter Server 認証情報を入力し、[解決 (Resolve)] をクリックします。  
すでに登録がされている場合には置き換えられます。

#### 結果

[コンピュート マネージャ] パネルに、コンピュート マネージャのリストが表示されます。マネージャの名前をクリックすると、マネージャの詳細を表示して編集できます。また、マネージャに適用するタグを管理できます。

## タグの管理

オブジェクトにタグを追加すると、より簡単に検索を行うことができます。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 つのオブジェクトに最大で 15 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

さまざまな条件を使用して、NSX-T インベントリ全体でオブジェクトを検索できます。

検索結果は関連性でソートされます。これらの結果は、検索クエリに基づいてフィルタリングできます。

**注：** 演算子としても機能する特殊文字を検索クエリで使用する場合には、先頭にバックスラッシュを追加する必要があります。演算子として機能する文字は、+、-、=、&&、||、<、>、!、(、)、{、}、[、]、^、"、`、?、:、/、\ 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 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 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	検索クエリ
名前またはプロパティに Logical を含むオブジェクト	Logical
正確な論理スイッチ名	display_name:LSP-301
! などの特殊文字を含む名前	Logical\!

検索結果には 10 個のオブジェクト タイプが表示されます。オブジェクト タイプごとに、上位 5 つの結果が表示されます。

- 4 検索結果ウィンドウで、下部にある [...の結果を表示 (View ... Results)] リンクをクリックすると、詳細検索ページが開き、検索を絞り込むことができます。
- 5 1 つ以上の条件を指定して、検索を絞り込みます。

- 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

## 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。

次の表では、NSX Manager でサポートされるホスト キーを優先順位の高いものから順番に示します。

表 15-3. 優先順にリストされた NSX Manager ホスト キー

NSX Manager でサポートされるホスト キー タイプ	キー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

### 手順

- 1 リモート サーバに root としてログインします。

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する方が安全です。

- 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 NSX Manager でサポートされるキーと使用可能なキーを比較します。

この例では、許容されるキーは ED25519 のみです。

#### 4 キーのフィンガープリントを取得します。

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64 | sed 's/./44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

## 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、データプレーンは影響を受けませんが、設定の変更はできません。

バックアップには次の 3 つのタイプがあります。

<b>クラスタのバックアップ</b>	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。
<b>ノードのバックアップ</b>	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。
<b>インベントリのバックアップ</b>	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。

<b>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</b>	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。
<b>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</b>	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。 <a href="#">自動バックアップのスケジュール設定</a> 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行うことが重要です。

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。

**注：** NSX Manager のバックアップおよびリストア時には、DNE Key Manager は含まれません。DNE Key Manager には、別のバックアップおよびリストアの手順が必要です。[DNE Key Manager のバックアップとリストア](#)を参照してください。

## 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

バックアップは、NSX Manager がアクセスできるファイル サーバに保存されます。バックアップを行う前に、このサーバの場所を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

バックアップは、NSX Manager がアクセスできるファイル サーバに保存されます。バックアップを行う前に、このサーバの場所を設定する必要があります。

### 前提条件

バックアップ ファイル サーバの SSH フィンガープリントを入手します。フィンガープリントとして使用できるのは、SHA256 ハッシュの ECDSA キーだけです。[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。

### 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 バックアップ ファイル 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 バックアップ ファイル 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。  
  
存在するディレクトリを使用してください。
- 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、ファイルをバックアップ ファイル 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 5 分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。

## 結果

**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 構成のリストア

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フレーズが必要です。

## 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 バックアップのリストア

バックアップをリストアすると、バックアップ時のネットワークの状態がリストアされます。NSX Manager で保守されている構成はリストアされますが、ノードの追加や削除など、バックアップの作成以降にファブリックに行われた変更は調整されます。

### 3 vCenter Server からの NSX-T の拡張機能の削除

コンピューティング マネージャを追加すると、NSX Manager はその ID を vCenter Server の拡張機能として追加します。この vCenter Server を NSX-T のインストールに登録しない場合は、vCenter Server の管理対象オブジェクト ブラウザ (MOB) を使用して拡張機能を削除できます。



## 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

- リストアに使用可能なバックアップを確認します。
- 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

バックアップをリストアします。

## バックアップのリストア

バックアップをリストアすると、バックアップ時のネットワークの状態がリストアされます。NSX Manager で保守されている構成はリストアされますが、ノードの追加や削除など、バックアップの作成以降にファブリックに行われた変更は調整されます。

