

NSX-T Data Center 管理ガイド

変更日：2022 年 5 月 06 日
VMware NSX-T Data Center 2.5

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2022 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

VMware NSX-T Data Center の管理について 12

1 NSX Manager の概要 13

2 Tier-0 ゲートウェイ 16

- Tier-0 ゲートウェイの追加 16
- IP プレフィックス リストの作成 20
- コミュニティ リストの作成 21
- スタティック ルートの設定 22
- ルート マップの作成 23
- ルートマップの追加時に正規表現を使用したコミュニティ リストの照合 25
- BGP の設定 25
- BFD の設定 29
- IPv6 レイヤー 3 転送の設定 29
- IPv6 アドレス割り当て用の SLAAC および DAD プロファイルの作成 30

3 Tier-1 ゲートウェイ 32

- Tier-1 ゲートウェイの追加 32

4 セグメント 35

- セグメント プロファイル 35
 - QoS セグメント プロファイルの理解 36
 - IP アドレス検出セグメント プロファイルの理解 38
 - SpoofGuard セグメント プロファイルの理解 40
 - セグメント セキュリティのセグメント プロファイルの理解 42
 - MAC アドレス検出セグメント プロファイルの理解 43
- セグメントの追加 45

5 Virtual Private Network (VPN) 47

- IPsec VPN の理解 48
 - ポリシーベース IPsec VPN の使用 48
 - ルートベース IPsec VPN の使用 49
- レイヤー 2 VPN の理解 51
- VPN サービスの追加 52
 - IPsec VPN サービスの追加 53
 - L2 VPN サービスの追加 55
- IPsec VPN セッションの追加 57
 - ポリシーベース IPsec セッションの追加 57

ルートベース IPsec セッションの追加	61
サポートされているコンプライアンス スイートについて	64
TCP MSS クランプの理解	65
L2 VPN セッションの追加	66
L2 VPN サーバ セッションの追加	66
L2 VPN クライアント セッションの追加	68
リモート側の L2 VPN 構成ファイルのダウンロード	69
ローカル エンドポイントの追加	71
プロファイルの追加	72
IKE プロファイルの追加	72
IPsec プロファイルの追加	75
DPD プロファイルの追加	77
L2 VPN クライアントとしての自律 Edge の追加	78
IPsec VPN セッションの認識された状態の確認	80
VPN セッションの監視とトラブルシューティング	83

6 ネットワーク アドレス変換 85

ゲートウェイでの NAT の設定	85
------------------	----

7 ロード バランシング 87

キー ロード バランサの概念	88
ロード バランサ リソースの拡張	88
サポートされているロード バランサの機能	89
ロード バランサ トポロジ	90
ロード バランサ コンポーネントの設定	92
ロード バランサの追加	92
アクティブ モニターの追加	94
パッシブ モニターの追加	97
サーバ プールの追加	98
仮想サーバ コンポーネントの設定	102
サーバ プールと仮想サーバに作成されたグループ	124

8 転送ポリシー 126

転送ポリシーの追加または編集	127
----------------	-----

9 IP アドレス管理 (IPAM) 129

DNS ゾーンの追加	129
DNS フォワーダ サービスの追加	130
DHCP サーバの追加	131
Tier-0 または Tier-1 の DHCP リレー サーバの設定	132
IP アドレス プールの追加	133

IP アドレス ブロックの追加 134

10 セキュリティ 135

セキュリティ設定の概要 135

セキュリティに関する用語 136

Identity Firewall 136

Identity Firewall のワークフロー 137

レイヤー 7 コンテキスト プロファイル 139

レイヤー 7 ファイアウォール ルールのワークフロー 141

属性 142

分散ファイアウォール 146

ファイアウォール ドラフト 146

分散ファイアウォールの追加 148

分散ファイアウォール パケット ログ 152

デフォルトの接続方法の選択 154

ファイアウォール除外リストの管理 155

特定のドメインのフィルタリング (FQDN/URL) 156

物理ワークロードへのセキュリティ ポリシーの拡張 157

共有アドレス セット 164

East-West ネットワーク セキュリティ：サードパーティ サービスのチェーン 164

ネットワーク保護の主な概念 (East-West) 164

East-West トラフィックに関する NSX-T Data Center の要件 165

East-West ネットワーク セキュリティの手順 166

East-West トラフィックのイントロスペクション用サービスの展開 166

サービス プロファイルの追加 168

サービス チェーンの追加 168

East-West トラフィックのリダイレクト ルールの追加 169

ゲートウェイ ファイアウォールの設定 172

ゲートウェイ ファイアウォールのポリシーおよびルールの追加 172

North-South ネットワーク セキュリティ：サードパーティ サービスの挿入 175

North-South ネットワーク セキュリティの手順 175

North-South トラフィックのイントロスペクション用サービスの展開 175

トラフィックのリダイレクトを設定 178

North-South トラフィックへのリダイレクト ルールの追加 179

トラフィックのリダイレクトの監視 180

エンドポイントの保護 180

エンドポイント保護について 180

エンドポイントの保護の設定 184

エンドポイント保護の管理 200

セキュリティ プロファイル 212

セッション タイマーの作成 212

- フラッド防止 214
- DNS セキュリティの設定 216
- グループとプロファイルの優先順位の管理 217

11 インベントリ 219

- サービスの追加 219
- グループの追加 220
- コンテキスト プロファイルの追加 222

12 監視 224

- ファイアウォールの IPFIX プロファイルの追加 224
- スイッチの IPFIX プロファイルの追加 225
- IPFIX コレクタの追加 226
- ポート ミラーリング プロファイルの追加 227
- 簡易ネットワーク管理プロトコル (SNMP) 227
- vRealize Log Insight によるシステムの監視 228
- vRealize Operations Manager によるシステムの監視 229
- vRealize Network Insight Cloud によるシステムの監視 233
- 高度な監視ツール 243
 - ポート接続情報の表示 244
 - トレースフロー 244
 - ポート ミラーリング セッションの開始 247
 - ポート ミラーリング セッションのフィルタの設定 250
 - IPFIX の設定 251
 - 論理スイッチ ポート アクティビティの監視 421

13 論理スイッチ 422

- BUM フレーム レプリケーション モードの理解 423
- 論理スイッチの作成 424
- 論理スイッチへの仮想マシンの接続 426
 - vCenter Server 上でホストされた仮想マシンの NSX-T Data Center 論理スイッチへの接続 426
 - 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 Data Center 論理スイッチへの接続 428
 - KVM 上でホストされた仮想マシンの NSX-T Data Center 論理スイッチへの接続 433
- 論理スイッチ ポートの作成 434
- レイヤー 2 接続のテスト 435
- NSX Edge アップリンク用の VLAN 論理スイッチの作成 438
- 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 440
 - QoS スwitchング プロファイルの理解 441
 - ポート ミラーリング スwitchング プロファイルの理解 444
 - IP アドレス検出スswitchング プロファイルの理解 446
 - SpoofGuard の理解 448

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	451
MAC 管理スイッチング プロファイルの理解	453
カスタム プロファイルと論理スイッチの関連付け	454
論理ポートとカスタム プロファイルの関連付け	455
拡張ネットワーク スタック	456
ENS 論理コアの自動割り当て	456
ゲスト VLAN 間ルーティングの設定	457
レイヤー 2 ブリッジ	459
Edge ブリッジ プロファイルの作成	459
Edge ベースのブリッジの設定	460
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	463

14 分散論理ルーター 466

Tier-1 論理ルーター	466
Tier-1 論理ルーターの作成	468
Tier-1 論理ルーターへのダウンリンク ポートの追加	469
Tier-0 または Tier-1 論理ルーターへの VLAN ポートの追加	470
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	471
Tier-1 論理ルーターのスタティック ルートの設定	472
スタンドアローン Tier-1 論理ルーターの作成	474
Tier-0 論理ルーター	476
Tier-0 分散論理ルーターの作成	477
Tier-0 と Tier-1 の接続	478
NSX Edge アップリンク用の VLAN 論理スイッチへの Tier-0 論理ルーターの接続	481
ループバック ルーター ポートの追加	484
Tier-0 または Tier-1 論理ルーターへの VLAN ポートの追加	485
スタティック ルートの設定	485
BGP 構成オプション	489
Tier-0 分散論理ルーター上の BFD の設定	495
Tier-0 分散論理ルーターのルート再配分を有効にする	496
ECMP ルーティングの理解	499
IP プリフィックス リストの作成	503
コミュニティ リストの作成	504
ルート マップの作成	504
転送タイマーの設定	505

15 高度な NAT 507

ネットワーク アドレス変換	507
Tier-1 NAT	509
Tier-0 NAT	515
再帰 NAT	516

16 高度なグループ オブジェクト 519

- IP セットの作成 519
- IP アドレス プールの作成 520
- MAC セットの作成 520
- NSGroup の作成 521
- サービスとサービス グループの設定 523
 - NSService の作成 523
- 仮想マシンのタグの管理 524

17 高度な DHCP 525

- DHCP 525
 - DHCP サーバ プロファイルの作成 525
 - DHCP サーバの作成 526
 - 論理スイッチへの DHCP サーバの接続 527
 - 論理スイッチからの DHCP サーバの切り離し 527
 - DHCP リレー プロファイルの作成 527
 - DHCP リレー サービスの作成 528
 - 論理ルーター ポートへの DHCP リレー サービスの追加 528
 - DHCP リースの削除 529
- メタデータ プロキシ 529
 - メタデータ プロキシ サーバの追加 529
 - 論理スイッチへのメタデータ プロキシ サーバの接続 530
 - 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 530

18 高度な IP アドレス管理 532

- IP アドレス ブロックの管理 532
- IP アドレス ブロックのサブネットの管理 533

19 高度なロード バランシング 534

- キー ロード バランサの概念 535
- ロード バランサ コンポーネントの構成 535
 - ロード バランサの作成 536
 - アクティブ健全性モニターの構成 537
 - パッシブ健全性モニターの設定 540
 - ロード バランシング用サーバ プールの追加 541
 - 仮想サーバ コンポーネントの設定 545

20 高度なファイアウォール 566

- 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 566
- 論理スイッチのブリッジ ポートへのファイアウォールの構成 567
- 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 567

分散ファイアウォールの有効化と無効化	568
ファイアウォール ルール セクションの追加	568
ファイアウォール ルール セクションの削除	569
セクション ルールを有効または無効にする	570
セクション ログの有効化または無効化	570
ファイアウォール除外リストの設定	570
ファイアウォール ルールについて	571
ファイアウォール ルールの追加	572
ファイアウォール ルールの削除	574
デフォルトの分散ファイアウォール ルールの編集	575
ファイアウォール ルールの順序の変更	576
ファイアウォール ルールのフィルタ	576

21 運用管理 577

モニタリング ダッシュボードの表示	578
カテゴリごとのオブジェクトの使用量と容量の表示	580
設定変更の認識された状態の確認	582
オブジェクトの検索	586
オブジェクト属性によるフィルタリング	587
コンピュート マネージャの追加	587
Active Directory の追加	589
LDAP サーバの追加	590
Active Directory の同期	591
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	592
ユーザーのパスワードの管理	592
アプライアンスのパスワードのリセット	593
認証ポリシーの設定	595
vIDM ホストからの証明書サムプリントの取得	595
VMware Identity Manager Integration の設定	596
VMware Identity Manager 機能の検証	598
NSX Manager、vIDM、および関連コンポーネント間の時刻の同期	600
ロールベースのアクセス コントロール	601
ロールの割り当てまたはプリンシパル ID の追加	613
NSX Manager のバックアップとリストア	615
バックアップの構成	616
古いバックアップの削除	617
利用可能なバックアップのリスト	618
バックアップのリストア	619
アップグレード中のバックアップとリストア	621
vCenter Server からの NSX-T Data Center の拡張機能の削除	621
NSX Manager クラスターの管理	622

NSX Manager クラスタの構成および状態の表示	622
NSX Manager クラスタのシャットダウンとパワーオン	625
NSX Manager の再起動	625
NSX Manager の IP アドレスの変更	626
NSX Manager ノードのサイズ変更	627
vCenter Server での ESXi ホスト トランスポート ノードの追加と削除	628
NSX Edge クラスタでの NSX Edge トランスポート ノードの置き換え	629
NSX Manager ユーザー インターフェイスを使用した NSX Edge トランスポート ノードの置き換え	629
API を使用した NSX Edge トランスポート ノードの置き換え	630
vCenter Server が失われ、リカバリできない場合の NSX-T のリカバリ	631
NSX-T Data Center の複数サイトの展開	633
アプライアンスの設定	640
ライセンス キーの追加とライセンス使用レポートの生成	641
証明書の設定	642
証明書のインポート	642
証明書署名要求ファイルの作成	643
CA 証明書のインポート	644
自己署名証明書の作成	645
NSX Manager ノードまたは NSX Manager クラスタ仮想 IP の証明書の置き換え	646
証明書失効リストのインポート	646
証明書失効リストでの NSX Manager の設定	647
CSR の証明書のインポート	648
パブリック証明書とプライベート キーの保存	648
コンプライアンス ベースの設定	649
コンプライアンス状態レポートの表示	649
コンプライアンスの状態レポートのコード	650
ロード バランサのグローバル FIPS コンプライアンス モードの設定	652
サポート バンドルの収集	654
ログ メッセージとエラー コード	655
リモート ログの構成	657
ログ メッセージ ID	665
Syslog 問題のトラブルシューティング	666
アプライアンス仮想マシンでのシリアル ログの構成	667
カスタマー エクスペリエンス向上プログラム	667
カスタマー エクスペリエンス向上プログラム構成の編集	667
オブジェクトへのタグの追加	668
リモート サーバの SSH フィンガープリントの検索	670
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	670
外部ロード バランサの構成	671

22 NSX Cloud の使用 673

Cloud Service Manager のクイック ツアー	673
クラウド	674
システム	680
NSX Cloud 検疫ポリシーを使用した脅威の検出	682
NSX 強制モード の検疫ポリシー	683
Native Cloud 強制モード の検疫ポリシー	689
ホワイトリストへの仮想マシンの登録	689
NSX 強制モード	690
現在サポートされているワークロード仮想マシンのオペレーティング システム	691
NSX 強制モード の仮想マシンのオンボーディング	691
NSX 強制モード での仮想マシンの管理	700
Native Cloud 強制モード	701
Native Cloud 強制モード での仮想マシンの管理	701
NSX Cloud でサポートされる NSX-T Data Center の機能	705
NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化	706
ネイティブ クラウド サービスの使用	710
パブリック クラウドのサービス挿入	711
NSX 管理対象仮想マシンでの NAT の有効化	718
Syslog 転送の有効化	718
NSX 強制モードでの VPN の設定	719
よくある質問 (FAQ)	723

23 NSX Intelligence の使用 726

NSX Intelligence の使い方	726
NSX Intelligence ホーム ページのツアー	726
NSX Intelligence グラフィック要素について	729
NSX Intelligence のビューとフローについて	731
グループ ビューの操作	731
仮想マシン ビューの操作	736
トラフィック フローの操作	738
NSX Intelligence 推奨事項の操作	740
NSX Intelligence の推奨事項について	740
新しい NSX Intelligence の推奨事項の生成	740
生成された推奨事項の確認と発行	742
NSX Intelligence のバックアップとリストア	743
NSX Intelligence のバックアップの設定	744
NSX Intelligence のバックアップ	745
NSX Intelligence のバックアップのリストア	746
NSX Intelligence の問題のトラブルシューティング	747
NSX Intelligence アプライアンスの状態の確認	747
NSX Intelligence サポート バンドルの収集	751

VMware NSX-T Data Center の管理について

『NSX-T Data Center 管理ガイド』には、VMware NSX-T™ Data Center 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。NSX Cloud の設定方法についても記載されています。

対象読者

この情報は、NSX-T Data Center 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、<https://www.vmware.com/topics/glossary> を参照してください。

NSX Manager の概要

1

NSX Manager には、NSX-T 環境を管理できる Web ベースのユーザー インターフェイスが用意されています。API 呼び出しを処理する API サーバもホストします。

NSX Manager の Web インターフェイスでは、リソースを設定する方法が 2 つあります。

- ポリシー インターフェイス：[ネットワーク]、[セキュリティ]、[インベントリ]、[プランとトラブルシューティング] タブ。
- 詳細設定インターフェイス：[ネットワークとセキュリティの詳細設定] タブ。

ポリシー インターフェイスと詳細設定インターフェイスの使用する条件

使用するユーザー インターフェイスは、常に同じ基準で決める必要があります。使用できるユーザー インターフェイスが限定される場合もあります。

- NSX-T Data Center 2.4 以降で新しい環境を展開する場合、ほとんどの状況では、新しいポリシーベースのユーザー インターフェイスのほうが環境の作成と管理に適しています。
 - ポリシーベースのユーザー インターフェイスでは一部の機能が使用できません。これらの機能が必要な場合は、すべての構成で詳細設定ユーザー インターフェイスを使用します。
- NSX-T Data Center 2.4 以降にアップグレードする場合は、引き続き [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで設定の変更を行う必要があります。

表 1-1. ポリシー インターフェイスと詳細設定インターフェイスの使用する条件


ポリシー インターフェイス	詳細設定インターフェイス
新しい環境の場合は、ポリシーベースのインターフェイスを使用します。	詳細設定インターフェイスで作成した環境。たとえば、ポリシーベースのインターフェイスよりも前のバージョンからアップグレードした場合。
NSX Cloud 環境	他のプラグインと統合する環境。たとえば、NSX Container Plugin、Openstack などのクラウド管理プラットフォーム。

表 1-1. ポリシー インターフェイスと詳細設定インターフェイスの使用する条件（続き）

ポリシー インターフェイス	詳細設定インターフェイス
<p>ポリシー インターフェイスでのみ使用可能なネットワーク機能：</p> <ul style="list-style-type: none"> ■ DNS サービスと DNS ゾーン ■ VPN ■ NSX Cloud の転送ポリシー 	<p>詳細設定インターフェイスでのみ使用可能なネットワーク機能：</p> <ul style="list-style-type: none"> ■ 転送タイマー ■ ネクストホップとして BFD とインターフェイスを持つスタティック ルート ■ メタデータ プロキシ ■ 隔離されたセグメントに接続された DHCP サーバと静的割り当て
<p>ポリシー インターフェイスでのみ使用可能なセキュリティ機能：</p> <ul style="list-style-type: none"> ■ エンドポイントの保護 ■ ネットワーク イントロスペクション（East-West サービス挿入） ■ コンテキスト プロファイル <ul style="list-style-type: none"> ■ L7 アプリケーション ■ FQDN ■ 新しい分散ファイアウォールとゲートウェイ ファイアウォールのレイアウト <ul style="list-style-type: none"> ■ カテゴリ ■ 自動サービス ルール ■ ドラフト 	<p>詳細設定インターフェイスでのみ使用可能なセキュリティ機能：</p> <ul style="list-style-type: none"> ■ CPU およびメモリしきい値 ■ ブリッジ ファイアウォール ■ 送信元と宛先の IP に基づく分散ファイアウォール ルール

ポリシー インターフェイスの使用

ポリシー インターフェイスを使用する場合は、このインターフェイスですべてのオブジェクトを作成します。詳細設定インターフェイスでオブジェクトを作成しないでください。

詳細設定インターフェイスでは、ポリシー インターフェイスで作成したオブジェクトを変更できます。ポリシーで作成されたオブジェクトの設定には、[詳細構成] のリンクが含まれる場合があります。このリンクをクリックすると、詳細設定インターフェイスが開き、構成の微調整を行うことができます。ポリシーで作成されたオブジェクトを詳細設定インターフェイスで直接表示することもできます。ポリシーで管理されている設定は、詳細設定インターフェイスに表示できますが、その横に  アイコンが表示されます。詳細設定ユーザー インターフェイスで変更を行うことはできません。

ポリシー インターフェイスと詳細設定インターフェイスの場所

ポリシーベースのインターフェイスと詳細設定インターフェイスは、NSX Manager ユーザー インターフェイスの異なる部分に表示され、異なる API URI を使用します。

表 1-2. ポリシー インターフェイスと詳細設定インターフェイス

ポリシー インターフェイス	詳細設定インターフェイス
<ul style="list-style-type: none"> ■ [ネットワーク] タブ ■ [セキュリティ] タブ ■ [インベントリ] タブ ■ [プランとトラブルシューティング] タブ 	[ネットワークとセキュリティの詳細設定] タブ
/policy/api で始まる API URI	/api で始まる API URI

注： [システム] タブは、すべての環境で使用されます。Edge ノード、Edge クラスタまたはトランスポート ゾーンを変更する場合、その変更がポリシー ベースのユーザー インターフェイスに表示されるまでに最大で 5 分ほどかかることがあります。POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload を使用すると、すぐに同期できます。

ポリシー API の使用方法については、[NSX-T Policy API スタート ガイド](#)を参照してください。

ポリシー インターフェイスと詳細設定インターフェイスで作成されたオブジェクトの名前

使用するインターフェイスによって、作成されるオブジェクトの名前が異なります。

表 1-3. オブジェクト名

ポリシー インターフェイスで作成されたオブジェクト	詳細設定インターフェイスで作成されたオブジェクト
セグメント	論理スイッチ
Tier-1 ゲートウェイ	Tier-1 論理ルーター
Tier-0 ゲートウェイ	Tier-0 論理ルーター
グループ	NSGroup、IP セット、MAC セット
セキュリティ ポリシー	ファイアウォール セクション
ルール	ファイアウォール ルール
ゲートウェイ ファイアウォール	Edge ファイアウォール

Tier-0 ゲートウェイ

2

Tier-0 ゲートウェイは、Tier-0 論理ルーターの機能を実行します。また、論理ネットワークと物理ネットワーク間のトラフィックを処理します。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

Edge ノードは、1 つの Tier-0 ゲートウェイまたは論理ルーターのみをサポートします。Tier-0 ゲートウェイまたは論理ルーターを作成する場合は、NSX Edge クラスターの Edge ノードの数以上の Tier-0 ゲートウェイまたは論理ルーターを作成しないようにしてください。

注： [ネットワークとセキュリティの詳細設定] タブでは、Tier-0 論理ルーターという用語で Tier-0 ゲートウェイを表しています。

この章には、次のトピックが含まれています。

- Tier-0 ゲートウェイの追加
- IP プレフィックス リストの作成
- コミュニティ リストの作成
- スタティック ルートの設定
- ルート マップの作成
- ルートマップの追加時に正規表現を使用したコミュニティ リストの照合
- BGP の設定
- BFD の設定
- IPv6 レイヤー 3 転送の設定
- IPv6 アドレス割り当て用の SLAAC および DAD プロファイルの作成

Tier-0 ゲートウェイの追加

Tier-0 ゲートウェイには、Tier-1 ゲートウェイとのダウンリンク接続と物理ネットワークとのアップリンク接続があります。

アクティブ/アクティブまたはアクティブ/スタンバイになるように、Tier-0 ゲートウェイの HA（高可用性）モードを設定できます。次のサービスは、アクティブ/スタンバイ モードでのみサポートされます。

- NAT
- ロード バランシング
- ステートフル ファイアウォール
- VPN

Tier-0 および Tier-1 ゲートウェイでは、単一層およびマルチティア トポロジの両方で、すべてのインターフェイス（アップリンク、サービス ポート、およびダウンリンク）に対して次のようなアドレス設定がサポートされます。

- IPv4 のみ
- IPv6 のみ
- デュアル スタック - IPv4 と IPv6 の両方

IPv6 またはデュアル スタック アドレス設定を使用するには、[ネットワーク] - [ネットワーク設定] - [グローバル ネットワーク構成] で、[IPv4 と IPv6] を L3 転送モードとして有効にします。

Tier-0 ゲートウェイのルート再配分を設定する場合、2 つの送信元グループ（Tier-0 サブネットとアドバタイズされた Tier-1 サブネット）から選択できます。Tier-0 サブネット グループの送信元は次のとおりです。

送信元のタイプ	説明
接続されたインターフェイスとセグメント	これには、外部インターフェイス サブネット、サービス インターフェイス サブネット、Tier-0 に接続されたセグメント サブネットが含まれます。
スタティック ルート	Tier-0 ゲートウェイに設定したスタティック ルート。
NAT IP	Tier-0 ゲートウェイによって所有され、Tier-0 ゲートウェイに設定された NAT ルールから検出された NAT IP アドレス。
IPsec のローカル IP	VPN セッションの確立に使用されるローカル IPSEC エンドポイント IP アドレス。
DNS フォワーダの IP	クライアントからの DNS クエリのリスナー IP。DNS クエリをアップストリーム DNS サーバに転送するために使用される送信元 IP としても使用されます。

アドバタイズされた Tier-1 サブネット グループの送信元は次のとおりです。

送信元のタイプ	説明
接続されたインターフェイスとセグメント	これには、Tier-1 ゲートウェイに接続されたセグメント サブネット、Tier-1 ゲートウェイに設定されたサービス インターフェイス サブネットが含まれます。
スタティック ルート	Tier-1 ゲートウェイに設定したスタティック ルート。
NAT IP	Tier-1 ゲートウェイによって所有され、Tier-1 ゲートウェイに設定された NAT ルールから検出された NAT IP アドレス。
LB VIP	ロード バランシング仮想サーバの IP アドレス。
LB SNAT IP	ロード バランサによって送信元 NAT に使用される IP アドレスまたは IP アドレスの範囲。
DNS フォワーダの IP	クライアントからの DNS クエリのリスナー IP。DNS クエリをアップストリーム DNS サーバに転送するために使用される送信元 IP としても使用されます。
IPsec ローカル エンドポイント	IPsec ローカル エンドポイントの IP アドレス。

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 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 [Tier-0 ゲートウェイの追加] をクリックします。
- 4 ゲートウェイの名前を入力します。
- 5 HA（高可用性）モードを選択します。

デフォルトのモードは、アクティブ/アクティブです。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。

重要： ゲートウェイを作成した後に HA モードを変更することはできません。

- 6 HA モードがアクティブ/スタンバイの場合は、フェイルオーバー モードを選択します。

オプション	説明
プリエンプティブ	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。
非プリエンプティブ	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) NSX Edge クラスタを選択します。
- 8 (オプション) 1 つ以上のタグを追加します。
- 9 (オプション) [追加設定] をクリックします。
 - a [内部中継サブネット] フィールドに、サブネットを入力します。

これは、このゲートウェイ内のコンポーネント間の通信に使用されるサブネットです。デフォルトは 169.254.0.0/28 です。
 - b [T0-T1 中継サブネット] フィールドに、1 つ以上のサブネットを入力します。

これらのサブネットは、このゲートウェイとそれにリンクしているすべての Tier-1 ゲートウェイ間の通信に使用されます。このゲートウェイを作成して、Tier-1 ゲートウェイをリンクすると、Tier-0 ゲートウェイ側と Tier-1 ゲートウェイ側のリンクには実際の IP アドレスが割り当てられます。[Tier-0 ゲートウェイ] 画面と [Tier-1 ゲートウェイ] 画面で、[追加設定] - [ルーター リンク] の順に移動すると、このアドレスを確認できます。デフォルトは 100.64.0.0/16 です。
 - c IPv6 アドレスの設定で [ND プロファイル] と [DAD プロファイル] を選択します。

これらのプロファイルは、IPv6 アドレスのステートレス アドレス自動構成 (SLAAC) と重複アドレス検出 (DAD) の設定で使用されます。デフォルトのプロファイルが作成されます。
- 10 [保存] をクリックします。

- 11 ルート再配分を構成するには、[ルート再配分] および [設定] をクリックします。

送信元を 1 つ以上選択します。

- Tier-0 サブネット：[スタティック ルート]、[NAT IP]、[IPsec のローカル IP]、[DNS フォワーダの IP]、[接続されたインターフェイスとセグメント]。

[接続されたインターフェイスとセグメント] では、[サービス インターフェイスのサブネット]、[外部インターフェイスのサブネット]、[ループバック インターフェイスのサブネット]、[接続されたセグメント] の 1 つ以上の項目を選択できます。

- アドバタイズされた Tier-1 サブネット：[DNS フォワーダの IP]、[スタティック ルート]、[LB VIP]、[NAT IP]、[LB SNAT IP]、[IPsec ローカル エンドポイント]、[接続されたインターフェイスとセグメント]。

[接続されたインターフェイスとセグメント] では、[サービス インターフェイスのサブネット] または [接続されたセグメント] を選択できます。

- 12 インターフェイスを構成するには、[インターフェイス] および [設定] をクリックします。

- a [インターフェイスの追加] をクリックします。

- b 名前を入力します。

- c タイプを選択します。

HA モードがアクティブ/スタンバイの場合、選択できるのは [外部]、[サービス]、[ループバック] です。HA モードがアクティブ/アクティブの場合は、[外部] または [ループバック] を選択できます。

- d IP アドレスを CIDR 形式で入力します。

- e セグメントを選択します。

- f インターフェイス タイプが [サービス] でない場合は、NSX Edge ノードを選択します。

- g (オプション) インターフェイス タイプが [ループバック] でない場合は、MTU 値を入力します。

- h (オプション) タグを追加して ND プロファイルを選択します。

- 13 (オプション) HA モードがアクティブ/スタンバイの場合は、[HA VIP 構成] の横にある [設定] をクリックして、HA VIP を構成します。

HA VIP が設定されている場合、1 つのアップリンクが切断されていても、Tier-0 ゲートウェイは動作します。物理ルーターは HA VIP とのみ通信します。HA VIP は、BGP ではなくスタティック ルートで機能するように設計されています。

- a [HA VIP 構成の追加] をクリックします。

- b IP アドレスとサブネット マスクを入力します。

HA VIP サブネットは、割り当て先のインターフェイスのサブネットと同じにする必要があります。

- c 2 つの異なる Edge ノードから 2 つのインターフェイスを選択します。

- 14 [ルーティング] をクリックして、IP プリフィックス リスト、コミュニティ リスト、スタティック ルート、およびルート マップを追加します。

- 15 [BGP] をクリックして BGP を構成します。

16 [高度な設定] をクリックして、[ネットワークとセキュリティの詳細設定] - [ルーター] 画面の順に移動し、追加構成を行います。

- a レイヤー 3 転送モードを構成するには、[グローバル構成] タブをクリックします。
- b [編集] をクリックします。
- c [IPv4] または [IPv4 と IPv6] を選択します。

デフォルトは IPv4 のみです。IPv6 のみはサポートされません。IPv6 を有効にするには、[IPv4 と IPv6] を選択します。

- d [保存] をクリックします。

IP プレフィックス リストの作成

IP プレフィックス 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 プレフィックス 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 プレフィックス 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。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レフィックス リストを作成する際は、特定のネットワーク アドレスを指定しない IP プレフィックス（ドロップダウン リストから [任意] を選択）を作成し、それ以外のすべてのルートを許可するには、[許可] アクションを作成します。

前提条件

Tier-0 ゲートウェイ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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン（3 つのドット）をクリックして [編集] を選択します。
- 4 [ルーティング] をクリックします。
- 5 [IP プレフィックス リスト] の横にある [設定] をクリックします。
- 6 [IP プレフィックス リストの追加] をクリックします。
- 7 IP プレフィックス リストの名前を入力します。
- 8 [設定] をクリックして IP プレフィックスを追加します。

- 9 [プレフィックスの追加] をクリックします。
 - a IP アドレスを CIDR 形式で入力します。
例 : 192.168.100.3/27。
 - b (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。
 - c 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。
 - d [追加] をクリックします。
- 10 追加のプレフィックスを指定するには、前の手順を繰り返します。
- 11 [保存] をクリックします。

コミュニティ リストの作成

コミュニティ リストに基づいたルート マップを設定できるように、BGP コミュニティ リストを作成できます。

コミュニティ リストは、コミュニティ属性値を含むユーザー定義リストです。これらのリストは、BGP 更新メッセージのコミュニティ属性を照合または操作するために使用できます。

BGP コミュニティ属性 (RFC 1997) と BGP ラージ コミュニティ属性 (RFC 8092) の両方がサポートされています。BGP コミュニティ属性は、2 つの 16 ビット値に分割された 32 ビットの値です。BGP のラージ コミュニティ属性には、それぞれ 4 オクテットの 3 つのコンポーネントがあります。

ルート マップでは、BGP コミュニティまたはラージ コミュニティ属性に一致または設定できます。この機能を使用すると、ネットワーク オペレーターは BGP コミュニティ属性に基づいてネットワーク ポリシーを実装できます。

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 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン (3 つのドット) をクリックして [編集] を選択します。
- 4 [ルーティング] をクリックします。
- 5 [コミュニティ リスト] の横にある [設定] をクリックします。
- 6 [コミュニティ リストの追加] をクリックします。
- 7 コミュニティ リストの名前を入力します。

- 8 コミュニティのリストを指定します。標準コミュニティの場合は、aa:nn 形式を使用します（例：300:500）。ラージコミュニティの場合は、aa:bb:cc の形式を使用します（例：11:22:33）。通常のコミュニティと大規模なコミュニティの両方をリストに入れることはできません。通常のコミュニティのみ、または大規模なコミュニティのみを含める必要があります。

さらに、次の正規表現から 1 つ以上を選択できます。リストにラージ コミュニティが含まれている場合、これらを追加できません。

- NO_EXPORT_SUBCONFED：EBGP ピアにアドバタイズしません。
- NO_ADVERTISE：どのピアにもアドバタイズしません。
- 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。

- 9 [保存] をクリックします。

スタティック ルートの設定

Tier-0 ゲートウェイ上に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に、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 ゲートウェイには、接続された Tier-0 ゲートウェイ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。

再帰的なスタティック ルートがサポートされています。

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 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン（3 つのドット）をクリックして [編集] を選択します。
- 4 [ルーティング] をクリックします。
- 5 [スタティック ルート] の横にある [設定] をクリックします。
- 6 [スタティック ルートの追加] をクリックします。
- 7 名前およびネットワーク アドレスを CIDR 形式で入力します。IPv6 ベースのスタティック ルートがサポートされています。IPv6 プリフィックスに指定できるのは、IPv6 ネクスト ホップのみです。
- 8 [ネクスト ホップの設定] をクリックして、ネクスト ホップの情報を追加します。
- 9 [ネクスト ホップの追加] をクリックします。
- 10 IP アドレスを入力します。
- 11 アドミニストレーティブ ディスタンスを指定します。
- 12 ドロップダウン リストからインターフェイスを選択します。
- 13 [追加] ボタンをクリックします。

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。

ルート マップの作成

ルート マップは、IP プレフィックス 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。一致が見つかり、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 レベルとルートの再配分で参照することができます。

前提条件

- IP プレフィックス リストまたはコミュニティ リストが設定されていることを確認します。[IP プレフィックス リストの作成](#)または[コミュニティ リストの作成](#)を参照してください。
- 正規表現を使用してコミュニティ リストのルートマップ一致基準を定義する方法については、[ルートマップの追加時に正規表現を使用したコミュニティ リストの照合](#)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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン（3 つのドット）をクリックして [編集] を選択します。
- 4 [ルーティング] をクリックします。
- 5 [ルート マップ] の横にある [設定] をクリックします。
- 6 [ルート マップの追加] をクリックします。
- 7 名前を入力し、[設定] をクリックして一致の基準を追加します。
- 8 [一致の基準を追加] をクリックして、1 つ以上の一致基準を追加します。

9 各基準について、[IP プレフィックス] または [コミュニティ リスト] を選択して、[設定] をクリックして1つ以上の一致式を指定します。

a [コミュニティ リスト] を選択した場合は、コミュニティ リストのメンバーの照合方法を定義する一致式を指定します。コミュニティ リストごとに、次の一致オプションを使用できます。

- [いずれかに一致]：コミュニティ リストのコミュニティのいずれかに一致している場合に、ルート マップで設定アクションを実行します。
- [すべてに一致]：順序に関係なく、コミュニティ リストのすべてのコミュニティに一致している場合に、ルート マップで設定アクションを実行します。
- [完全に一致]：コミュニティ リストのすべてのコミュニティとその順序が一致している場合に、ルート マップで設定アクションを実行します。
- [コミュニティの正規表現と一致]：NRLI に関連付けられたすべての標準コミュニティが正規表現に一致している場合に、ルート マップで設定アクションを実行します。
- [ラージ コミュニティの正規表現と一致]：NRLI に関連付けられたすべてのラージ コミュニティが正規表現に一致している場合に、ルート マップで設定アクションを実行します。

標準コミュニティとルートを照合するには、一致条件 `MATCH_COMMUNITY_REGEX` を使用します。ルートとラージ コミュニティを照合するには、一致基準の `MATCH_LARGE_COMMUNITY_REGEX` を使用します。標準コミュニティまたはラージ コミュニティのいずれかの値を含むルートを許可する場合は、2つの一致基準を作成する必要があります。一致式が同じ一致基準に指定されている場合、標準コミュニティとラージ コミュニティの両方を含むルートのみが許可されます。

一致基準が1つの場合、一致式に AND 演算子が適用されます。この場合、すべての一致式を満たした場合に一致とみなされます。複数の一致基準がある場合は、OR 演算が適用されます。この場合、いずれかの一致基準を満たした場合に一致とみなされます。

10 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	<p>コミュニティのリストを指定します。標準コミュニティの場合は、aa:nn 形式を使用します（例：300:500）。ラージ コミュニティの場合は、aa:bb:cc の形式を使用します（例：11:22:33）。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。</p> <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED：EBGP ピアにアドバタイズしません。 ■ NO_ADVERTISE：どのピアにもアドバタイズしません。 ■ 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。
ローカル プリファレンス	この値は、外部の BGP 送信パスを選択する場合に使用します。値が最も高いパスが優先されます。

11 [アクション] 列で、[許可] または [拒否] を選択します。

IP プレフィックス リストまたはコミュニティ リストに一致する IP アドレスのアドバタイズを許可または拒否できます。

12 [保存] をクリックします。

ルートマップの追加時に正規表現を使用したコミュニティ リストの照合

正規表現を使用して、コミュニティ リストのルートマップの一致条件を定義できます。BGP 正規表現は、POSIX 1003.2 の正規表現に基づいています。

次の式は、POSIX 正規表現のサブセットです。

式	説明
.	任意の 1 文字に一致します。
*	0 回以上のパターンの出現に一致します。
+	1 回以上のパターンの出現に一致します。
?	パターンの 0 個または 1 回の出現と一致します。
^	行の先頭に一致します。
\$	行の末尾に一致します。
—	BGP 正規表現では、この文字には特別な意味があります。これは、スペース、カンマ、AS セットの区切り文字 ({ と })、コンフェデレーションの区切り文字 ((と)) と一致します。また、行の先頭と行の末尾にも一致します。したがって、この文字は AS 値の境界が一致する場合に使用できます。この文字は、技術的には (^[,{}()])\$ と評価されます。

次に、ルート マップで正規表現を使用する場合の例を示します。

式	説明
^101	101 で始まるコミュニティ属性を持つルートと一致します。
^[0-9]+	0 から 9 の数字で始まるコミュニティ属性を持ち、このような数字が 1 個以上連続するルートと一致します。
.*	任意のコミュニティ属性を持つルートか、コミュニティ属性のないルートと一致します。
.+	任意のコミュニティ値を持つルートに一致します。
^\$	コミュニティの値がないか null のルートを一致します。

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 ゲートウェイと物理インフラストラクチャ内のルーター間に外部または内部 BGP (eBGP または iBGP) 接続を設定します。

BGP を設定する場合は、Tier-0 ゲートウェイにローカル自律システム (AS) 番号を設定する必要があります。また、リモート AS 番号を設定する必要があります。EBGP ネイバーは、Tier-0 アップリンクと同じサブネットに直接接続している必要があります。同じサブネット内にない場合は、BGP マルチホップを使用する必要があります。

BGPv6 は、単一ホップおよびマルチホップでサポートされています。BGPv6 ネイバーは、IPv6 アドレスのみをサポートします。再配分、プリフィックス リスト、およびルート マップは、IPv6 プリフィックスでサポートされています。