### 前提条件

- バックアップ ファイル サーバの SSH フィンガープリントを入手します。フィンガープリントとして使用できるのは、SHA256 ハッシュの ECDSA キーだけです。[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。
- オブジェクトが設定されていない新規の NSX Manager インストールを使用していることを確認します。[NSX Manager のバックアップをリストアする準備](#)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)] - [ユーティリティ (Utilities)] の順に選択します。
- 3 [リストア (Restore)] タブをクリックします。
- 4 [編集 (Edit)] をクリックして、バックアップ ファイル サーバを構成します。
- 5 IP アドレスまたはホスト名を入力します。
- 6 必要に応じてポート番号を変更します。  
デフォルトは 22 です。
- 7 サーバへのログインで使用する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を絶対ディレクトリパスで入力します。
- 9 バックアップ データの暗号化で使したパスフレーズを入力します。
- 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。
- 11 [保存 (Save)] をクリックします。
- 12 バックアップを選択します。
- 13 [リストア (Restore)] をクリックします。

リストア操作のステータスが表示されます。バックアップの作成後にファブリック ノードまたはトランスポート ノードを削除または追加した場合には、ノードへのログインやスクリプトの実行など、特定の操作を実行するように指示されます。

リストア操作の完了後、リストアの完了画面が開き、復元の結果、バックアップ ファイルのタイムスタンプ、リストア操作の開始時間と終了時間が表示されます。リストアに失敗すると、エラーが発生した手順 (Current Step: Restoring Cluster (DB)、Current Step: Restoring Node など) が画面に表示されます。クラスタまたはノードのいずれか一方のリストアが失敗した場合、エラーは一時的なものである可能性があります。その場合、[再試行 (Retry)] をクリックする必要はありません。Manager を再開または再起動すると、リストアが続行します。

クラスタまたはノードのリストアを確認するには、次の CLI コマンドを実行してシステム ログ ファイルを表示し、クラスタのリストアに失敗しました、ノードのリストアに失敗しました という文字列を検索します。

```
get log-file syslog
```

Manager を再開するには、次の CLI コマンドを実行します。

```
restart service manager
```

Manager を再起動するには、次の CLI コマンドを実行します。

```
reboot
```

## 結果

**注：** バックアップ後にコンピューティング マネージャを追加した場合、リストア後にコンピューティング マネージャを再度追加すると、登録に失敗したことを示すエラー メッセージが表示されます。エラーを解決した後、コンピューティング マネージャを正常に追加できます。詳細については、[コンピュート マネージャの追加の手順 5](#) を参照してください。vCenter Server に保存されている NSX-T に関する情報を削除する場合は、[vCenter Server からの NSX-T の拡張機能の削除](#)の手順を実行します。

## vCenter Server からの NSX-T の拡張機能の削除

コンピューティング マネージャを追加すると、NSX Manager はその ID を vCenter Server の拡張機能として追加します。この vCenter Server を NSX-T のインストールに登録しない場合は、vCenter Server の管理対象オブジェクト ブラウザ (MOB) を使用して拡張機能を削除できます。

### 手順

- 1 vSphere Web Client に管理者としてログインします。
- 2 ESXi ホストを選択します。
- 3 [管理] - [設定] タブの順にクリックします。
- 4 メニューから [システムの詳細設定] を選択します。
- 5 [Config.HostAgent.plugins.solo.enableMob] オプションを有効にします。
- 6 MOB にログインします。
- 7 プロパティ テーブルの [コンテンツ] プロパティの値である、[コンテンツ] リンクをクリックします。
- 8 プロパティ テーブルの [extensionManager] プロパティの値である、[ExtensionManager] リンクをクリックします。
- 9 メソッド テーブルの [UnregisterExtension] リンクをクリックします。
- 10 [値] テキスト フィールドに **com.vmware.nsx.management.nsx** と入力します。
- 11 パラメータ テーブルの下ページの右側にある [メソッドの呼び出し] リンクをクリックします。  
メソッドの結果は **void** と表示されますが、拡張機能は削除されます。
- 12 拡張機能が削除されていることを確認するには、前のページの [FindExtension] メソッドをクリックし、拡張機能に同じ値を入力して呼び出します。  
結果は **void** となるはずです。

## 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、コントロール 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。

- 全クラスタを復元できない場合は、[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どうか確認します。変更されている場合には、バックアップからリストアします。

#### 前提条件

- バックアップが最新の状態であることを確認します。
- リストアを実行します。「[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 リストアを完了します。
- 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 クラスタを再展開します。

## DNE Key Manager のバックアップとリストア

DNE（分散ネットワーク暗号化）Key Manager には、独自のバックアップおよびリストア手順があります。NSX Manager をバックアップまたはリストアするときに、DNE Key Manager は含まれません。

### DNE Key Manager のバックアップ

DNE Key Manager をバックアップするには、次の CLI コマンドを実行します。

```
backup node file <filename> [passphrase <passphrase>]
```

ファイルを暗号化するためのパスフレーズを指定しなかった場合は、指定するように求められます。予防策として、次の CLI コマンドを使用して、リモートの場所にバックアップ ファイルをコピーすることができます。

```
copy file <filename> url <url>
```