アクティブ/アクティブ モードの Tier-0 ゲートウェイは、サービス ルーター間の iBGP をサポートしています。ゲートウェイ 1 が North バウンズの物理ルーターと通信できない場合、トラフィックはアクティブ/アクティブ クラスタ内のゲートウェイ 2 に再ルーティングされます。ゲートウェイ 2 が物理ルーターと通信できる場合、ゲートウェイ 1 と物理ルーター間のトラフィックは影響を受けません。

NSX Edge での ECMP の実装は、プロトコル番号、送信元アドレスと宛先アドレス、送信元ポートと宛先ポートの 5-tuple に基づいています。

iBGP 機能には次の機能と制限があります。

- 再配分、プリフィックス リスト、およびルート マップがサポートされます。
- ルート リフレクタはサポートされません。
- BGP コンフェデレーション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>>) に管理者権限でログインします。

2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。

3 Tier-0 ゲートウェイを編集するには、メニュー アイコン (3 つのドット) をクリックして [編集] を選択します。

4 [BGP] をクリックします。

a ローカル AS 番号を入力します。

アクティブ/アクティブ モードの場合、デフォルトの ASN 値 (65000) がすでに入力されています。アクティブ/スタンバイ モードの場合、デフォルトの ASN の値はありません。

b [BGP] 切り替えボタンをクリックして、BGP を有効または無効にします。

アクティブ/アクティブ モードの場合、[BGP] がデフォルトで有効になります。アクティブ/スタンバイ モードの場合、[BGP] がデフォルトで無効になります。

c このゲートウェイがアクティブ/アクティブ モードの場合は、[サービス ルーター間の iBGP] 切り替えボタンをクリックしてサービス ルーター間の iBGP を有効または無効にします。デフォルトでは有効になっています。

ゲートウェイがアクティブ/スタンバイ モードの場合、この機能は使用できません。

d [ECMP] 切り替えボタンをクリックして ECMP を有効または無効にします。

- e [Multipath Relax] 切り替えボタンをクリックして、AS パスの属性値のみが異なり、AS パスの長さは同じである複数のパス間の負荷分散を有効または無効にします。

注： [Multipath Relax] を機能させるには、[ECMP] を有効にする必要があります。

- f [グレースフル リスタート] フィールドで、[無効]、[ヘルパーのみ] または [グレースフル リスタートとヘルパー] を選択します。

必要に応じて、[グレースフル リスタート タイマー] と [グレースフル リスタート失効タイマー] を変更します。

デフォルトでは、グレースフル リスタート モードは [ヘルパーのみ] に設定されています。ヘルパー モードは、グレースフル リスタートが可能なネイバーから学習したルートに関連付けられているトラフィックの中断を軽減するのに便利です。再起動の実行中、ネイバーはフォワーディング テーブルを維持している必要があります。

すべてのゲートウェイの BGP ピアリングが常にアクティブになっているため、Tier-0 ゲートウェイでグレースフル リスタート機能を有効にすることは推奨しません。グレースフル リスタート機能を有効にすると、フェイルオーバー時に、リモート ネイバーが代替 Tier-0 ゲートウェイを選択するまでに時間がかかります。このため、BFD ベースのコンバージェンスが遅延します。

注：ネイバー固有の設定でオーバーライドされない限り、Tier-0 の設定がすべての BGP ネイバーに適用されます。

5 IP アドレスのプリフィックスを追加して、[ルートの集約] を設定します。

- a [プリフィックスの追加] をクリックします。
- b IP アドレスのプリフィックスを CIDR 形式で入力します。
- c [サマリのみ] オプションで [はい] または [いいえ] を選択します。

6 [保存] をクリックします。

BGP ネイバーを設定する前に、グローバル BGP の設定を保存する必要があります。

7 [BGP ネイバー] を設定します。

- a ネイバーの IP アドレスを入力します。
- b [BFD] を有効または無効にします。
- c [リモート AS の番号] に値を入力します。

iBGP の場合は、手順 4a と同じ AS 番号を入力します。eBGP の場合は、物理ルーターの AS 番号を入力します。

- d [出力フィルタ] で値を設定します。
- e [入力フィルタ] で値を設定します。

- f [Allowas-in] 機能を有効または無効にします。

この機能は、デフォルトで無効になっています。この機能が有効な場合、BGP ネイバーは同じ AS を持つルートを受信できます。たとえば、同じサービス プロバイダを使用して 2 つの場所が相互接続されている場合などが該当します。この機能はすべてのアドレス ファミリに適用されます。特定のアドレス ファミリに適用することはできません。

- g [送信元アドレス] フィールドでは、送信元アドレスを選択して、この特定の送信元アドレスを使用したネイバーとのピアリング セッションを確立できます。何も選択しない場合、ゲートウェイは自動的に 1 つを選択します。
- h [IP アドレス ファミリ] フィールドで、[IPv4]、[IPv6] または [無効] を選択します。
- i [ホップの上限] に値を入力します。
- j [グレースフル リスタート] フィールドで、[無効]、[ヘルパーのみ] または [グレースフル リスタートとヘルパー] を選択できます。

オプション	説明
未選択	このネイバーのグレースフル リスタートは、Tier-0 ゲートウェイの BGP 設定に従います。
[無効]	<ul style="list-style-type: none"> ■ Tier-0 ゲートウェイの BGP が [無効] に設定されている場合、このネイバーのグレースフル リスタートは無効になります。 ■ Tier-0 ゲートウェイの BGP が [ヘルパーのみ] に設定されている場合、このネイバーのグレースフル リスタートは無効になります。 ■ Tier-0 ゲートウェイの BGP が [グレースフル リスタートとヘルパー] に設定されている場合、このネイバーのグレースフル リスタートは無効になります。
[ヘルパーのみ]	<ul style="list-style-type: none"> ■ Tier-0 ゲートウェイの BGP が [無効] に設定されている場合、このネイバーのグレースフル リスタートは「ヘルパーのみ」に設定されます。 ■ Tier-0 ゲートウェイの BGP が [ヘルパーのみ] に設定されている場合、このネイバーのグレースフル リスタートは「ヘルパーのみ」に設定されます。 ■ Tier-0 ゲートウェイの BGP が [グレースフル リスタートとヘルパー] に設定されている場合、このネイバーのグレースフル リスタートは「ヘルパーのみ」に設定されます。
[グレースフル リスタートとヘルパー]	<ul style="list-style-type: none"> ■ Tier-0 ゲートウェイの BGP が [無効] に設定されている場合、このネイバーのグレースフル リスタートは「グレースフル リスタートとヘルパー」に設定されます。 ■ Tier-0 ゲートウェイの BGP が [ヘルパーのみ] に設定されている場合、このネイバーのグレースフル リスタートは「グレースフル リスタートとヘルパー」に設定されます。 ■ Tier-0 ゲートウェイの BGP が [グレースフル リスタートとヘルパー] に設定されている場合、このネイバーのグレースフル リスタートは「グレースフル リスタートとヘルパー」に設定されます。

- k [タイマーとパスワード] をクリックします。

- l [BFD の間隔] に値を入力します。

単位はミリ秒です。仮想マシンで実行されている Edge ノードの場合、最小値は 1,000 です。ベアメタル Edge ノードの場合、最小値は 300 です。

- m [BFD の乗数] に値を入力します。

- n [ホールド ダウン時間] に値を入力します。

- o [キープ アライブ時間] に値を入力します。
 - p パスワードを入力します。
- BGP ピア間の MD5 認証を設定する場合、必須となります。

8 [保存] をクリックします。

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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン (3 つのドット) をクリックして [編集] を選択します。
- 4 [詳細設定] をクリックします。

これにより、[ネットワークとセキュリティの詳細設定] - [ルータ] 画面が表示されます。論理ルーターの 1 つとしてゲートウェイが表示されます。[Tier-0 分散論理ルーター上の BFD の設定](#) に示す手順を行います。

IPv6 レイヤー 3 転送の設定

IPv4 レイヤー 3 転送はデフォルトで有効になっています。IPv6 レイヤー 3 転送を設定することもできます。

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 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
 - 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン (3 つのドット) をクリックして [編集] を選択します。
 - 4 [高度な設定] をクリックします。
- これにより、[ネットワークとセキュリティの詳細設定] - [ルータ] 画面が表示されます。論理ルーターの 1 つとしてゲートウェイが表示されます。
- 5 [グローバル構成] タブをクリックします。
 - 6 [L3 転送モード] フィールドで、[IPv4 と IPv6] を選択します。
- IPv6 のみはサポートされません。
- 7 [ネットワーク] タブに移動して、ゲートウェイを再度編集します。

8 [詳細設定] に移動します。

- a [内部中継サブネット] に構成可能な IPv6 アドレスはありません。システムは IPv6 リンク ローカル アドレスを自動的に使用します。
- b [T0-T1 中継サブネット] に IPv6 サブネットを入力します。

9 [インターフェイス] に移動して、IPv6 のインターフェイスを追加します。

IPv6 アドレス割り当て用の SLAAC および DAD プロファイルの作成

論理ルーター インターフェイスで IPv6 を使用する場合、IP アドレスの割り当てにステートレス アドレスの自動設定 (SLAAC) を設定できます。SLAAC では、ルーターのアドバタイズを介して、ローカル ネットワーク ルーターからアドバタイズされたネットワーク プリフィックスに基づいてホストのアドレス指定を行います。重複アドレス検出 (DAD) により、IP アドレスの一意性が保証されます。

前提条件

[ネットワークとセキュリティの詳細設定] - [ルーター] - [グローバル設定] の順に移動し、[L3 転送モード] に **IPv4** と **IPv6** を選択します。

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 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 Tier-0 ゲートウェイを編集するには、メニュー アイコン (3 つのドット) をクリックして [編集] を選択します。
- 4 [追加設定] をクリックします。
- 5 [ND プロファイル] (SLAAC プロファイル) を作成するには、メニュー アイコン (3 つのドット) をクリックして、[新規作成] を選択します。
 - a プロファイルの名前を入力します。
 - b モードを選択します。
 - [無効] : ルーター アドバタイズ メッセージが無効になります。
 - [SLAAC (RA を介した DNS)] : ルーター アドバタイズ メッセージを使用して、アドレスと DNS 情報が生成されます。
 - [SLAAC (DHCP を介した DNS)] : ルーター アドバタイズ メッセージを使用してアドレスが生成され、DHCP サーバにより DNS 情報が生成されます。
 - [DHCP (DHCP を介したアドレスと DNS)] : DHCP サーバによってアドレスと DNS 情報が生成されます。
 - [SLAAC (DHCP を介したアドレスと DNS)] : アドレスと DNS 情報が DHCP サーバによって生成されます。このオプションは NSX Edge のみでサポートされます。KVM ホストまたは ESXi ホストではサポートされません。

- c ルーター アドバタイズ メッセージの到達可能時間と再転送間隔を入力します。
 - d ドメイン名を入力し、ドメイン名の有効期間を指定します。これらの値は **SLAAC (RA を介した DNS)** モードの場合にのみ入力してください。
 - e DNS サーバを入力し、DNS サーバの有効期間を指定します。これらの値は **SLAAC (RA を介した DNS)** モードの場合にのみ入力してください。
 - f ルーター アドバタイズの値を入力します。
 - [RA の間隔] : 連続するルーター アドバタイズ メッセージの送信間隔。
 - [ホップ制限] : アドバタイズされたルートの有効期間。
 - [ルーターの有効期間] : ルーターの有効期間。
 - [プリフィックスの有効期限] : プリフィックスの有効期間 (秒)。
 - [プリフィックスの優先時間] : 有効なアドレスが優先される時間。
- 6 [DAD プロファイル] を作成するには、メニュー アイコン (3 つのドット) をクリックして、[新規作成] を選択します。
- a プロファイルの名前を入力します。
 - b モードを選択します。
 - [Loose] : 重複アドレスの通知は受信しますが、検出された重複アドレスに対して何も行いません。
 - [Strict] : 重複アドレスの通知を受信します。重複アドレスは使用不能になります。
 - c [待機時間 (秒)] に、NS パケット間の間隔を指定します。
 - d [待機時間 (秒)] で定義された間隔で、重複アドレスの検出に使用する NS パケットの数を [NS 再試行回数] に入力します。

Tier-1 ゲートウェイ

3

Tier-1 ゲートウェイは Tier-1 論理ルーターの機能を実行します。セグメントにはダウンリンク接続され、Tier-0 ゲートウェイにはアップリンク接続されています。

注： [ネットワークとセキュリティの詳細設定] タブでは、Tier-1 ゲートウェイを表す用語として、Tier-1 論理ルーターが使用されています。

Tier-1 ゲートウェイのルート アドバタイズおよびスタティック ルートを設定できます。再帰的なスタティック ルートがサポートされています。

この章には、次のトピックが含まれています。

- Tier-1 ゲートウェイの追加

Tier-1 ゲートウェイの追加

Tier-1 ゲートウェイは通常、North バウンドの Tier-0 ゲートウェイと、South バウンドのセグメントに接続されています。

Tier-0 および Tier-1 ゲートウェイでは、単一層およびマルチティア トポロジの両方で、すべてのインターフェイス（アップリンク、サービス ポート、およびダウンリンク）に対して次のようなアドレス設定がサポートされます。

- IPv4 のみ
- IPv6 のみ
- デュアル スタック - IPv4 と IPv6 の両方

IPv6 またはデュアル スタック アドレス設定を使用するには、[ネットワーク] - [ネットワーク設定] - [グローバル ネットワーク構成] で、[IPv4 と IPv6] を L3 転送モードとして有効にします。

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 [ネットワーク] - [Tier-1 ゲートウェイ] の順に選択します。
- 3 [Tier-1 ゲートウェイの追加] をクリックします。
- 4 ゲートウェイの名前を入力します。
- 5 （オプション）マルチティア トポロジを作成するには、この Tier-1 ゲートウェイに接続する Tier-0 ゲートウェイを選択します。

6 フェイルオーバー モードを選択します。

オプション	説明
プリエンプティブ	優先 NSX Edge ノードで障害が発生し、リカバリした場合は、この優先ノードがピアを先取りして、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。
非プリエンプティブ	優先 NSX Edge ノードで障害が発生し、リカバリした場合は、ピアがアクティブ ノードかどうかを確認されます。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。デフォルトのオプションです。

7 (オプション) この Tier-1 ゲートウェイでステートフル サービス (NAT、ロード バランサまたはファイアウォール) をホストする場合は、NSX Edge クラスタを選択します。

NSX Edge クラスタを選択すると、(ステートフル サービスを設定していなくても) サービス ルーターが常に作成され、North-South トラフィック パターンに影響します。

8 (オプション) NSX Edge ノードを選択します。

9 (オプション) [スタンバイの再配置を有効にする] 切り替えボタンをクリックして、スタンバイの再配置を有効または無効にします。

スタンバイの再配置とは、アクティブまたはスタンバイ状態の論理ルーターが稼動している Edge ノードに障害が発生した場合に、別の Edge ノード上に新しいスタンバイ論理ルーターを作成し、高可用性を維持することを意味します。アクティブな論理ルーターが実行されている Edge ノードで障害が発生した場合、元のスタンバイ論理ルーターがアクティブになり、新しいスタンバイ論理ルーターが作成されます。スタンバイ論理ルーターが実行されている Edge ノードで障害が発生した場合は、このルーターが新しいスタンバイ論理ルーターに置き換わります。

10 [保存] をクリックします。

11 (オプション) [ルート アドバタイズ] をクリックします。

次から 1 つ以上を選択します。

- [すべてのスタティック ルート]
- [すべての NAT IP アドレス]
- [すべての DNS フォワーダのルート]
- [すべてのロード バランサ VIP ルート]
- [接続されているすべてのセグメントおよびサービス ポート]
- [すべてのロード バランサ SNAT IP ルート]
- [すべての IPsec ローカル エンドポイント]

[ルート アドバタイズ ルールの設定] フィールドで [設定] をクリックして、ルート アドバタイズ ルールを追加します。

- 12 (オプション) [サービス インターフェイス] をクリックし、[設定] をクリックしてセグメントの接続を構成します。VLAN によってバックアップされるセグメントやワンアームロード バランシングなど、一部のトポロジで必要になります。
- a [インターフェイスの追加] をクリックします。
 - b 名前および IP アドレスを CIDR 形式で入力します。
 - c セグメントを選択します。
 - d [MTU] フィールドに 64 ~ 9,000 までの値を入力します。
 - e [ND プロファイル] フィールドで、プロファイルを選択します。
 - f [保存] をクリックします。
- 13 (オプション) [スタティック ルート] をクリックし、[設定] をクリックしてスタティック ルートを構成します。
- a [スタティック ルートの追加] をクリックします。
 - b 名前とネットワーク アドレスを入力します。アドレスには CIDR または IPv6 CIDR 形式を使用します。
 - c [ネクスト ホップの設定] をクリックして、ネクスト ホップ情報を追加します。
 - d [保存] をクリックします。

セグメント

4

セグメントは論理スイッチの機能を実行します。

注： [ネットワークとセキュリティの詳細設定] タブでは、セグメントを表す用語として、論理スイッチが使用されています。

この章には、次のトピックが含まれています。

- セグメント プロファイル
- セグメントの追加

セグメント プロファイル

セグメント プロファイルには、セグメントとセグメント 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セグメント プロファイルをサポートします。

次のタイプのセグメント プロファイルを使用できます。

- QoS（サービス品質）
- IP 検出
- SpoofGuard
- セグメント セキュリティ
- MAC アドレス管理

注： デフォルトのセグメント プロファイルの編集や削除はできません。デフォルトのセグメント プロファイルと別の設定が必要な場合は、カスタム セグメント プロファイルを作成します。デフォルトでは、セグメント セキュリティ プロファイルを除くすべてのカスタム セグメント プロファイルは、対応するデフォルト セグメント プロファイルの設定を継承します。たとえば、デフォルトでは、カスタムの IP 検出セグメント プロファイルの設定はデフォルトの IP 検出セグメント プロファイルと同じになります。

デフォルト セグメント プロファイルやカスタム セグメント プロファイルには、それぞれ一意の ID があります。この ID を使用して、セグメント プロファイルをセグメントまたはセグメント ポートと関連付けます。

1 個のセグメントまたはセグメント ポートは、各タイプの 1 個のセグメント プロファイルのみと関連付けることができます。たとえば、2 個の QoS セグメント プロファイルを 1 個のセグメントまたはセグメント ポートと関連付けることはできません。

セグメントの作成時にセグメント プロファイルに関連付けない場合は、NSX Manager によって対応するデフォルトのシステム定義セグメント プロファイルが関連付けられます。子セグメント ポートは、システム定義のデフォルト セグメント プロファイルを親セグメントから継承します。

セグメントやセグメント ポートを作成または更新するときに、デフォルト セグメント プロファイルまたはカスタム セグメント プロファイルに関連付けできます。セグメント プロファイルをセグメントと関連付けたり、関連付けを解除したりすると、次の基準に従って、子セグメント ポート用のセグメント プロファイルが適用されます。

- 親セグメントにプロファイルが関連付けられている場合、子セグメント ポートはその親からセグメント プロファイルを継承します。
- 親セグメントにセグメントプロファイルが関連付けられていない場合、デフォルト セグメント プロファイルがセグメントに割り当てられ、セグメント ポートはそのデフォルト セグメント 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セグメント 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セグメント プロファイルをオーバーライドします。

注： カスタム セグメント プロファイルをセグメントと関連付けたが、子セグメント ポートのうち 1 つに対してデフォルト セグメント プロファイルを維持する場合は、デフォルト セグメント プロファイルのコピーを作成し、それを特定のセグメント ポートと関連付ける必要があります。

セグメントやセグメント ポートと関連付けられているカスタム セグメント プロファイルを削除することはできません。セグメントやセグメント ポートがカスタム セグメント 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 ビューの割り当て先のセクションで、リストされているセグメントおよびセグメント ポートをクリックします。

QoS セグメント 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 のサービス クラス (CoS) は、トラフィックが輻輳によりセグメント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 Data Center は、仮想マシンによって、またはセグメント 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。ピーク帯域幅の速度はセグメント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セグメントに適用され、子のセグメント ポートに継承されます。

QoS セグメント プロファイルの作成

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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [セグメント] - [セグメント プロファイル] の順に選択します。
- 3 [セグメント プロファイルの追加] をクリックして、[QoS] を選択します。
- 4 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	プロファイルの名前です。
モード	<p>[モード] ドロップダウン メニューから [信頼する] または [信頼しない] のいずれかのオプションを選択します。</p> <p>「信頼する」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。「信頼する」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>「信頼しない」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。「信頼しない」モードの DSCP 値の範囲は 0 ～ 63 です。</p> <p>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。</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>

オプション	説明
サービス 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 (Ingress)	<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ます。バースト サイズは、ピーク帯域幅の期間に基づいて設定されます。バースト サイズの設定でバースト期間を設定します。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に、平均、ピーク、バースト サイズの設定を使用できます。</p> <p>たとえば、平均帯域幅が 30 Mbps、ピーク帯域幅が 60 Mbps、許可された期間が 0.1 秒の場合、バースト サイズは $60 * 1,000,000 * 0.10/8 = 750,000$ バイトになります。</p> <p>デフォルト値は 0 で、入力方向トラフィックのレート制限を無効にします。</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>たとえば、論理スイッチの平均帯域幅が 3,000 Kbps、ピーク帯域幅が 6,000 Kbps、許可された期間が 0.1 秒の場合、バースト サイズは $6,000 * 1,000 * 0.10/8 = 75,000$ バイトになります。</p> <p>デフォルト値は 0 で、入力方向ブロードキャスト トラフィックのレート制限を無効にします。</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、出力方向トラフィックのレート制限を無効にします。</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、デフォルト値が使用されます。

5 [保存] をクリックします。

IP アドレス検出セグメント プロファイルの理解

IP アドレス検出では、DHCP と DHCPv6 スヌーピング、ARP (Address Resolution Protocol) スヌーピング、ネイバー検出 (ND) スヌーピング、および仮想マシン ツールを使用して、MAC および IP アドレスを学習します。

注： デフォルトの IP 検出セグメント プロファイルでは、IPv6 の IP 検出方法が無効になっています。セグメントで IPv6 の IP 検出を有効にするには、IPv6 オプションを有効にして IP 検出プロファイルを作成し、そのプロファイルをセグメントに適用する必要があります。また、分散ファイアウォールにより、すべてのワークロード間で IPv6 ネイバー検出パケットが許可されることを確認します（デフォルトでは許可されています）。

検出された MAC アドレスおよび IP アドレスは、ARP/ND を抑制して、同じセグメントに接続されている仮想マシン間のトラフィックを最小にするために使用されます。また、このアドレスは、SpoofGuard および分散ファイアウォール (DFW) のコンポーネントでも使用可能です。DFW はアドレス割り当てを使用し、ファイアウォール ルール内のオブジェクトの IP アドレスを決定します。

DHCP/DHCPv6 スヌーピングは、DHCP/DHCPv6 クライアントとサーバ間で交換された DHCP/DHCPv6 パケットを検査し、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 (Gratuitous ARP) パケットを検査し、IP アドレスと MAC アドレスを学習します。

仮想マシン ツールは、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 アドレスおよび IP または IPv6 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。

ND スヌーピングは ARP スヌーピングに相当する IPv6 です。Neighbor Solicitation (NS) と Neighbor Advertisement (NA) メッセージを検査し、IP アドレスと MAC アドレスを学習します。

重複アドレス検出は、新しく検出された IP アドレスが別のポートの認識済みの割り当てリストにすでに含まれているかどうかを確認します。このチェックは、同じセグメント上のポートに実行されます。アドレスの重複が検出されると、新しく検出されたアドレスは認識済みの割り当てリストではなく、検出リストに追加されます。重複するすべての IP アドレスは検出タイムスタンプに関連付けられます。除外する割り当てリストに追加したり、またはスヌーピングを無効にしたりして、認識済みの割り当てリスト内の IP アドレスが削除されると、最も古いタイムスタンプの重複 IP アドレスが認識済みの割り当てリストに移動します。重複するアドレス情報は API 呼び出しを介して使用できます。

デフォルトでは、ARP スヌーピングと ND スヌーピングの検出方法は、初回使用時に信頼する (TOFU) と呼ばれるモードで動作します。TOFU モードでは、アドレスが検出され、認識済みの割り当てリストに追加されると、その割り当ては認識済みのリストに永久に残ります。TOFU は、ARP/ND スヌーピングを使用して検出された最初の n 個の固有の <IP, MAC, VLAN> の割り当てに適用されます。n は、設定可能な割り当て制限です。ARP/ND スヌーピングの TOFU を無効にすることができます。これは、毎回使用時に信頼する (TOEU) モードで動作します。TOEU モードの場合、アドレスが検出されると、そのアドレスは認識済みの割り当てリストに追加されます。アドレスが削除されるか期限切れになると、認識済みの割り当てリストから削除されます。DHCP スヌーピングと仮想マシン ツールは常に TOEU モードで動作します。

注： TOFU は、SpoofGuard と同じではありません。SpoofGuard と同じ方法でトラフィックをブロックしません。詳細については、『[SpoofGuard セグメント プロファイルの理解](#)』を参照してください。

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。

各ポートでは、NSX Manager は、ポートに割り当てられない IP アドレスが含まれる、除外する割り当てリストを保持します。[ネットワークとセキュリティの詳細設定] - [スイッチング] - [ポート] の順に移動してポートを選択することで、検出された割り当てを除外する割り当てリストに追加できます。また、既存の検出済みまたは認識済みの割り当てを削除するには、[除外する割り当て] にコピーします。

IP 検出セグメント プロファイルの作成

NSX-T Data Center には、いくつかのデフォルトの IP 検出スイッチング プロファイルがあります。追加の IP 検出スイッチング プロファイルを作成することもできます。

前提条件

IP 検出スイッチング プロファイルの概念について理解しておく必要があります。[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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [セグメント] - [セグメント プロファイル] の順に選択します。
- 3 [セグメント プロファイルの追加] をクリックして、[IP 検出] を選択します。
- 4 IP 検出スイッチング プロファイルの詳細を指定します。

オプション	説明
名前	名前を入力します。
ARP スヌーピング	IPv4 環境用。仮想マシンに固定 IP アドレスが設定されている場合に適用できます。
ARP 割り当て制限	ポートに割り当てられる IPv4 IP アドレスの最大数。許容されている最小値は 1（デフォルト）、最大値は 256 です。
ARP ND 割り当て制限のタイムアウト	TOFU が無効になっている場合に、ARP/ND 割り当てテーブル内の IP アドレスがタイムアウトになる時間の値（分単位）。アドレスがタイムアウトになった場合は、新たに検出されたアドレスで置き換えられます。
DHCP スヌーピング	IPv4 環境用。仮想マシンに IPv4 アドレスが設定されている場合に適用できます。
DHCP V6 スヌーピング	IPv6 環境用。仮想マシンに IPv6 アドレスが設定されている場合に適用できます。
仮想マシン ツール	ESXi ホストの仮想マシン専用。
IPv6 の仮想マシン ツール	ESXi ホストの仮想マシン専用。
ネイバー検出 (ND) スヌーピング	IPv6 環境用。仮想マシンに固定 IP アドレスが設定されている場合に適用できます。
ネイバー検出割り当ての制限	ポートに割り当てられる IPv6 IP アドレスの最大数。
初回使用時に信頼する	ARP スヌーピングおよび ND スヌーピングに適用できます。
重複 IP アドレスの検出	すべてのスヌーピング方法と IPv4 と IPv6 の両方の環境に使用します。

- 5 [保存] をクリックします。

SpoofGuard セグメント プロファイルの理解

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 のセグメントアドレス 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 はポートまたはセグメント レベルで設定することができます。SpoofGuard を導入環境で使用するのにはいくつかの理由があります。

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

NSX-T Data Center 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 検査は、すべて ARP/GARP/ND ペイロードにマッピングする MAC ソース、IP ソースおよび IP-MAC ソース に対するものです。

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

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

トラフィックをセグメントに送信するには、ポート レベルとセグメント 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 レベルとセグメントレベルの SpoofGuard を有効または無効にするには、SpoofGuard のセグメント プロファイルを使用します。

SpoofGuard セグメント プロファイルの作成

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/セグメント 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。

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 [ネットワーク] - [セグメント] - [セグメント プロファイル] の順に選択します。
- 3 [セグメント プロファイルの追加] をクリックして、[SpoofGuard] を選択します。
- 4 名前を入力します。
- 5 ポート レベルの SpoofGuard を有効にするには、[ポート割り当て] を [有効] に設定します。
- 6 [保存] をクリックします。

セグメント セキュリティのセグメント プロファイルの理解

セグメント 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、セグメント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。セグメント 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、セグメントの整合性を保護することができます。

デフォルトのセグメント セキュリティ プロファイルでは、DHCP 設定 Server Block と Server Block - IPv6 が有効になっています。つまり、デフォルトのセグメント セキュリティ プロファイルを使用するセグメントは、DHCP サーバから DHCP クライアントへのトラフィックをブロックします。セグメントで DHCP サーバのトラフィックを許可する場合は、セグメントにカスタム セグメント セキュリティ プロファイルを作成する必要があります。

セグメント セキュリティ セグメント プロファイルの作成

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セグメント セキュリティ セグメント 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

セグメント セキュリティ セグメント 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [セグメント] - [セグメント プロファイル] の順に選択します。
- 3 [セグメント プロファイルの追加] をクリックして、[セグメント セキュリティ] を選択します。
- 4 セグメント セキュリティ プロファイルの詳細を入力します。

オプション	説明
名前	プロファイルの名前です。
BPDU フィルタ	[BPDU フィルタ] ボタンを切り替えて BPDU フィルタを有効にします。デフォルトは無効です。 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。

オプション	説明
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。このリストから選択できるようにするには、[BPDU フィルタ] を有効にする必要があります。
DHCP フィルタ	<p>[サーバ ブロック] ボタンおよび [クライアント ブロック] ボタンを切り替えて、DHCP フィルタを有効にします。どちらもデフォルトは無効です。</p> <p>DHCP サーバのブロックにより、DHCP サーバから DHCP クライアントへのトラフィックがブロックされます。DHCP サーバから DHCP リレー エージェントへのトラフィックはブロックされないことに注意してください。</p> <p>DHCP クライアントのブロックでは DHCP 要求がブロックされるため、仮想マシンによる DHCP IP アドレスの取得を防止できます。</p>
DHCPv6 フィルタ	<p>[サーバ ブロック - IPv6] ボタンおよび [クライアント ブロック - IPv6] ボタンを切り替えて、DHCP フィルタを有効にします。どちらもデフォルトは無効です。</p> <p>DHCPv6 サーバのブロックにより、DHCPv6 サーバから DHCPv6 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。UDP 送信元ポート番号が 547 のパケットがフィルタされます。</p> <p>DHCPv6 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。UDP 送信元ポート番号が 546 のパケットがフィルタされます。</p>
非 IP トラフィックをブロック	<p>[非 IP トラフィックをブロック] ボタンを切り替えて、IPv4、IPv6、ARP および BPDU トラフィックのみを許可します。</p> <p>それ以外のトラフィックはブロックされます。IPv4、IPv6、ARP、GARP および BPDU トラフィックは、アドレスの割り当ておよび SpoofGuard に設定されたその他のポリシーに基づいて許可されます。</p> <p>デフォルトではこのオプションは無効で、非 IP トラフィックは通常のトラフィックとして処理されます。</p>
RA ガード	入力方向の IPv6 ルーター アドバタイズを除外するには、[RA ガード] ボタンを切り替えます。ICMPv6 タイプ 134 パケットが除外されます。このオプションはデフォルトで有効です。
レート制限	<p>ブロードキャスト トラフィックとマルチキャスト トラフィックのレート制限を設定します。このオプションはデフォルトで有効です。</p> <p>レート制限は、ブロードキャストの大量発生などのイベントから論理スイッチや仮想マシンを保護するために使用できます。</p> <p>接続の問題を回避するため、レートの制限の最小値は 10 pps 以上にする必要があります。</p>

5 [保存] をクリックします。

MAC アドレス検出セグメント プロファイルの理解

MAC 管理セグメント 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は、ESXi 仮想マシンの vNIC がセグメント ポートに接続する際に、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。この期間は設定できません。[MAC アドレス学習のエイジング時間] には、事前定義の値 (600) が表示されます。

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

学習可能な MAC アドレスの数は設定可能です。最大値は 4,096 で、これがデフォルトです。また、制限に達したときのポリシーを設定することもできます。次のオプションがあります。

- [ドロップ]: 不明な送信元 MAC アドレスからのパケットをドロップします。この MAC アドレスへの受信パケットは、不明なユニキャストとして扱われます。ポートは、不明なユニキャストのフラッドが有効になっている場合にのみ、パケットを受信します。
- [許可]: アドレスは学習されませんが、不明な送信元 MAC アドレスからのパケットは転送されます。この MAC アドレスへの受信パケットは、不明なユニキャストとして扱われます。ポートは、不明なユニキャストのフラッドが有効になっている場合にのみ、パケットを受信します。

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

MAC アドレス検出セグメント プロファイルの作成

MAC アドレス検出セグメント プロファイルを作成して、MAC アドレスを管理できます。

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 [ネットワーク] - [セグメント] - [セグメント プロファイル] の順に選択します。
- 3 [セグメント プロファイルの追加] をクリックして、[MAC アドレス検出] を選択します。
- 4 MAC アドレス検出の詳細を入力します。

オプション	説明
名前	プロファイルの名前です。
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。デフォルトは無効です。
MAC ラーニング	MAC 学習機能を有効または無効にします。デフォルトは無効です。
MAC の制限ポリシー	[許可] または [ドロップ] を選択します。デフォルトは [許可] です。MAC ラーニングを有効にする場合は、このオプションを使用できます。

オプション	説明
不明なユニキャスト フラッディング	不明なユニキャスト フラッディング機能を有効または無効にします。デフォルトは有効です。MAC ラーニングを有効にする場合は、このオプションを使用できます。
MAC の制限	MAC アドレスの最大数を設定します。デフォルトは 4096 です。MAC ラーニングを有効にする場合は、このオプションを使用できます。
MAC アドレス学習のエイジング時間	参考情報。このオプションは設定できません。事前定義の値は 600 です。

- 5 [保存] をクリックします。

セグメントの追加

セグメントはゲートウェイおよび仮想マシンに接続されます。セグメントは論理スイッチの機能を実行します。

仮想マシンの VIF ID の検索については、[論理スイッチへの仮想マシンの接続](#)を参照してください。

注： 拡張データ パス モードに設定されている N-VDS スイッチは、IP 検出、SpoofGuard、IPFIX のプロファイルをサポートします。

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 [ネットワーク] - [セグメント] の順に選択します。
- 3 [セグメント の追加] をクリックします。
- 4 セグメントの名前を入力します。
- 5 接続しているゲートウェイを選択します。

既存の Tier-0 または Tier-1 ゲートウェイを選択するか、[なし] を選択することができます。デフォルト値は [なし] です。これは、セグメントが論理スイッチであることを意味します。サブネットが設定されている場合は、Tier-0 または Tier-1 ゲートウェイにリンクできます。

- 6 接続しているゲートウェイが Tier-1 ゲートウェイである場合は、タイプ（[フレキシブル] または [固定]）を選択します。

フレキシブルなセグメントは、ゲートウェイからリンク解除できます。固定セグメントは、削除することはできませんが、ゲートウェイからリンクを解除することはできません。

- 7 サブネットを指定するには、[サブネットの設定] を設定をクリックします。
- 8 トランスポート ゾーン（オーバーレイまたは VLAN）を選択します。
- 9 トランスポート ゾーンのタイプが VLAN の場合は、VLAN ID のリストを指定します。
- 10 レイヤー 2 VPN を使用してセグメントを拡張する場合は、[L2 VPN] テキスト ボックスをクリックして、L2 VPN サーバまたはクライアント セッションを選択します。

複数選択が可能です。

- 11 [VPN トンネル ID] で、セグメントの識別に使用する一意の値を入力します。
- 12 [保存] をクリックします。

13 セグメント ポートを追加するには、表示されたプロンプトで [はい] をクリックして、セグメントの設定を続行します。

- a [ポート] と [設定] をクリックします。
- b [セグメント ポートを追加] をクリックします。
- c ポート名を入力します。
- d [ID] に、このポートに接続されている仮想マシンまたはサーバの VIF UUID を入力します。
- e タイプ ([親]、[子]、または [独立型]) を選択します。

コンテナまたは VMware HCX などの使用事例を除いて、このテキスト ボックスは空白のままで設定してください。このポートが仮想マシンのコンテナ用である場合は、[子] を選択します。このポートがコンテナのホスト仮想マシン用である場合は、[親] を選択します。このポートがベア メタル コンテナまたはサーバ用である場合は、[独立型] を選択します。

- f コンテキスト ID を入力します。

[タイプ] が [子] の場合は親の VIF ID を、[タイプ] が [独立型] の場合は、トランスポート ノード ID を入力します。

- g トラフィック タグを入力します。

コンテナおよびその他の使用事例の場合は、VLAN ID を入力します。

- h アドレスの割り当て方法を、[IP アドレス プール]、[MAC アドレス プール]、[両方]、または [なし] の中から選択します。

- i タグを指定します。

- j アドレスの割り当てを適用するには、アドレスの割り当てを適用する論理ポートの IP (IPv4 アドレス、IPv6 アドレスまたは IPv6 サブネット) と MAC アドレスを指定します。たとえば、IPv6 の場合、2001::/64 は IPv6 サブネット、2001::1 はホスト IP になります。2001::1/64 は無効な入力になります。VLAN ID を指定することもできます。

手動でのアドレスの割り当てを指定した場合、自動検出されたアドレスの割り当てがオーバーライドされます。

- k このポートのセグメント プロファイルを選択します。

14 セグメント プロファイルを選択するには、[セグメント プロファイル] をクリックします。

15 [保存] をクリックします。

Virtual Private Network (VPN)

5

NSX-T Data Center は NSX Edge ノード上の IPsec 仮想プライベート ネットワーク (IPsec VPN) および レイヤー 2 VPN (L2 VPN) をサポートします。IPsec VPN により、NSX Edge ノードとリモート サイトとのサイト間接続が提供されます。L2 VPN を使用すると、同じ IP アドレスを使用しながら、地理的な境界を越えて仮想マシンのネットワーク接続を維持できるようになり、データセンターを拡張できます。

注： IPsec VPN および L2 VPN は、NSX-T Data Center Limited Export Release ではサポートされていません。

VPN サービスを設定する前に、1 つ以上の Tier-0 または Tier-1 ゲートウェイが設定された NSX Edge ノードが機能している必要があります。詳細については、『NSX-T Data Center インストール ガイド』の「NSX Edge のインストール」を参照してください。

NSX-T Data Center 2.4 以降では、NSX Manager ユーザー インターフェイスを使用して新しい VPN サービスも設定できます。NSX-T Data Center の以前のリリースで VPN サービスを設定するには、REST API 呼び出しを使用する必要があります。

重要： NSX-T Data Center 2.4 以降を使用して VPN サービスを設定する場合は、Tier-0 ゲートウェイなど、NSX Manager のユーザー インターフェイスを使用して作成された新しいオブジェクトを使用するか、NSX-T Data Center 2.4 以降のリリースに含まれるポリシー API を使用する必要があります。NSX-T Data Center 2.4 リリースの前に設定された既存の Tier-0 または Tier-1 論理ルーターを使用するには、引き続き API 呼び出しを使用して VPN サービスを設定する必要があります。

事前定義された値と設定を含むシステムのデフォルトの設定プロファイルは、VPN サービスの設定中に使用可能になります。異なる設定を含む新しいプロファイルを定義して、VPN サービスの設定中に選択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。

- [IPsec VPN の理解](#)
- [レイヤー 2 VPN の理解](#)
- [VPN サービスの追加](#)
- [IPsec VPN セッションの追加](#)
- [L2 VPN セッションの追加](#)
- [ローカル エンドポイントの追加](#)
- [プロファイルの追加](#)

- [L2 VPN クライアントとしての自律 Edge の追加](#)
- [IPsec VPN セッションの認識された状態の確認](#)
- [VPN セッションの監視とトラブルシューティング](#)