### DNE Key Manager のリストア

リストアする前に、DNE Key Manager が NSX Manager に接続されていることを確認します。次の API 呼び出しを行って、現在の DNE Key Manager の ID を取得します。

```
GET https://<nsx-mgr>/api/v1/network-encryption/key-managers
```

ID が返された場合は、次の API 呼び出しを行って DNE Key Manager を削除します。

```
DELETE https://<nsx-mgr>/api/v1/network-encryption/key-managers/<key-manager-id>
```

次の CLI コマンドを実行して、リストアを実行します。

```
restore node file <filename> [passphrase <passphrase>]
```

パスフレーズには、バックアップ コマンドの実行時に使用したものを指定する必要があります。すべてのキー ポリシーのローテーションを行い、新たにリストアされた DNE Key Manager を管理プレーンに参加させるように求められます。詳細については、『NSX-T インストール ガイド』の「管理プレーンへの DNE Key Manager の参加」を参照してください。

## 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 制御プレーンの障害を回避するには、NSX Controller クラスタに、本番環境用の 3 台のメンバー ホストが必要です。1 台の物理ハイパーバイザー ホストで発生した障害による NSX 制御プレーンへの影響を回避するには、各コントローラを個別のハイパーバイザー ホスト（合計 3 台の物理ハイパーバイザー ホスト）に配置する必要があります。本番環境のワークロードを処理しないラボや事前検証 (POC) 環境の場合は、リソースを節約するために単一のコントローラで実行することもできます。

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 台のメンバーのうち 2 台がオンラインであれば、クラスタは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 台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。オンラインにできない場合は、置き換えることができます。「[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 台のメンバーのうち 1 台のみ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のいずれもオンラインにできない場合は、障害の発生した NSX Controller を置き換えるか、NSX Controller クラスタを再展開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 15-4. 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-768BB5FCAC7F) 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 3 つ以上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ったか、または何らかの理由で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 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。
  - b 管理プレーンに新しい NSX Controller を参加させます。
  - c コントロール 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、コントロール 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
```

## 結果

**注：** detach コマンドを使用して削除されたコントローラには、一部の設定情報が残っています。コントローラを再度コントローラ クラスタに参加させる場合は、コントローラ上で 次の CLI コマンドを実行し、古い情報を削除する必要があります。