IPsec VPN の理解

Internet Protocol Security (IPsec) VPN は、エンドポイントと呼ばれる IPsec ゲートウェイを使用してパブリック ネットワーク経由で接続されている 2 つのネットワーク間のトラフィック フローを保護します。NSX Edge では、IP トンネルと Encapsulating Security Payload (ESP) を使用するトンネル モードのみをサポートしています。ESP は、IP プロトコル番号 50 を使用して、IP のすぐ上で動作します。

IPsec VPN は、IKE プロトコルを使用して、セキュリティ パラメータをネゴシエートします。UDP ポートは、デフォルトで 500 に設定されます。ゲートウェイで NAT が検出されると、ポートは UDP 4500 に設定されます。

NSX Edge は、ポリシーベースまたはルートベースの IPsec VPN をサポートします。

IPsec VPN サービスは、Active-Standby 高可用性モードが必要な Tier-0 ゲートウェイでサポートされています。詳細については、[Tier-0 ゲートウェイの追加](#)を参照してください。NSX-T Data Center 2.5 以降では、IPsec VPN も Tier-1 ゲートウェイでサポートされます。IPsec VPN サービスを設定する場合は、Tier-0 または Tier-1 のいずれかのゲートウェイに接続されているセグメントを使用できます。

NSX-T Data Center の IPsec VPN サービスは、ゲートウェイレベルのフェイルオーバー機能を利用して高可用性サービスをサポートします。フェイルオーバーが発生するとトンネルが再確立され、VPN 設定データが同期されます。トンネルが再確立されるときに、IPsec VPN の状態は同期されません。

ブリシェード キー モード認証および IP ユニキャスト トラフィックは、NSX Edge ノードとリモート VPN サイト間でサポートされています。また、証明書認証は NSX-T Data Center 2.4 以降でサポートされています。サポートされるのは、次のいずれかの署名ハッシュ アルゴリズムで署名された証明書タイプのみです。

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

ポリシーベース IPsec VPN の使用

ポリシーベース IPsec VPN では、VPN ポリシーをパケットに適用して VPN トンネルの通過前に IPsec で保護するトラフィックを決定する必要があります。

このタイプの VPN は静的と見なされます。これは、ローカル ネットワーク トポロジや構成が変更されると、その変更に合わせて VPN ポリシー設定も更新する必要があるためです。

ポリシーベース IPsec VPN を NSX-T Data Center で使用する際は、IPsec トンネルを使用して NSX Edge ノードの背後にある 1 つ以上のローカル サブネットをリモート VPN サイトのピア サブネットと接続します。

NAT デバイスの背後に NSX Edge ノードを展開できます。この展開で NAT デバイスは、NSX Edge ノードの VPN アドレスを、インターネットに接するパブリックにアクセス可能なアドレスに変換します。リモート VPN サイトはこのパブリック アドレスを使用して NSX Edge ノードにアクセスします。

リモート VPN サイトを NAT デバイスの背後に設置することもできます。IPsec トンネルをセットアップするには、リモート VPN サイトのパブリック IP アドレスとその ID (FQDN または IP アドレス) を指定する必要があります。両端では、VPN アドレス用に静的な一対一の NAT が要求されます。

注： DNAT は、ポリシーベースの IPsec VPN が設定されている Tier-1 ゲートウェイでサポートされていません。

次の表に示すように、サポートされるトンネルの最大数は NSX Edge ノードのサイズで決まります。

表 5-1. サポートされる IPsec トンネルの数

Edge ノード サイズ	VPN セッションあたりの IPsec トン ネル数 (ポリシー ベース)	VPN サービスあたりのセッション数	
		VPN サービスあたりのセッション数	VPN サービスあたりの IPsec トンネル 数 (セッションあたり 16 トンネル)
小規模	該当なし (事前検証 (POC)/ラボのみ)	該当なし (事前検証 (POC)/ラボのみ)	該当なし (事前検証 (POC)/ラボのみ)
中規模	128	128	2048
大規模	128 (ソフトリミット)	256	4096
ベア メタル	128 (ソフトリミット)	512	6000

制限： ポリシー ベースの IPsec VPN のアーキテクチャでは、VPN トンネルの冗長性の設定に制限があります。

ポリシーベース IPsec VPN の構成方法については、[IPsec VPN サービスの追加](#)を参照してください。

ルートベース IPsec VPN の使用

ルート ベース IPsec VPN は、プロトコルに BGP などを使用し、スタティック ルートあるいは仮想トンネル インターフェイス (VTI) と呼ばれる特別なインターフェイスを介して動的に学習したルートに基づいて、トラフィックのトンネリングを行います。IPsec は、VTI を通過するすべてのトラフィックを保護します。

注：

- OSPF 動的ルーティングでは、IPsec VPN トンネル経由でルーティングを実行できません。
- VTI の動的ルーティングは、Tier-1 ゲートウェイに基づく VPN でサポートされません。

ルートベースの IPsec VPN は、IPsec 経由の GRE (Generic Routing Encapsulation) に似ていますが、IPsec 処理を適用する前にパケットに追加のカプセル化が行われない点が異なります。

この VPN トンネルでは、VTI が NSX Edge ノードに作成されています。各 VTI は IPsec トンネルに関連付けられます。暗号化されたトラフィックは、VTI インターフェイスを経由してサイト間をルーティングされます。IPsec の処理は VTI でのみ発生します。

VPN トンネルの冗長性

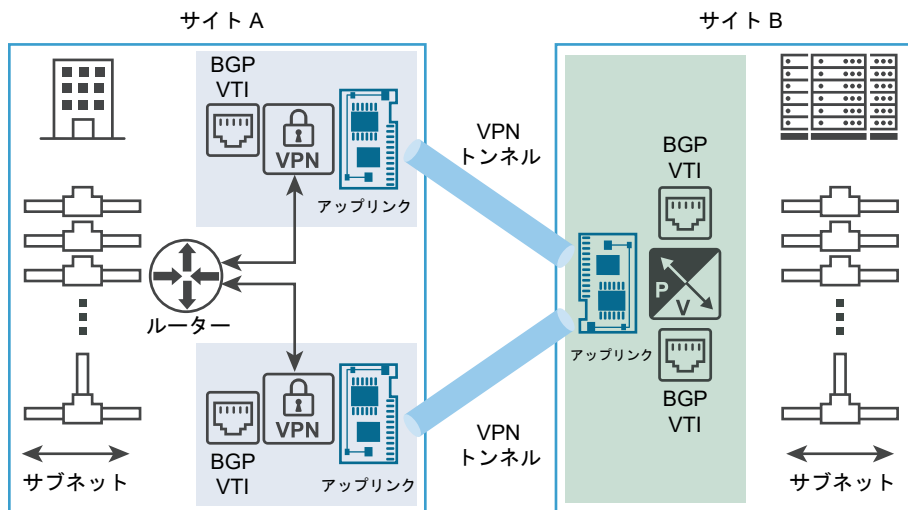
VPN トンネルの冗長性は、Tier-0 ゲートウェイで設定されているルートベースの IPsec VPN セッションで設定できます。トンネルの冗長性により、2 つのサイト間に複数のトンネルを設定できます。1 つのトンネルはプライマリとして使用します。プライマリ トンネルが使用不能になると、別のトンネルにフェイルオーバーされます。この機能は、サイトに複数の接続オプションがあり、リンクの冗長性で異なる ISP が必要な場合に便利です。

重要：

- NSX-T Data Center では、BGP を使用している場合にのみ、IPsec VPN トンネルの冗長性がサポートされます。
- VPN トンネルの冗長性を実現する場合は、ルートベースの IPsec VPN トンネルに静的ルーティングを使用しないでください。

次の図では、2 つのサイト間の IPsec VPN トンネルの冗長性を論理的に表現しています。この図で、サイト A とサイト B はそれぞれのデータセンターを表します。この例で、NSX-T Data Center はサイト A の Edge VPN ゲートウェイを管理していないことを前提としています。NSX-T Data Center が管理しているのは、サイト B の Edge Gateway 仮想アプライアンスです。

図 5-1. ルートベースの IPsec VPN トンネルの冗長性



図のように、VTI を使用すると、2 つの独立した IPsec VPN トンネルを設定できます。トンネルの冗長性を実現するため、動的ルーティングは BGP プロトコルを使用するように設定されています。両方の IPsec VPN トンネルが使用可能な場合は、引き続き稼働します。サイト A から NSX Edge ノード経由でサイト B に送信されるトラフィックはすべて、VTI 経由でルーティングされます。データトラフィックが IPsec の処理に進み、関連する NSX Edge ノードのアップリンク インターフェイスから送信されます。NSX Edge ノードのアップリンク インターフェイスでサイト B の VPN ゲートウェイから受信したすべての IPsec トラフィックは、復号化されてから VTI に転送され、通常ルーティングが行われます。

必要なフェイルオーバー時間内にピアとの切断を検出できるように、BGP HoldDown タイマーと KeepAlive タイマーの値を構成する必要があります。[BGP の設定](#) を参照してください。

レイヤー 2 VPN の理解

レイヤー 2 VPN (L2 VPN) を使用することで、同一のブロードキャスト ドメインにある複数のサイトにまたがってレイヤー 2 ネットワーク (VNI または VLAN) を拡張できます。この接続は、L2 VPN サーバと L2 VPN クライアントの間でルート ベースの IPsec トンネルを使用して保護されます。

注： この L2 VPN 機能は NSX-T Data Center でのみ利用可能です。サードパーティ製品との相互運用性はありません。

拡張ネットワークは単一のブロードキャスト ドメインを持つ単一のサブネットであるため、仮想マシンはサイト間で移動しても同一のサブネットに留まり、IP アドレスは変更されません。そのため、ネットワーク サイト間で仮想マシンをシームレスに移行できます。仮想マシンは、VNI ベース ネットワークまたは VLAN ベース ネットワークのいずれかで実行できます。また、L2 VPN は、クラウド プロバイダに対して、ワークロードやアプリケーションで使用される既存の IP アドレスを変更せずに、テナントのオンボードを行うためのメカニズムを提供します。

データセンターの移行のサポートに加え、L2 VPN を使用したオンプレミス ネットワークの拡張は、ディザスタ リカバリ プランを使用する際や、需要の増加に対応するためにオフプレミスのコンピュート リソースを動的に利用する際に有効です。

各 L2 VPN セッションには、1 つの GRE (Generic Routing Encapsulation) トンネルがあります。トンネルの冗長性はサポートされていません。L2 VPN セッションは、最大 4,094 個の L2 セグメントに拡張できます。

NSX-T Data Center では、L2 VPN サービスは Tier-0 ゲートウェイでのみサポートされます。セグメントは、Tier-0 または Tier-1 のいずれかのゲートウェイに接続可能で、L2 VPN サービスを使用します。

NSX-T Data Center 2.5 リリース以降では、NSX-T Data Center 環境で管理されている NSX Edge で、L2 VPN サービスを使用して VLAN ベースのセグメントを拡張できます。このサポートにより、VLAN から VNI、VLAN から VLAN、VNI から VNI に L2 ネットワークを拡張できます。

また、ESX NSX で管理されている分散仮想スイッチ (N-VDS) を使用した VLAN トランクもサポートされています。コンピューティング リソースと I/O リソースに余裕がある場合、VLAN トランクにより、単一のインターフェイス上で 1 つの NSX Edge クラスタから複数の VLAN ネットワークを拡張できます。

L2 VPN サービスのサポートは、次のシナリオで提供されます。

- NSX-T Data Center L2 VPN サーバと、NSX Data Center for vSphere 環境の管理対象の NSX Edge でホストされている L2 VPN クライアントの間 管理対象の L2 VPN クライアントは、VLAN と VNI の両方をサポートします。
- NSX-T Data Center L2 VPN サーバと、スタンドアローンまたは管理対象外の NSX Edge でホストされている L2 VPN クライアントの間。管理対象外の L2 VPN クライアントは、VLAN のみをサポートします。
- NSX-T Data Center L2 VPN サーバと、自律 NSX Edge でホストされている L2 VPN クライアントの間 自律 L2 VPN クライアントは VLAN のみをサポートします。
- NSX-T Data Center 2.4 以降のリリースでは、L2 VPN サービスは NSX-T Data Center L2 VPN サーバと NSX-T Data Center L2 VPN クライアント間でサポートされます。このシナリオでは、オンプレミスの 2 つの Software-Defined データセンター (SDDC) 間で論理 L2 セグメントを拡張できます。

VPN サービスの追加

NSX Manager ユーザー インターフェイスを使用すると、IPsec VPN（ポリシーベースまたはルートベース）または L2 VPN のいずれかを追加できます。

次のセクションでは、VPN サービスの設定に必要なワークフローについて説明します。このセクションのトピックでは、NSX Manager ユーザー インターフェイスを使用して、IPsec VPN または L2 VPN のいずれかを追加する方法の詳細について説明します。

ポリシーベース IPsec VPN 設定のワークフロー

ポリシーベース IPsec VPN サービス ワークフローを設定するには、おおまかに次のような手順を実行する必要があります。

- 1 既存の Tier-0 または Tier-1 ゲートウェイを使用して、IPsec VPN サービスを作成し、有効にします。[IPsec VPN サービスの追加](#) を参照してください。
- 2 システムのデフォルト値を使用しない場合は、DPD (Dead Peer Detection) プロファイルを作成します。[DPD プロファイルの追加](#) を参照してください。
- 3 システムのデフォルト以外の IKE プロファイルを使用するには、IKE（インターネット キー交換）プロファイルを定義します。[IKE プロファイルの追加](#) を参照してください。
- 4 [IPsec プロファイルの追加](#)を使用して IPsec プロファイルを設定します。
- 5 [ローカル エンドポイントの追加](#)を使用して、NSX Edge にホストされる VPN サーバを作成します。
- 6 ポリシーベース IPsec VPN セッションを設定し、プロファイルを適用して、ローカル エンドポイントを接続します。[ポリシーベース IPsec セッションの追加](#)を参照してください。トンネルで使用するローカルおよびピア サブネットを指定します。ローカル サブネットからピア サブネットへのトラフィックは、セッションで定義されたトンネルで保護されます。

ルートベース IPsec VPN 設定のワークフロー

ルートベース IPsec VPN 設定のワークフローでは、おおまかに次のような手順を実行する必要があります。

- 1 既存の Tier-0 または Tier-1 ゲートウェイを使用して、IPsec VPN サービスを設定し、有効にします。[IPsec VPN サービスの追加](#) を参照してください。
- 2 デフォルトの IKE プロファイルを使用しない場合は、IKE プロファイルを定義します。[IKE プロファイルの追加](#) を参照してください。
- 3 システム デフォルトの IPsec プロファイルを使用しない場合は、[IPsec プロファイルの追加](#)を使用してプロファイルを作成します。
- 4 デフォルトの DPD プロファイルを使用しない場合は、DPD プロファイルを作成します。[DPD プロファイルの追加](#) を参照してください。
- 5 [ローカル エンドポイントの追加](#)を使用してローカル エンドポイントを追加します。

- 6 ルートベース IPsec VPN セッションを設定し、プロファイルを適用して、セッションにローカル エンドポイントを接続します。設定で VTI IP アドレスを指定し、同じ IP アドレスを使用してルーティングを設定します。ルートは、スタティックまたはダイナミック（BGP を使用）のいずれかになります。[ルートベース IPsec セッションの追加](#) を参照してください。

L2 VPN 設定のワークフロー

L2 VPN を設定する場合は、サーバ モードで L2 VPN サービスを設定し、クライアント モードで別の L2 VPN サービスを設定する必要があります。L2 VPN サーバによって生成されたピア コードを使用して、L2 VPN サーバと L2 VPN クライアントのセッションを設定する必要があります。次に、L2 VPN サービスの設定に関するおおまかなワークフローを示します。

- 1 サーバ モードで L2 VPN サービスを作成します。
 - a Tier-0 ゲートウェイを使用してルートベース IPsec VPN トンネルを設定し、このルートベース IPsec トンネルを使用して L2 VPN サーバ サービスを設定します。[L2 VPN サーバ サービスの追加](#) を参照してください。
 - b L2 VPN サーバ セッションを設定します。このセッションでは、新しく作成したルートベース IPsec VPN サービスと L2 VPN サーバ サービスを割り当てるため、GRE IP アドレスが自動的に割り当てられます。[L2 VPN サーバ セッションの追加](#) を参照してください。
 - c L2 VPN サーバ セッションにセグメントを追加します。この手順は、[L2 VPN サーバ セッションの追加](#)にも記載されています。
 - d リモート側の [L2 VPN 構成ファイルのダウンロード](#)の手順に従って L2 VPN サーバ サービス セッションのピア コードを取得します。L2 VPN クライアント セッションが自動的に設定されるように、このコードをリモート サイトに適用し、使用する必要があります。
- 2 クライアント モードで L2 VPN サービスを作成します。
 - a 別の Tier-0 ゲートウェイを使用して別ルートベース IPsec VPN サービスを設定し、ここで設定した Tier-0 ゲートウェイを使用して L2 VPN クライアント サービスを設定します。詳細については、[L2 VPN クライアント サービスの追加](#)を参照してください。
 - b L2 VPN サーバ サービスで生成されるピア コードをインポートして、L2 VPN クライアント セッションを定義します。[L2 VPN クライアント セッションの追加](#) を参照してください。
 - c 前の手順で定義した L2 VPN クライアント セッションにセグメントを追加します。この手順は、[L2 VPN クライアント セッションの追加](#)に記載されています。

IPsec VPN サービスの追加

NSX-T Data Center は、Tier-0 または Tier-1 ゲートウェイとリモート サイトのサイト間 IPsec VPN サービスをサポートします。ポリシーベースまたはルートベースの IPsec VPN サービスを作成できます。ポリシーベースまたはルートベースの IPsec VPN セッションのいずれかを設定する前に、最初に IPsec VPN サービスを作成する必要があります。

注： IPsec VPN は NSX-T Data Center Limited Export Release ではサポートされていません。

ローカル エンドポイントの IP アドレスが、IPsec VPN セッションが構成されている論理ルーター内で NAT を通過している場合、IPsec VPN はサポートされません。

前提条件

- IPsec VPN について理解しておく必要があります。[IPsec VPN の理解](#) を参照してください。
- 1 つ以上の Tier-0 または Tier-1 ゲートウェイが設定され、使用できる状態になっている必要があります。詳細については、[Tier-0 ゲートウェイの追加](#)または[Tier-1 ゲートウェイの追加](#)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>>) に管理者権限でログインします。

2 [ネットワーク] - [VPN] - [VPN サービス] に移動します。

3 [サービスの追加] - [IPsec] を選択します。

4 IPsec サービスの名前を入力します。

この名前は必須です。

5 [ゲートウェイ] ドロップダウン メニューから、この IPsec VPN サービスに関連付ける Tier-0 または Tier-1 ゲートウェイを選択します。

6 [管理状態] を有効または無効にします。

デフォルトでは、値は `Enabled` に設定されています。つまり、新しい IPsec VPN サービスが設定されると、Tier-0 または Tier-1 ゲートウェイで IPsec VPN サービスが有効に設定されます。

7 [IKE ログ レベル] の値を設定します。

デフォルトでは、`Info` レベルに設定されています。

8 タグ グループにこのサービスを含める場合は、[タグ] の値を入力します。

9 IPsec セッション ルールに IP アドレスが指定されている場合でも、IPsec による保護なしで指定のローカル IP アドレスとリモート IP アドレスの間でデータ パケットの交換を許可する場合は、[グローバル バイパス ルール] をクリックします。[ローカル ネットワーク] と [リモート ネットワーク] テキスト ボックスに、バイパス ルールが適用されるローカルおよびリモートのサブネットのリストを入力します。

デフォルトでは、ローカル サイトおよびリモート サイト間のデータ交換時に IPsec の保護を使用します。これらのルールは、この IPsec VPN サービス内で作成されたすべての IPsec VPN セッションに適用されます。

10 [保存] をクリックします。

新規の IPsec VPN サービスが正常に作成されると、残りの IPsec VPN の設定を続行するかどうか尋ねられます。[はい] をクリックすると、[IPsec VPN サービスの追加] パネルに戻ります。[セッション] リンクが有効になり、このリンクをクリックして IPsec VPN セッションを追加できるようになります。

次のステップ

[IPsec VPN セッションの追加](#)の情報を参照して、IPsec VPN セッションを追加します。また、IPsec VPN の設定を完了するために必要なプロファイルおよびローカル エンドポイントの情報を指定します。

L2 VPN サービスの追加

Tier-0 ゲートウェイに L2 VPN サービスを設定します。L2 VPN サービスを有効にするときに、Tier-0 ゲートウェイに IPsec VPN サービスが存在していない場合は、まずこのサービスを作成する必要があります。L2 VPN サーバ（宛先ゲートウェイ）と L2 VPN クライアント（送信元ゲートウェイ）の間に L2 VPN トンネルを設定します。

L2 VPN サービスを設定するには、このセクションの以下のトピックの情報を使用します。

前提条件

- IPsec VPN および L2 VPN について理解しておく必要があります。[IPsec VPN の理解](#)および[レイヤー 2 VPN の理解](#)を参照してください。
- 1 つ以上の Tier-0 ゲートウェイが設定され、使用できる状態になっている必要があります。[Tier-0 ゲートウェイの追加](#)を参照してください。

手順

1 L2 VPN サーバ サービスの追加

L2 VPN サーバ サービスを設定するには、L2 VPN クライアントの接続先である宛先 NSX Edge においてサーバ モードで L2 VPN サービスを設定する必要があります。

2 L2 VPN クライアント サービスの追加

L2 VPN サーバ サービスを設定した後、別の NSX Edge インスタンスでクライアント モードの L2 VPN サービスを設定します。

L2 VPN サーバ サービスの追加

L2 VPN サーバ サービスを設定するには、L2 VPN クライアントの接続先である宛先 NSX Edge においてサーバ モードで L2 VPN サービスを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>>) に管理者権限でログインします。
- 2 （オプション）L2 VPN サーバとして設定する Tier-0 ゲートウェイに IPsec VPN サービスが存在していない場合は、次の手順に従ってサービスを作成します。
 - a [ネットワーク] - [VPN] - [VPN サービス] タブに移動し、[サービスの追加] - [IPsec] の順に選択します。
 - b IPsec VPN サービスの名前を入力します。
 - c [Tier-0 ゲートウェイ] ドロップダウン メニューから、L2 VPN サーバで使用する Tier-0 ゲートウェイを選択します。
 - d システムのデフォルト値と異なる値を使用する場合は、必要に応じて [IPsec サービスの追加] ペインで残りのプロパティを設定します。
 - e [保存] をクリックし、IPsec VPN サービス設定の続行を示すプロンプトが表示されたら、[いいえ] を選択します。

- 3 [ネットワーク] - [VPN] - [VPN サービス] タブに移動し、[サービスの追加] - [L2 VPN サーバ] の順に選択して L2 VPN サーバを作成します。
- 4 L2 VPN サーバの名前を入力します。
- 5 [Tier-0 ゲートウェイ] ドロップダウン メニューから、先ほど作成した IPsec サービスで使用したのと同じ Tier-0 ゲートウェイを選択します。
- 6 必要に応じて、この L2 VPN サーバの説明を入力します。
- 7 タグ グループにこのサービスを含める場合は、[タグ] の値を入力します。
- 8 [ハブ アンド スポーク] プロパティを有効または無効にします。

デフォルトでは、値は `Disabled` に設定されています。つまり、L2 VPN クライアントから受信したトラフィックは、L2 VPN サーバに接続しているセグメントにのみレプリケートされます。このプロパティが `Enabled` に設定されて場合、L2 VPN クライアントからのトラフィックは他のすべての L2 VPN クライアントにレプリケートされます。

- 9 [保存] をクリックします。

新しい L2 VPN サーバが正常に作成されると、残りの L2 VPN サービスの設定を続行するかどうかの質問が表示されます。[はい] をクリックすると、[L2 VPN サーバの追加] ペインが表示され、[セッション] リンクが有効になります。このリンクを使用して L2 VPN サーバ セッションを作成するか、[ネットワーク] - [VPN] - [L2 VPN セッション] タブを使用します。

次のステップ

ガイドとして [L2 VPN サーバ セッションの追加](#) の情報を使用して設定された L2 VPN サーバの L2 VPN サーバ セッションを設定します。

L2 VPN クライアント サービスの追加

L2 VPN サーバ サービスを設定した後、別の NSX Edge インスタンスでクライアント モードの L2 VPN サービスを設定します。

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 (オプション) まだ存在しない場合は、次の手順に従って、L2 VPN クライアント サービスの IPsec VPN サービスを作成します。
 - a [ネットワーク] - [VPN] - [VPN サービス] タブに移動し、[サービスの追加] - [IPsec] の順に選択します。
 - b IPsec VPN サービスの名前を入力します。
 - c [Tier-0 ゲートウェイ] ドロップダウン メニューから、L2 VPN クライアントで使用する Tier-0 ゲートウェイを選択します。

- d システムのデフォルト値と異なる値を使用する場合は、必要に応じて [IPsec サービスの追加] ペインで残りのプロパティを設定します。
 - e [保存] をクリックし、IPsec VPN サービス設定の続行を示すプロンプトが表示されたら、[いいえ] を選択します。
- 3 [ネットワーク] - [VPN] - [VPN サービス] タブに移動し、[サービスの追加] - [L2 VPN クライアント] の順に選択します。
 - 4 L2 VPN クライアント サービスの名前を入力します。
 - 5 [Tier-0 ゲートウェイ] ドロップダウン メニューから、先ほど作成したルートベース IPsec トンネルで使した Tier-0 ゲートウェイと同じものを選択します。
 - 6 必要であれば、[説明] と [タグ] の値を設定します。
 - 7 [保存] をクリックします。

新しい L2 VPN クライアント サービスが正常に作成されると、L2 VPN クライアントの残りの設定を続行するかどうかを確認されます。[はい] をクリックすると、[L2 VPN クライアントの追加] ペインに戻り、[セッション] リンクが有効になります。このリンクを使用して L2 VPN クライアント セッションを作成するか、[ネットワーク] - [VPN] - [L2 VPN セッション] タブを使用することができます。

次のステップ

設定した L2 VPN クライアント サービスの L2 VPN クライアント セッションを設定します。ガイドとして、[L2 VPN クライアント セッションの追加](#)に記載された情報を使用してください。

IPsec VPN セッションの追加

IPsec VPN サービスを設定した後は、設定する IPsec VPN のタイプに応じて、ポリシーベース IPsec VPN セッションまたはルートベース IPsec VPN セッションのいずれかを追加する必要があります。また、使用するローカルエンドポイントおよびプロファイルの情報を入力し、IPsec VPN サービスの設定を完了します。

ポリシーベース IPsec セッションの追加

ポリシーベース IPsec VPN を追加する場合、リモート VPN サイトのピア サブネットを持つ NSX Edge ノードの背後にある複数のローカル サブネットの接続に IPsec トンネルが使用されます。

次の手順では、NSX Manager ユーザー インターフェイスの [IPsec セッション] タブを使用してポリシーベース IPsec セッションを作成します。また、トンネル、IKE、および DPD プロファイルの情報を追加し、ポリシーベース IPsec VPN で使用する既存のローカル エンドポイントを選択します。

注： IPsec VPN サービスを正常に設定した後すぐに、IPsec VPN セッションを追加することもできます。IPsec VPN サービスの設定を続行するよう求められたら、[はい] をクリックし、[IPsec サービスの追加] パネルで [セッション] - [セッションの追加] の順に選択します。以下の手順の前半は、IPsec VPN サービスの設定を続行するよう求められたときに [いいえ] を選択したことが前提となっています。[はい] を選択した場合は、次の手順の手順 3 に進み、ポリシーベース IPsec VPN セッションの残りの設定を続行します。

前提条件

- 続行する前に、IPsec VPN サービスを設定する必要があります。[IPsec VPN サービスの追加](#) を参照してください。
- 追加するポリシーベース IPsec VPN セッションで使用するローカル エンドポイントの情報、ピア サイトの IP アドレス、ローカル ネットワークのサブネット、およびリモート ネットワークのサブネットを取得します。ローカル エンドポイントを作成するには、[ローカル エンドポイントの追加](#)を参照してください。
- 認証に事前共有キー (PSK) を使用している場合は、PSK 値を取得します。
- 認証に証明書を使用している場合は、必要なサーバ証明書と対応する CA 署名付き証明書がすでにインポートされていることを確認します。[証明書の設定](#) を参照してください。
- NSX-T Data Center によって提供される IPsec トンネル、IKE、または Dead Peer Detection (DPD) プロファイルのデフォルト値を使用しない場合、代わりに使用するプロファイルを構成します。詳細については、[プロファイルの追加](#)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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [IPsec セッション] タブに移動します。
- 3 [IPsec セッションの追加] - [ポリシー ベース] を選択します。
- 4 ポリシーベース IPsec VPN セッションの名前を入力します。
- 5 [VPN サービス] ドロップダウン メニューから、この新しい IPsec セッションを追加する IPsec VPN サービスを選択します。

注： [IPsec セッションの追加] ダイアログ ボックスでこの IPsec セッションを追加する場合は、[IPsec セッションの追加] ボタンの上に VPN サービスの名前がすでに示されています。

- 6 ドロップダウン メニューから既存のローカル エンドポイントを選択します。
このローカル エンドポイントの値は必須で、ローカル NSX Edge ノードの識別に使用されます。別のローカル エンドポイントを作成する場合は、3 つのドットで示されるメニュー (⋮) をクリックして、[ローカル エンドポイントの追加] を選択します。
- 7 [リモート IP] テキスト ボックスに、リモート サイトに必要な IP アドレスを入力します。
この値は必須です。
- 8 このポリシーベース IPsec VPN セッションのオプションの説明を入力します。
長さは最大 1,024 文字です。
- 9 IPsec VPN セッションを有効または無効にするには、[管理状態] をクリックします。
デフォルトでは、値は `Enabled` に設定されています。これは、NSX Edge ノードまで IPsec VPN セッションが設定されることを意味します。

- 10 (オプション) [コンプライアンス スイート] ドロップダウン メニューから、セキュリティ コンプライアンス スイートを選択します。

注： コンプライアンス スイートのサポートは、NSX-T Data Center 2.5 以降で提供されます。詳細については、[サポートされているコンプライアンス スイートについて](#)を参照してください。

デフォルトで選択される値は `None` です。コンプライアンス スイートを選択すると、[認証モード] が `Certificate` に設定されます。[詳細なプロパティ] セクションで、[IKE プロファイル] と [IPsec プロファイル] の値が、選択したセキュリティ コンプライアンス スイートのシステム定義プロファイルに設定されます。これらのシステム定義のプロファイルは編集できません。

- 11 [コンプライアンス スイート] が `None` に設定されている場合は、[認証モード] ドロップダウン メニューからモードを選択します。

使用されるデフォルトの認証モードは `PSK` です。つまり、IPsec VPN セッションには NSX Edge とリモート サイト間で共有されるプライベート キーが使用されます。`Certificate` を選択すると、ローカル エンドポイントの設定に使用されたサイト証明書が認証に使用されます。

- 12 [ローカル ネットワーク] と [リモート ネットワーク] テキスト ボックスに、このポリシーベース IPsec VPN セッションで使用する 1 つ以上の IP サブネット アドレスを入力します。

これらのサブネットは CIDR 形式にする必要があります。

- 13 [認証モード] が `PSK` に設定されている場合は、[事前共有キー] テキスト ボックスにキーの値を入力します。

このプライベート キーは、最大長が 128 文字の文字列です。

注意： PSK 値には機密情報が含まれているため、PSK 値を共有して保存する場合は注意してください。

- 14 ピア サイトを識別するために、[リモート ID] に値を入力します。

PSK 認証を使用するピア サイトの場合、この ID 値はパブリック IP アドレスまたはピア サイトの FQDN にする必要があります。証明書認証を使用するピア サイトの場合、この ID 値はピア サイトの証明書のコモン ネーム (CN) または識別名 (DN) にする必要があります。

注： たとえば、次のようにピア サイトの証明書で識別名 (DN) にメール アドレスが含まれている場合、

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

次の形式で [リモート ID] の値を入力します。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

ローカル サイトの証明書で識別名 (DN) にメール アドレスが含まれ、ピア サイトが `strongSwan` IPsec を使用している場合は、このピア サイトにローカル サイトの ID 値を入力します。次に例を示します。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```


- 15 ポリシーベースの IPsec VPN セッションで使用されるプロファイル、開始モード、TCP MSS クランプ モード、タグを変更するには、[詳細なプロパティ] をクリックします。

デフォルトでは、システムによって生成されたプロファイルが使用されます。デフォルトを使用しない場合は、別の利用可能なプロファイルを選択します。まだ設定されていないプロファイルを使用する場合は、3 つのドットで示されるメニュー (⋮) をクリックして別のプロファイルを作成します。[プロファイルの追加](#) を参照してください。

- a [IKE プロファイル] ドロップダウン メニューが有効になっている場合は、IKE プロファイルを選択します。
- b [IPsec プロファイル] ドロップダウン メニューが無効になっている場合は、IPsec トンネル プロファイルを選択します。
- c [DPD プロファイル] ドロップダウン メニューが有効になっている場合は、優先 DPD プロファイルを選択します。
- d [接続開始モード] ドロップダウン メニューから優先モードを選択します。

接続開始モードは、トンネルを作成するときにローカル エンドポイントで使用されるポリシーを定義します。デフォルト値は **Initiator** です。次の表では、使用可能なさまざまな接続開始モードについて説明します。

表 5-2. 接続開始モード

接続開始モード	説明
Initiator	デフォルト値です。このモードの場合、ローカル エンドポイントは IPsec VPN トンネルの作成を開始して、ピア ゲートウェイから受信するトンネル設定要求に応答します。
On Demand	このモードの場合、ローカル エンドポイントは、ポリシー ルールと一致する最初のパケット受信した後に IPsec VPN トンネルの作成を開始します。受信した開始要求にも応答します。
Respond Only	IPsec VPN は接続を開始しません。ピア サイトは接続要求を常に開始し、ローカル エンドポイントはこの接続要求に応答します。

- e IPsec 接続中に TCP セッションの最大セグメント サイズ (MSS) ペイロードを削減するには、[TCP MSS クランプ] を有効にして、[TCP MSS の方向] で値を選択します。必要であれば、[TCP MSS 値] を設定します。

詳細については、[TCP MSS クランプの理解](#)を参照してください。

- f 特定のグループの一部としてこのセッションを含める場合は、[タグ] にタグ名を入力します。

- 16 [保存] をクリックします。

結果

新しいポリシーベース IPsec VPN セッションが正常に設定されている場合は、使用可能な IPsec VPN セッションのリストに追加されます。このセッションは読み取り専用モードです。

次のステップ

- IPsec VPN トンネルの状態が [稼動中] であることを確認します。詳細については、[VPN セッションの監視とトラブルシューティング](#)を参照してください。

- 必要に応じて、セッションの行の左側にある 3 つのドットで示されるメニュー (⋮) をクリックして、IPsec VPN セッションの情報を管理します。実行できるアクションの中から 1 つを選択します。

ルートベース IPsec セッションの追加

ルート ベース IPsec VPN を追加すると、BGP などの優先プロトコルを使用して仮想トンネル インターフェイス (VTI) を介して動的に学習されたルートに基づとするトラフィックに対して、トンネリングが行われます。IPsec は、VTI を通過するすべてのトラフィックを保護します。

このトピックに記載されている手順では、[IPsec セッション] タブを使用してルートベース IPsec セッションを作成します。また、トンネル、IKE、および DPD プロファイルの情報の追加や、ルート ベース IPsec VPN で使用する既存のローカル エンドポイントの選択を行います。

注： IPsec VPN サービスを正常に設定した後すぐに、IPsec VPN セッションを追加することもできます。IPsec VPN サービスの設定を続行するよう求められたら、[はい] をクリックし、[IPsec サービスの追加] パネルで [セッション] - [セッションの追加] の順に選択します。以下の手順の前半は、IPsec VPN サービスの設定を続行するよう求められたときに [いいえ] を選択したことが前提となっています。[はい] を選択した場合は、次の手順の手順 3 に進み、手順に沿ってルートベース IPsec VPN セッションの続きの設定を行います。

前提条件

- 続行する前に、IPsec VPN サービスを設定する必要があります。[IPsec VPN サービスの追加](#) を参照してください。
- ローカル エンドポイント、ピア サイトの IP アドレス、追加するルート ベース IPsec セッションで使用するトンネル サービスの IP サブネット アドレスの情報を取得します。ローカル エンドポイントを作成するには、[ローカル エンドポイントの追加](#) を参照してください。
- 認証に事前共有キー (PSK) を使用している場合は、PSK 値を取得します。
- 認証に証明書を使用している場合は、必要なサーバ証明書と対応する CA 署名付き証明書がすでにインポートされていることを確認します。[証明書の設定](#) を参照してください。
- NSX-T Data Center から提供された IPsec トンネル、IKE、または Dead Peer Detection (DPD) プロファイルのデフォルト値を使用しない場合は、代わりに使用するプロファイルを構成します。詳細については、[プロファイルの追加](#) 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [IPsec セッション] に移動します。
- 3 [IPsec セッションの追加] - [ルート ベース] を選択します。
- 4 ルートベース IPsec セッションの名前を入力します。
- 5 [VPN サービス] ドロップダウン メニューから、この新しい IPsec セッションを追加する IPsec VPN サービスを選択します。

注： [IPsec セッションの追加] ダイアログ ボックスでこの IPsec セッションを追加する場合は、[IPsec セッションの追加] ボタンの上に VPN サービスの名前がすでに示されています。

- 6 ドロップダウン メニューから既存のローカル エンドポイントを選択します。

このローカル エンドポイントの値は必須で、ローカル NSX Edge ノードの識別に使用されます。別のローカル エンドポイントを作成する場合は、3 つのドットで示されるメニュー (⋮) をクリックして、[ローカル エンドポイントの追加] を選択します。

- 7 [リモート IP アドレス] テキスト ボックスにリモート サイトの IP アドレスを入力します。

この値は必須です。

- 8 このルート ベース IPsec VPN セッションのオプションの説明を入力します。

長さは最大 1,024 文字です。

- 9 IPsec セッションを有効または無効にするには、[管理状態] をクリックします。

デフォルトの値は `Enabled` に設定されています。これは、NSX Edge ノードまで IPsec セッションが設定されることを意味します。

- 10 (オプション) [コンプライアンス スイート] ドロップダウン メニューから、セキュリティ コンプライアンス スイートを選択します。

注： コンプライアンス スイートのサポートは、NSX-T Data Center 2.5 以降で提供されます。詳細については、[サポートされているコンプライアンス スイートについて](#)を参照してください。

デフォルト値は `None` に設定されています。コンプライアンス スイートを選択すると、[認証モード] が `Certificate` に設定されます。[詳細なプロパティ] セクションで、[IKE プロファイル] と [IPsec プロファイル] の値が、選択したコンプライアンス スイートのシステム定義プロファイルに設定されます。これらのシステム定義のプロファイルは編集できません。

- 11 [トンネル インターフェイス] に IP サブネット アドレスを CIDR 形式で入力します。

このアドレスは必須です。

- 12 [コンプライアンス スイート] が `None` に設定されている場合は、[認証モード] ドロップダウン メニューからモードを選択します。

使用されるデフォルトの認証モードは `PSK` です。つまり、IPsec VPN セッションには NSX Edge とリモート サイト間で共有されるプライベート キーが使用されます。`Certificate` を選択すると、ローカル エンドポイントの設定に使用されたサイト証明書が認証に使用されます。

- 13 認証モードに `PSK` を選択した場合は、[事前共有キー] テキスト ボックスにキーの値を入力します。

このプライベート キーは、最大長が 128 文字の文字列です。

注意： PSK 値には機密情報が含まれているため、PSK 値を共有して保存する場合は注意してください。

14 [リモート ID] の値を入力します。

PSK 認証を使用するピア サイトの場合、この ID 値はパブリック IP アドレスまたはピア サイトの FQDN にする必要があります。証明書認証を使用するピア サイトの場合、この ID 値はピア サイトの証明書の共通名 (CN) または識別名 (DN) にする必要があります。