```
deactivate control-cluster
```

## 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。

---

**注意：** 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。

## ログ収集システム メッセージ

ESXi で実行されているものを除くすべての NSX-T コンポーネントからのログ メッセージは、RFC 5424 で指定された Syslog 形式に準拠しています。ログ ファイルは、/var/log ディレクトリにあります。

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、監査ログをトリガします。

RFC 5424 は次の重要度レベルを定義します。

重要度	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
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、メッセージの種類を識別するものです。メッセージ ID のリストについては、[ログ メッセージ ID](#) 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。

- 重要度。可能な値 : 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。メッセージ ID は、メッセージの種類を識別します。ID は[ログ メッセージ ID](#)に記載されています。

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 ID

ログメッセージのメッセージ ID のフィールドは、メッセージの種類を識別します。`set logging-server` コマンドの `messageid` パラメータを使用して、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。

表 15-5. ログメッセージ ID

メッセージ ID	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
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

表 15-5. ログ メッセージ ID（続き）

メッセージ ID	例
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） 認識 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。スイッチとファイアウォールに IPFIX を設定できます。スイッチの場合、VIF（仮想インターフェイス）と pNIC（物理 NIC）でネットワーク フローがエクスポートされます。ファイアウォールの場合、分散ファイアウォール コンポーネントが管理するネットワーク フローがエクスポートされます。

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。

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 パケットが次の 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。
  - 内側のパケットを記述するいくつかのエンタープライズ エントリが含まれます。
- 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含む内部パケット 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。
  - 外側のパケットを説明するいくつかのエンタープライズ エントリが含まれます。

## 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 スイッチの IPFIX を設定するには、[スイッチの IPFIX コレクタ (Switch IPFIX 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 [保存 (Save)] をクリックします。

## スイッチの IPFIX プロファイルの設定

スイッチに IPFIX プロファイルを設定できます。

## 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 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 [スイッチの IPFIX プロファイル (Switch IPFIX Profiles)] タブをクリックします。
- 4 [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
名前と説明	名前を入力します。必要に応じて説明も入力します。
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バ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バ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。

設定	説明
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。

5 [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。

6 [保存 (Save)] をクリックします。

## ファイアウォールの IPFIX コレクタの設定

ファイアウォールに IPFIX コレクタを設定できます。

### 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 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 [ファイアウォールの IPFIX コレクタ (Firewall IPFIX Collectors)] タブをクリックします。
- 4 [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 4 個のコレクタを追加できます。
- 5 [保存 (Save)] をクリックします。

## ファイアウォールの IPFIX プロファイルの設定

ファイアウォールに IPFIX プロファイルを設定できます。

### 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 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 [ファイアウォールの IPFIX プロファイル (Firewall IPFIX Profiles)] タブをクリックします。
- 4 [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
名前と説明	名前を入力します。必要に応じて説明も入力します。
コレクタの設定	ドロップダウン リストからコレクタを選択します。
アクティブなフロー エクスポートのタイムアウト (分)	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 1 です。



設定	説明
優先順位	このパラメータは、論理プロファイルが複数の IPFIX プロファイルに対応している場合の競合を解決します。IPFIX エクスポートは、最も高い優先順位のプロファイルのみを使用します。小さい値ほど、優先順位が高くなります。
監視ドメイン ID	このパラメータは、ネットワーク フローの送信元の監視ドメインを特定します。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。

5 [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、論理スイッチ、NSGroup です。NSGroup を選択する場合、1 台以上の論理スイッチまたは論理ポートが含まれている必要があります。NSGroup に IP セットまたは MAC セットのみが含まれている場合は、無視されます。

6 [保存 (Save)] をクリックします。

## 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] - [トレースフロー] 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] を選択し、[ポート] 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] - [トレースフロー] 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	ターゲット情報を指定
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展開されている（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] 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	送信元のポートを入力します。	宛先の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	送信元のポートを入力します。	宛先の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] 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、観測タイプ（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。表示される観測記録に、フィルタとして [すべて]、[配信済み]、[ドロップ] を適用することができます。ドロップされた観測記録がある場合は、デフォルトで [ドロップ] フィルタが適用されます。ドロップされた観測記録がない場合は、[すべて] フィルタが適用されます。グラフィカル マップには、バックプレーンとルーター リンクが表示されます。ブリッジ情報は表示されません。

## 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する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。

ポートのステータスと統計情報が表示されます。

- 5 ホストが学習した MAC アドレスの CSV ファイルをダウンロードするには、[MAC テーブルをダウンロード (Download MAC Table)] をクリックします。

---

**注：** ホストが KVM の場合、MAC テーブルのダウンロードはサポートされていないため、エラー メッセージが表示されます。

---

## 6 ポート上のアクティビティを監視するには、[追跡を開始 (Begin Tracking)] クリックします。

ポート追跡ページが開きます。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。

### 結果

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witch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witch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に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 vNIC 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

### 結果

**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。

# 仮想マシンで実行中のアプリケーションのデータの表示

NS グループのメンバーである仮想マシンで実行されているアプリケーションの情報を表示できます。これは、テクニカル プレビュー機能です。

### 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 NS グループの名前をクリックします。
- 4 [アプリケーション] タブをクリックします。
- 5 [アプリケーション データの収集] をクリックします。

この処理には数分かかることがあります。処理が完了すると、次の情報が表示されます。

- プロセスの合計数。

- Web 層、データベース層、アプリケーション層などの階層を示す円。階層ごとのプロセス数も表示されます。

6 円をクリックすると、その階層のプロセスに関する詳細が表示されます。

## プリンシパル ID の表示

NSX Manager で管理されているプリンシパル ID を表示できます。

プリンシパルは、NSX-T コンポーネントまたは OpenStack 製品などのサードパーティ アプリケーションです。ID を作成すると、プリンシパルはこの ID を使用してオブジェクトを作成し、同じ ID のエンティティにのみオブジェクトの変更または削除を許可します。エンタープライズ管理者は、すべてのオブジェクトを変更または削除できます。プリンシパル名でオブジェクトを作成すると、警告が表示されます。操作を続行する前に、管理者が警告を了承する必要があります。

1 つのプリンシパルに複数の ID を作成できます。プリンシパル名とノード ID の組み合わせは一意にする必要があります。同じ名前を持つ異なる ID が、その名前で作成されたオブジェクトにアクセスできます。各 ID には、権限グループ `read_write_api_users`、`read_only_api_users` または `superusers` が関連付けられています。

プリンシパル ID を作成または削除するには、NSX-T API を使用する必要があります。詳細については、『NSX-T API リファレンス』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)] - [ユーザー (Users)] の順に選択します。
- 3 [プリンシパル ID (Principal Identities)] タブをクリックします。

## 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。

**注：** 以下の手順では、DNE Key Manager からサポート バンドルが収集されません。DNE Key Manager で CLI コマンドを実行し、サポート バンドルを収集する必要があります。次はその例です。

```
nsx-keymanager> get support-bundle file support-bundle.tgz
support-bundle-zyz created, use the following command to transfer the file:
copy file support-bundle.tgz url <url>
```

### 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。

---

**注：** 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。