注： たとえば、次のようにピア サイトの証明書で識別名 (DN) にメールアドレスが含まれている場合、

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

次の形式で [リモート ID] の値を入力します。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

ローカル サイトの証明書で識別名 (DN) にメールアドレスが含まれ、ピア サイトが strongSwan IPsec を使用している場合は、このピア サイトにローカル サイトの ID 値を入力します。次に例を示します。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

15 特定のグループ タグの一部としてこの IPsec セッションを含める場合は、[タグ] にタグ名を入力します。**16** ルートベースの IPsec VPN セッションで使用されるプロファイル、開始モード、TCP MSS クランプ モード、タグを変更するには、[詳細なプロパティ] をクリックします。

デフォルトでは、システムによって生成されたプロファイルが使用されます。デフォルトを使用しない場合は、別の利用可能なプロファイルを選択します。まだ設定されていないプロファイルを使用する場合は、3 つのドットで示されるメニュー (⋮) をクリックして別のプロファイルを作成します。[プロファイルの追加](#) を参照してください。

- a [IKE プロファイル] ドロップダウン メニューが有効になっている場合は、IKE プロファイルを選択します。
- b [IPsec プロファイル] ドロップダウン メニューが無効になっていない場合は、IPsec トンネル プロファイルを選択します。

- c [DPD プロファイル] ドロップダウン メニューが有効になっている場合は、優先 DPD プロファイルを選択します。
- d [接続開始モード] ドロップダウン メニューから優先モードを選択します。

接続開始モードは、トンネルを作成するときにローカル エンドポイントで使用するポリシーを定義します。デフォルト値は **Initiator** です。次の表では、使用可能なさまざまな接続開始モードについて説明します。

表 5-3. 接続開始モード

接続開始モード	説明
Initiator	デフォルト値です。このモードの場合、ローカル エンドポイントは IPsec VPN トンネルの作成を開始して、ピア ゲートウェイから受信するトンネル設定要求に応答します。
On Demand	ルートベースの VPN では使用しないでください。このモードは、ポリシーベースの VPN にのみ適用されます。
Respond Only	IPsec VPN は接続を開始しません。ピア サイトは接続要求を常に開始し、ローカル エンドポイントはこの接続要求に応答します。

- 17 IPsec 接続中に TCP セッションの最大セグメント サイズ (MSS) ペイロードを削減するには、[TCP MSS クランプ] を有効にして、[TCP MSS の方向] で値を選択します。必要であれば、[TCP MSS 値] を設定します。

詳細については、[TCP MSS クランプの理解](#)を参照してください。

- 18 特定のグループ タグの一部としてこの IPsec セッションを含める場合は、[タグ] にタグ名を入力します。
- 19 [保存] をクリックします。

結果

新しいルート ベース IPsec VPN セッションが正常に設定されている場合は、使用可能な IPsec VPN セッションのリストにこのセッションが追加されます。このセッションは読み取り専用モードです。

次のステップ

- IPsec VPN トンネルの状態が [稼動中] であることを確認します。詳細については、[VPN セッションの監視とトラブルシューティング](#)を参照してください。
- スタティック ルートまたは BGP のいずれかを使用してルーティングを構成します。[スタティック ルートの設定](#)または [BGP の設定](#)を参照してください。
- 必要に応じて、セッションの行の左側にある 3 つのドットで示されるメニュー (⋮) をクリックして、IPsec VPN セッションの情報を管理します。実行できるアクションの中から 1 つを選択します。

サポートされているコンプライアンス スイートについて

NSX-T Data Center 2.5 以降では、IPsec VPN セッションで使用するセキュリティ プロファイルの設定に使用するセキュリティ コンプライアンス スイートを指定できます。

セキュリティ コンプライアンス スイートには、さまざまなセキュリティ パラメータの値が事前に定義されています。これらの値は変更できません。コンプライアンス スイートを選択すると、事前定義の値が、設定中の IPsec VPN セッションのセキュリティ プロファイルに自動的に適用されます。

次の表に、NSX-T Data Center の IKE プロファイルでサポートされるコンプライアンス スイートと、各スイートの事前定義の値を示します。

コンプライアンス スイート名	IKE バージョン	暗号化アルゴリズム	ダイジェスト アルゴリズム	Diffie-Hellman グループ
CNSA	IKE v2	AES 256	SHA2 384	グループ 15、グループ 20
FIPS	IKE FLEX	AES 128	SHA2 256	グループ 20
Foundation	IKE v1	AES 128	SHA2 256	グループ 14
PRIME	IKE v2	AES GCM 128	未設定	グループ 19
Suite-B-GCM-128	IKE v2	AES 128	SHA2 256	グループ 19
Suite-B-GCM-256	IKE v2	AES 256	SHA2 384	グループ 20

次の表に、NSX-T Data Center の IPsec プロファイルでサポートされるコンプライアンス スイートと、各スイートの事前定義の値を示します。

コンプライアンス スイート名	暗号化アルゴリズム	ダイジェスト アルゴリズム	PFS グループ	Diffie-Hellman グループ
CNSA	AES 256	SHA2 384	有効	グループ 15、グループ 20
FIPS	AES GCM 128	未設定	有効	グループ 20
Foundation	AES 128	SHA2 256	有効	グループ 14
PRIME	AES GCM 128	未設定	有効	グループ 19
Suite-B-GCM-128	AES GCM 128	未設定	有効	グループ 19
Suite-B-GCM-256	AES GCM 256	未設定	有効	グループ 20

TCP MSS クランプの理解

TCP MSS クランプを使用すると、IPsec トンネルを介した接続の確立中に TCP セッションで使用される最大セグメント サイズ (MSS) 値を削減できます。この機能は、NSX-T Data Center 2.5 以降でサポートされています。

TCP MSS は、ホストが単一の TCP セグメントで許容される最大データ量（バイト単位）です。TCP 接続の各終端は、3 ウェイ ハンドシェイク中に目的の MSS 値をピアエンドに送信します。MSS は TCP SYN パケットで 사용되는 TCP ヘッダー オプションの 1 つです。TCP MSS は、送信側ホストの出力方向インターフェイスの最大転送ユニット (MTU) に基づいて計算されます。

TCP トラフィックが IPsec VPN または任意の VPN トンネルを通過すると、元のパケットにヘッダーが追加され、セキュリティが維持されます。IPsec トンネル モードの場合、使用される追加ヘッダーは、IP アドレス、ESP、および UDP（ネットワークにポート変換が存在する場合）です。これらの追加ヘッダーにより、カプセル化されたパケットのサイズが VPN インターフェイスの MTU を超過します。パケットは、DF ポリシーに基づいて断片化またはドロップする可能性があります。

パケットの断片化またはドロップを回避するには、TCP MSS クランプ機能を有効にして、IPsec セッションの MSS 値を調整します。[ネットワーク] - [VPN] - [IPsec セッション] の順に移動します。IPsec セッションを追加するか、既存のセッションを編集する場合は、[詳細なプロパティ] セクションを展開し、[TCP MSS クランプ] を有効にします。

IPsec セッションに適した計算済みの MSS 値を設定するには、[TCP MSS の方向] と [TCP MSS 値] の両方を設定します。設定した MSS 値が MSS クランプに使用されます。MSS を動的に計算する場合は、[TCP MSS の方向] を設定し、[TCP MSS 値] は空白のままにします。MSS 値は、VPN インターフェイスの MTU、VPN のオーバーヘッド、パスの MTU (PMTU) に基づいて自動的に計算されます。MTU または PMTU の変更を動的に処理するため、各 TCP ハンドシェイクで有効な MSS が再計算されます。

L2 VPN セッションの追加

L2 VPN サーバと L2 VPN クライアントを構成した後に、両方の L2 VPN セッションを追加して、L2 VPN サービスの設定を完了する必要があります。

L2 VPN サーバ セッションの追加

L2 VPN サーバ サービスを作成した後に、L2 VPN セッションを追加して、既存のセグメントに接続する必要があります。

次の手順では、NSX Manager ユーザー インターフェイスの [L2 VPN セッション] タブを使用して、L2 VPN サーバ セッションを作成します。既存のローカル エンドポイントおよびセグメントを選択して、L2 VPN サーバ セッションに接続することもできます。

注： L2 VPN サーバ サービスを正常に設定した後すぐに、L2 VPN サーバ セッションを追加することもできます。L2 VPN サーバの設定を続行するように求められたら、[はい] をクリックし、[L2 VPN サーバの追加] パネルで [セッション] - [セッションの追加] の順に選択します。次の手順の中の最初のいくつかでは、L2 VPN サーバの設定を続行するように求められたときに [いいえ] を選択したことが前提となっています。[はい] を選択した場合は、次の手順の中の手順 3 に進み、手順に沿ってルートベース L2 VPN サーバ セッションの残りの設定を行います。

前提条件

- 続行する前に、L2 VPN サーバ サービスを設定する必要があります。[L2 VPN サーバ サービスの追加](#) を参照してください。
- 追加している L2 VPN サーバ セッションで使用するローカル エンドポイントおよび リモート IP アドレスの情報を取得します。ローカル エンドポイントを作成するには、[ローカル エンドポイントの追加](#)を参照してください。
- L2 VPN サーバ セッションで使用する事前共有キー (PSK) およびトンネル インターフェイス サブネットの値を取得します。

- 作成している L2 VPN サーバ セッションに接続する既存セグメントの名前を取得します。詳細については、[セグメントの追加](#)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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [L2 VPN セッション] タブに移動します。
- 3 [L2 VPN セッションの追加] - [L2 VPN サーバ] を選択します。
- 4 L2 VPN サーバ セッションの名前を入力します。
- 5 [L2 VPN サービス] ドロップダウン メニューから、L2 VPN セッションを作成している L2 VPN サーバ サービスを選択します。

注： この L2 VPN サーバ セッションを [L2VPN サーバ セッションの設定] ダイアログ ボックスから追加している場合、L2 VPN サーバ サービスは [L2 セッションの追加] ボタンの上にすでに示されています。

- 6 ドロップダウン メニューから既存のローカル エンドポイントを選択します。

別のローカル エンドポイントを作成する場合は、3 つのドットで示されるメニュー (⋮) をクリックして、[ローカル エンドポイントの追加] を選択します。
- 7 リモート サイトの IP アドレスを入力します。
- 8 L2 VPN サーバ セッションを有効または無効にするには、[管理状態] をクリックします。

この値はデフォルトで **有効** に設定されているため、L2 VPN サーバ セッションは NSX Edge ノードまで設定されます。
- 9 [プリシェアード キー] にプライベート キーの値を入力します。

注意： PSK 値には機密情報が含まれているため、PSK 値を共有して保存する場合は注意してください。

- 10 [トンネル インターフェイス] に IP サブネット アドレスを CIDR 形式で入力します。

例：4.5.6.6/24。このサブネット アドレスは必須です。
- 11 [リモート ID] の値を入力します。

証明書認証を使用するピア サイトの場合、この ID はピア サイトの証明書のコモン ネームにする必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。可能であれば、VPN のパブリック IP アドレス、または VPN サービスの FQDN を Remote ID として使用します。
- 12 特定のグループの一部としてこのセッションを含める場合は、[タグ] にタグ名を入力します。
- 13 VPN サービスの設定を続行する場合は、[保存] をクリックして、[はい] をクリックします。

[L2VPN セッションの追加] パネルに戻り、[セグメント] リンクを有効にできるようになりました。
- 14 既存のセグメントを L2 VPN サーバ セッションに接続します。
 - a [セグメント] - [セグメントの設定] の順にクリックします。
 - b [セグメントの設定] ダイアログ ボックスで [セグメントの設定] をクリックして、既存のセグメントを L2 VPN サーバ セッションに接続します。

- c [セグメント] ドロップダウン メニューから、セッションに接続する VNI ベースまたは VLAN ベースのセグメントを選択します。
- d [VPN トンネル ID] に、選択したセグメントの識別に使用する一意の値を入力します。
- e [保存] をクリックしてから、[閉じる] をクリックします。

[L2VPN セッションの設定] ペインまたはダイアログ ボックス内の L2 VPN サーバ セッションの [セグメント] 数が増加しました。

15 L2 VPN サーバ セッションの設定を終了するには、[編集を終了] をクリックします。

結果

[VPN サービス] タブで設定した L2 VPN サーバ サービスの [セッション] 数が増加しました。

次のステップ

L2 VPN サービスの設定を完了するには、クライアント モードで L2 VPN サービスを作成し、さらに L2 VPN クライアント セッションも作成する必要があります。[L2 VPN クライアント サービスの追加](#)および [L2 VPN クライアント セッションの追加](#)を参照してください。

L2 VPN クライアント セッションの追加

L2 VPN クライアント サービスを作成した後で、L2 VPN クライアント セッションを追加し、既存のセグメントに接続する必要があります。

次の手順では、NSX Manager ユーザー インターフェイスで [L2 VPN セッション] タブを使用して、L2 VPN クライアント セッションを作成します。L2 VPN クライアント セッションに接続する既存のローカル エンドポイントとセグメントも選択します。

注： L2 VPN クライアント サービスが正常に設定された後ですぐに L2 VPN クライアント セッションを追加することもできます。L2 VPN クライアントの設定を続行するよう求められたら、[はい] を選択し、[L2 VPN クライアント] パネルで [セッション] - [セッションの追加] の順に選択します。次の手順では、最初のいくつかの手順で、L2 VPN クライアントの設定を続行するよう求められたときに [いいえ] を選択した場合を想定しています。[はい] を選択した場合は、次の手順の手順 3 に進み、L2 VPN クライアント セッションの残りの設定を続行します。

前提条件

- 続行する前に、L2 VPN クライアント サービスが設定されている必要があります。[L2 VPN クライアント サービスの追加](#) を参照してください。
- 追加する L2 VPN クライアント セッションで使用するローカル IP アドレスとリモート IP アドレスの IP アドレス情報を取得します。
- L2 VPN サーバの設定中に生成されたピア コードを取得します。[リモート側の L2 VPN 構成ファイルのダウンロード](#) を参照してください。
- 作成する L2 VPN クライアント セッションに接続する既存のセグメントの名前を取得します。[セグメントの追加](#) 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [L2 VPN セッション] の順に選択します。
- 3 [L2 VPN セッションの追加] - [L2 VPN クライアント] を選択します。
- 4 L2 VPN クライアント セッションの名前を入力します。
- 5 [VPN サービス] ドロップダウン メニューから、L2 VPN セッションが関連付けられている L2 VPN クライアント サービスを選択します。

注： [L2VPN クライアント セッションの設定] ダイアログ ボックスからこの L2 VPN クライアント セッションを追加する場合、L2 VPN クライアント サービスは、[L2 セッションの追加] ボタンの上にすでに示されています。

- 6 [ローカル IP アドレス] テキスト ボックスに、L2 VPN クライアント セッションの IP アドレスを入力します。
- 7 L2 VPN クライアント セッションに使用される IPSec トンネルのリモート IP アドレスを入力します。
- 8 L2 VPN サーバ サービスの設定時に生成されたピア コードを [ピア設定] テキスト ボックスに入力します。
- 9 [管理状態] を有効または無効にします。

この値はデフォルトで **有効** に設定されているため、L2 VPN サーバ セッションは NSX Edge ノードまで設定されます。

- 10 VPN サービスの設定を続行する場合は、[保存] をクリックして、[はい] をクリックします。
- 11 既存のセグメントを L2 VPN クライアント セッションに接続します。
 - a [セグメント] - [セグメントの追加] の順に選択します。
 - b [セグメントの設定] ダイアログ ボックスで、[セグメントの追加] をクリックします。
 - c [セグメント] ドロップダウン メニューから、L2 VPN クライアント セッションに接続する VNI ベースまたは VLAN ベースのセグメントを選択します。
 - d [VPN トンネル ID] に、選択したセグメントの識別に使用する一意の値を入力します。
 - e [閉じる] をクリックします。

- 12 L2 VPN クライアント セッションの設定を完了するには、[編集を終了] をクリックします。

結果

[VPN サービス] タブで、設定済み L2 VPN クライアント サービスのセッション数が更新されます。

リモート側の L2 VPN 構成ファイルのダウンロード

L2 VPN クライアント セッションを構成するには、L2 VPN サーバ セッションを設定するときに生成されたピアコードを取得する必要があります。

前提条件

- L2 VPN サーバ サービスとセッションを正常に設定してから、処理を進める必要があります。[L2 VPN サーバ サービスの追加](#) 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [L2 VPN セッション] タブに移動します。
- 3 L2 VPN セッションのテーブルで、L2 VPN クライアント セッションの設定に使用する L2 VPN サーバ セッションの行を展開します。
- 4 [設定のダウンロード] をクリックして、警告ダイアログ ボックスで [はい] をクリックします。

L2VPNSession_<name-of-L2-VPN-server-session>_config.txt という名前のテキスト ファイルがダウンロードされます。このファイルには、リモート側 L2 VPN 構成のピア コードが含まれています。

注意： ピアコードには機密情報である PSK 値が含まれています。保存および共有する場合は、十分に注意してください。

たとえば、`L2VPNSession L2VPNServer config.txt` には次の設定が含まれています。

```
[
{
  "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/1-policyconnectivity-693/ipsec-vpn-services/IpssecService1/sessions/Routebase1",
  "peer_code":
    "MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFWsXAiOiIxNjkuMjU0LjY0LjIiLCJKc3RUYXBjcCI6IjE2OS4yNTQuNjQuMSIsImrlrZU9wdG1vbiI6ImrlrZXYYiIiwic2l0ZW5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0Iiwic2l0ZW5ja2FuZGUzLnRlcmlkIjoiaW50dGEuZmFzc2VudCkiLCJkbm91bnR5bGVzIjoiImdlbm91bnR5bGVzIiwiaWF0eSI6MTY5OTU0MDAwMDAifQ=="
}
]
```

- 5** L2 VPN クライアント サービスとセッションの設定に使用するピア コードをコピーします。

上記の構成ファイルの例では、L2 VPN クライアントの設定で使用するため、次のピア コードがコピーされています。

McW3ZjBjYzdJLHsic2l0ZU5hbWUiOiJsbnV0ZWJhc2UxIiwic3JjVGFWXSAiOiIxNjkumJyU0LjY0LjIiLCJkc3RUYXB
JcCI6IjE2OS4yNTQunJmMSIsImrlrZU9wdGl

vbiI6ImrlrZXxyIiwizw5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0IiwiZW5jcmlldEFuZERpZ2
VzdcI6ImFlcylnY20vc2hhLTllNiIsInBzayI

6IlZNd2FyzTEyMyIsInRlbm5lbHMtOlt7ImxvY2FsSWQiOiI2MC42MC42M4xiIiwicGVlcglkIjoINTAuNTAuNTAuMS
IsImxvY2FsVnRpSXAIoiIxNjkumi4yLjMvMzMifVl9

次のステップ

L2 VPN クライアントのサービスおよびセッションを構成します。[L2 VPN クライアント サービスの追加](#)および[L2 VPN クライアント セッションの追加](#)を参照してください。

ローカル エンドポイントの追加

設定する IPsec VPN で使用するローカル エンドポイントを構成する必要があります。

次の手順では、NSX Manager ユーザー インターフェイスの [ローカル エンドポイント] タブを使用します。3 つのドットで示されるメニュー (...) をクリックし、[ローカル エンドポイントの追加] を選択して、IPsec VPN セッションの追加中にローカル エンドポイントを作成することもできます。IPsec VPN セッションを設定している場合は、次の手順の中の手順 3 に進み、手順に沿って新しいローカル エンドポイントを作成します。

前提条件

- 設定中のローカル エンドポイントを使用する IPsec VPN セッションで証明書ベースの認証モードを使用する場合は、ローカル エンドポイントで使用する必要がある証明書についての情報を取得します。
- このローカル エンドポイントが関連付けられる IPsec VPN サービスが設定され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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [ローカル エンドポイント] に移動して、[ローカル エンドポイントの追加] をクリックします。
- 3 ローカル エンドポイントの名前を入力します。
- 4 [VPN サービス] ドロップダウン メニューから、このローカル エンドポイントが関連付けられている IPsec VPN サービスを選択します。
- 5 ローカル エンドポイントの IP アドレスを入力します。

Tier-0 ゲートウェイで実行されている IPsec VPN サービスの場合、ローカル エンドポイントの IP アドレスは、Tier-0 ゲートウェイのアップリンク インターフェイスと異なる IP アドレスを設定する必要があります。指定するローカル エンドポイントの IP アドレスは、Tier-0 ゲートウェイのループバック インターフェイスに関連付けられ、アップリンク インターフェイスを介してルーティング可能な IP アドレスとして公開されます。Tier-1 ゲートウェイで実行されている IPsec VPN サービスの場合、ローカル エンドポイントの IP アドレスをルーティング可能にするには、Tier-1 ゲートウェイの設定で IPsec ローカル エンドポイントのルート アドバタイズが有効になっている必要があります。詳細については、[Tier-1 ゲートウェイの追加](#)を参照してください。

- 6 IPsec VPN セッションに証明書ベースの認証モードを使用しする場合は、[サイトの証明書] ドロップダウン メニューからローカル エンドポイントで使用する証明書を選択します。
- 7 (オプション) 必要に応じて、[説明] に入力します。

8 [ローカル ID] に、ローカルの NSX Edge インスタンスの識別に使用する値を入力します。

このローカル ID がリモート サイトのピア ID になります。ローカル ID は、リモート サイトのパブリック IP アドレスまたは FQDN にする必要があります。ローカル エンドポイントを使用して定義された証明書ベースの VPN セッションの場合、ローカル ID はローカル エンドポイントに関連付けられている証明書から生成されます。[ローカル ID] テキスト ボックスに指定した ID は無視されます。VPN セッションの証明書から派生するローカル ID は、証明書に含まれている拡張機能によって異なります。

- 証明書に X509v3 拡張機能 `X509v3 Subject Alternative Name` が存在しない場合、識別名 (DN) がローカル ID 値として使用されます。
- 証明書に X509v3 拡張機能 `X509v3 Subject Alternative Name` がある場合、Subject Alternative Name の 1 つがローカル ID 値として取得されます。

9 [信頼されている CA (認証局) 証明書] と [証明書失効リスト] ドロップダウン メニューから、ローカル エンドポイントに必要な証明書を選択します。

10 必要に応じて、タグを指定します。

11 [保存] をクリックします。

プロファイルの追加

NSX-T Data Center は、IPsec VPN または L2 VPN サービスのいずれかの設定時にデフォルトで割り当てられるシステム生成の IPsec トンネル プロファイルおよび IKE プロファイルを提供します。IPsec VPN 設定用にシステム生成された DPD プロファイルが作成されます。

IKE および IPsec プロファイルは、ネットワーク サイト間の共有シークレット キーの認証、暗号化、および確立に使用されるアルゴリズムに関する情報を提供します。DPD プロファイルは、プローブ間で待機する時間に関する情報を秒単位で提供します。

NSX-T Data Center で提供されるデフォルトのプロファイルを使用しない場合は、このセクション内にあるトピックの情報をを使用して独自に設定できます。

IKE プロファイルの追加

インターネット キー交換 (IKE) プロファイルは、IKE トンネルの確立時にネットワーク サイト間の共有シークレット キーの認証、暗号化、および確立に使用されるアルゴリズムに関する情報を提供します。

NSX-T Data Center は、IPsec VPN または L2 VPN サービスの設定時にデフォルトで割り当てられるシステム生成の IKE プロファイルを提供します。次の表では、デフォルトで提供されるプロファイルを示します。

表 5-4. IPsec VPN または L2 VPN サービスで使用されるデフォルトの IKE プロファイル

デフォルトの IKE プロファイル名	説明
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> ■ L2 VPN サービス構成で使用されます。 ■ IKE V2、AES 128 暗号化アルゴリズム、SHA 2 256 アルゴリズム、および Diffie-Hellman グループ 14 キー交換アルゴリズムで設定されます。
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> ■ IPsec VPN サービス構成で使用されます。 ■ IKE V2、AES 128 暗号化アルゴリズム、SHA2 256 アルゴリズム、および Diffie-Hellman グループ 14 キー交換アルゴリズムで設定されます。

デフォルトの IKE プロファイルではなく、NSX-T Data Center 2.5 以降でサポートされるコンプライアンススイートのいずれかを選択することもできます。詳細については、[サポートされているコンプライアンススイートについて](#)を参照してください。

デフォルトで提供される IKE プロファイルまたはコンプライアンススイートを使用しない場合は、次の手順に従って独自の IKE 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [プロファイル] タブの順にクリックします。
- 3 プロファイルタイプに [IKE プロファイル] を選択し、[IKE プロファイルの追加] をクリックします。
- 4 IKE プロファイルの名前を入力します。
- 5 [IKE バージョン] ドロップダウンメニューから、使用する IKE バージョンを選択して、IPsec プロトコルスイートでセキュリティアソシエーション (SA) を設定します。

表 5-5. IKE バージョン

IKE バージョン	説明
IKEv1	選択すると、IPsec VPN が開始され、IKEv1 プロトコルのみに応答します。
IKEv2	これがデフォルトのバージョンです。選択すると、IPsec VPN が開始され、IKEv2 プロトコルのみに応答します。
IKE-Flex	このバージョンを選択すると、IKEv2 プロトコルでトンネルの確立に失敗した場合に、送信元サイトにフォールバックされず、IKEv1 プロトコルで接続が開始されます。リモートサイトから IKEv1 プロトコルで接続を開始した場合、接続は許可されます。

- 6 ドロップダウン メニューから暗号化、ダイジェスト、および Diffie-Hellman グループ アルゴリズムを選択します。複数のアルゴリズムを選択して適用したり、選択したアルゴリズムを適用しない場合に選択解除したりできます。

表 5-6. 使用するアルゴリズム

アルゴリズムのタイプ	有効な値	説明
暗号化	<ul style="list-style-type: none"> ■ AES 128 (デフォルト) ■ AES 256 ■ AES GCM 128 ■ AES GCM 192 ■ AES GCM 256 	<p>インターネット キー交換 (IKE) ネゴシエーション実行中に使用される暗号化アルゴリズム。</p> <p>AES-GCM アルゴリズムは IKEv2 でサポートされます。IKEv1 ではサポートされません。</p>
ダイジェスト	<ul style="list-style-type: none"> ■ SHA2 256 (デフォルト) ■ SHA 1 ■ SHA2 384 ■ SHA2 512 	<p>IKE ネゴシエーションの実行中に使用されるセキュア ハッシュ アルゴリズム。</p> <p>[暗号化アルゴリズム] テキスト ボックスで暗号化アルゴリズムとして AES-GCM のみが選択されている場合、RFC 5282 のセクション 8 の仕様のため、[ダイジェスト アルゴリズム] テキスト ボックスでハッシュ アルゴリズムを指定できません。擬似乱数関数 (PRF) アルゴリズムの HMAC-SHA2-256 が暗黙的に選択され、IKE セキュリティ アソシエーション (SA) のネゴシエーションで使用されます。IKE SA ネゴシエーションのフェーズ 1 を成功させるには、ピア ゲートウェイで PRF-HMAC-SHA2-256 アルゴリズムも設定する必要があります。</p> <p>[暗号化アルゴリズム] テキスト ボックスで、AES-GCM アルゴリズムの他に複数のアルゴリズムが指定されている場合、[ダイジェスト アルゴリズム] テキスト ボックスで 1 つ以上のハッシュ アルゴリズムを選択できます。IKE SA ネゴシエーションで使用する PRF アルゴリズムは、設定したハッシュ アルゴリズムに基づいて暗黙的に決まります。IKE SA ネゴシエーションのフェーズ 1 を成功させるには、照合する 1 つ以上の PRF アルゴリズムをピア ゲートウェイで設定する必要があります。たとえば、[暗号化アルゴリズム] テキスト ボックスで AES 128 と AES GCM 128 が選択され、[ダイジェスト アルゴリズム] テキスト ボックスに SHA1 が指定されている場合、IKE SA ネゴシエーションで PRF-HMAC-SHA1 アルゴリズムが使用されます。これは、ピア ゲートウェイでも設定する必要があります。</p>
Diffie-Hellman グループ	<ul style="list-style-type: none"> ■ グループ 14 (デフォルト) ■ グループ 2 ■ グループ 5 ■ グループ 15 ■ グループ 16 ■ グループ 19 ■ グループ 20 ■ グループ 21 	<p>ピア サイトおよび NSX Edge がセキュアでない通信チャネルを介して共有シークレット キーを確立するために使用する暗号化スキーム。</p>

注: 2つの暗号化アルゴリズムまたは2つのダイジェストアルゴリズムを使用して GUARD VPN Client (旧称 QuickSec VPN Client) と IPsec VPN トンネルを確立しようとする、GUARD VPN Client が提案するネゴシエーション リストに別のアルゴリズムが追加されます。たとえば、IPsec VPN トンネルの確立に使用される IKE プロファイルに暗号化アルゴリズムとして AES 128 と AES 256 を指定し、ダイジェストアルゴリズムとして SHA2 256 と SHA2 512 を指定した場合、GUARD VPN Client はネゴシエーション リストに AES 192 と SHA2 384 を追加します。この場合、NSX-T Data Center が IPsec VPN トンネルを確立するときに、ユーザーが選択した最初の暗号化アルゴリズムが使用されます。

- 7 デフォルト値の 86,400 秒 (24 時間) を変更する場合は、セキュリティ アソシエーション (SA) の有効期間の値を秒単位で入力します。
- 8 必要に応じて説明を入力し、タグを追加します。
- 9 [保存] をクリックします。

結果

利用可能な IKE プロファイルのテーブルに新しい行が追加されます。システム以外で作成されたプロファイルを編集または削除するには、3つのドットで示されるメニュー (⋮) をクリックし、利用可能なアクションのリストから選択します。

IPsec プロファイルの追加

インターネット プロトコル セキュリティ (IPsec) プロファイルは、IPsec トンネルの確立時にネットワーク サイト間の共有シークレット キーの認証、暗号化、および確立に使用されるアルゴリズムに関する情報を提供します。

NSX-T Data Center は、IPsec VPN または L2 VPN サービスの設定時にデフォルトで割り当てられるシステム生成の IPsec プロファイルを提供します。次の表では、デフォルトで提供される IPsec プロファイルを示します。

表 5-7. IPsec VPN または L2 VPN サービスで使用されるデフォルトの IPsec プロファイル

デフォルトの IPsec プロファイルの名前	説明
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> ■ L2 VPN で使用されます。 ■ AES GCM 128 暗号化アルゴリズムと Diffie-Hellman グループ 14 キー交換アルゴリズムで設定されます。
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> ■ IPsec VPN で使用されます。 ■ AES GCM 128 暗号化アルゴリズムと Diffie-Hellman グループ 14 キー交換アルゴリズムで設定されます。

デフォルトの IPsec プロファイルではなく、NSX-T Data Center 2.5 以降でサポートされるコンプライアンススイートのいずれかを選択することもできます。詳細については、[サポートされているコンプライアンススイートについて](#)を参照してください。

デフォルトで提供される IPsec プロファイルまたはコンプライアンススイートを使用しない場合は、次の手順に従って独自の設定を行うことができます。

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 [ネットワーク] - [VPN] - [プロファイル] タブに移動します。
- 3 プロファイル タイプに [IPsec プロファイル] を選択し、[IPsec プロファイルの追加] をクリックします。
- 4 IPsec プロファイルの名前を入力します。
- 5 ドロップダウン メニューから、暗号化、ダイジェスト、および Diffie-Hellman アルゴリズムを選択します。複数のアルゴリズムを選択して適用することができます。

使用しないアルゴリズムを選択解除します。

表 5-8. 使用するアルゴリズム

アルゴリズムのタイプ	有効な値	説明
暗号化	<ul style="list-style-type: none"> ■ AES GCM 128 (デフォルト) ■ AES 128 ■ AES 256 ■ AES GCM 192 ■ AES GCM 256 ■ 暗号化認証なし (AES GMAC 128) ■ 暗号化認証なし (AES GMAC 192) ■ 暗号化認証なし (AES GMAC 256) ■ 暗号化なし 	Internet Protocol Security (IPSec) ネゴシエーション実行中に使用される暗号化アルゴリズム。
ダイジェスト	<ul style="list-style-type: none"> ■ SHA 1 ■ SHA2 256 ■ SHA2 384 ■ SHA2 512 	IPSec ネゴシエーションの実行中に使用されるセキュア ハッシュ アルゴリズム。
Diffie-Hellman グループ	<ul style="list-style-type: none"> ■ グループ 14 (デフォルト) ■ グループ 2 ■ グループ 5 ■ グループ 15 ■ グループ 16 ■ グループ 19 ■ グループ 20 ■ グループ 21 	ピア サイトおよび NSX Edge がセキュアでない通信チャネルを介して共有シークレット キーを確立するために使用する暗号化スキーム。

- 6 VPN サービスで PFS グループ プロトコルを使用しない場合は、[PFS グループ] を選択解除します。
デフォルトで選択されています。
- 7 [SA の有効期間] テキスト ボックスで、デフォルトの秒数を変更してから、IPsec トンネルを再確立する必要があります。

SA の有効期間のデフォルト値には、24 時間 (86,400 秒) が使用されます。
- 8 IPsec トンネルで使用する [DF ビット] の値を選択します。

この値によって、受信データ パケットに含まれる「フラグメント化しない (DF)」ビットを処理する方法が決まります。次の表に、許容値を示します。

表 5-9. DF ビット値

DF ビット値	説明
COPY	デフォルト値です。この値を選択すると、NSX-T Data Center は受信パケットの DF ビットの値を転送するパケットにコピーします。この値は、暗号化の後に受信データ パケットに DF ビットが設定されると、パケットにも DF ビットが設定されることを意味します。
CLEAR	この値を選択すると、NSX-T Data Center は受信データ パケットの DF ビット値を無視します。暗号化パケットでは、DF ビットが常に 0 になります。

9 説明を入力し、必要に応じてタグを追加します。

10 [保存] をクリックします。

結果

利用可能な IPsec プロファイルのテーブルに新しい行が追加されます。システム以外で作成されたプロファイルを編集または削除するには、3 つのドットで示されるメニュー (...) をクリックし、利用可能なアクションのリストから選択します。

DPD プロファイルの追加

DPD (Dead Peer Detection) プロファイルは、IPsec ピアが稼動しているかどうかを検出するためにプローブ間で待機する秒数についての情報を提供します。

NSX-T Data Center には、`nsx-default-l3vpn-dpd-profile` という名前のシステム生成 DPD プロファイルがあり、IPsec VPN サービスを設定するときにデフォルトで割り当てられます。

提供されるデフォルトの DPD プロファイルを使用しない場合は、次の手順を使用して独自の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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [VPN] - [プロファイル] に移動します。
- 3 プロファイル タイプとして [DPD プロファイル] を選択し、[DPD プロファイルの追加] をクリックします。
- 4 DPD プロファイルの名前を入力します。
- 5 [DPD プローブ間隔] テキストボックスに、NSX-T Data Center が次の DPD プローブを送信するまで待機時間を秒単位で入力します。デフォルトは 60 秒です。

NSX Edge ノードがリモート ピア サイトからの応答を受信すると、DPD プローブ間隔タイマーが再起動します。次の DPD プローブが送信されてから 0.5 秒以内に、NSX Edge ノードがピア サイトからの応答を受信しないと、再転送タイマーが 0.5 秒に設定されます。再転送タイマーに達すると、NSX Edge ノードは次の DPD プローブを再転送します。リモート ピア サイトから応答がないと、再転送タイマーが急増します（最大で 6 秒まで）。再転送タイマーが期限切れになるたびに、NSX Edge ノードは DPD プローブの再転送を行います。30 回再転送を繰り返しても期限切れになる場合、NSX Edge ノードはピア サイトの停止を宣言し、停止したピアのリンクでセキュリティ アソシエーション (SA) を解除します。DPD プローブの再転送を 30 回行った場合の合計時間は約 2 分 45 秒です。

6 必要に応じて説明を入力し、タグを追加します。

7 [保存] をクリックします。

結果

使用可能な DPD プロファイルのテーブルに新しい行が追加されます。システム以外で作成されたプロファイルを編集または削除するには、3 つのドットで示されるメニュー (⋮) をクリックし、利用可能なアクションのリストから選択します。

L2 VPN クライアントとしての自律 Edge の追加

L2 VPN を使用して、NSX-T Data Center で管理されていないサイトにレイヤー 2 ネットワークを拡張できます。自律 NSX Edge は、L2 VPN クライアントとしてサイトに展開できます。自律 NSX Edge は展開が容易で、プログラミングも簡単です。これにより、高パフォーマンスの VPN を実現できます。自律 NSX Edge を展開するには、NSX-T Data Center で管理されていないホストで OVF ファイルを使用します。また、プライマリとセカンダリの自律 L2 VPN Edge クライアントを展開することで、VPN の冗長性による HA が可能になります。

前提条件

- ポート グループを作成して、ホストの vSwitch に割り当てます。
- 内部 L2 拡張ポートのポート グループを作成します。
- 追加する L2 VPN クライアント セッションで使用するローカル IP とリモート IP の IP アドレスを取得します。
- L2 VPN サーバの設定中に生成されたピア コードを取得します。

手順

- 1 vSphere Web Client を使用して、非 NSX 環境を管理する vCenter Server にログインします。
- 2 [ホストおよびクラスタ] を選択し、クラスタを展開して、利用可能なホストを表示します。
- 3 自律 NSX Edge をインストールするホストを右クリックして、[OVF テンプレートのデプロイ] を選択します。
- 4 URL を入力し、インターネットから OVF ファイルをダウンロードしてインストールするか、[参照] をクリックし、自律 NSX Edge OVF ファイルが格納されているコンピュータ上のフォルダに移動して、[次へ] をクリックします。
- 5 [名前およびフォルダの選択] ページで、自律 NSX Edge の名前を入力して、展開先のフォルダまたはデータセンターを選択します。その後、[次へ] をクリックします。
- 6 [コンピューティング リソースの選択] 画面で、コンピューティング リソースの宛先を選択します。
- 7 [OVF テンプレートの詳細] 画面でテンプレートの詳細を確認し、[次へ] をクリックします。
- 8 [設定] 画面で、展開設定オプションを選択します。
- 9 [ストレージの選択] 画面で、設定とディスク ファイルを格納する場所を選択します。

- 10 [ネットワークの選択] 画面で、展開したテンプレートで使用するネットワークを設定します。アップリンク インターフェイス用に作成したポート グループ、L2 拡張ポート用に作成したポート グループを選択し、HA インターフェイスを入力します。[次へ] をクリックします。

- 11 [テンプレートのカスタマイズ] 画面で次の値を入力し、[次へ] をクリックします。

- a CLI の admin パスワードを 2 回入力します。
- b CLI を有効にするためのパスワード 2 回入力します。
- c CLI の root パスワードを 2 回入力します。
- d 管理ネットワークの IPv4 アドレスを入力します。
- e 終了インターフェイスが、アップリンク インターフェイスのポート グループのネットワークにマッピングされるように、[外部ポート] の詳細 (VLAN ID、終了インターフェイス、IP アドレス、IP プリフィックス長) を入力します。

終了インターフェイスがトランク ポート グループに接続している場合は、VLAN ID を指定します。たとえば、**20,eth2,192.168.5.1,24** と入力します。VLAN ID を使用してポート グループを設定し、[外部ポート] に VLAN 0 を使用することもできます。

- f (オプション) 高可用性を設定するには、終了インターフェイスが適切な HA ネットワークにマッピングされるように、[HA ポート] の詳細を入力します。
- g (オプション) HA のセカンダリ ノードとして自律 NSX Edge を展開する場合は、[この自律 Edge をセカンダリ ノードとして展開する] を選択します。

プライマリ ノードと同じ OVF ファイルを使用し、プライマリ ノードの IP アドレス、ユーザー名、パスワード、サムプリントを入力します。

プライマリ ノードのサムプリントを取得するには、プライマリ ノードにログインし、次のコマンドを実行します。

```
get certificate api thumbprint
```

プライマリ ノードとセカンダリ ノードの VTEP IP アドレスが同じサブネットにあり、同じポート グループに接続していることを確認します。展開が完了して セカンダリ Edge を起動すると、プライマリ ノードに接続して Edge クラスタを形成します。

- 12 [設定内容の確認] 画面で自律 Edge の設定を確認し、[終了] をクリックします。

注： 展開中にエラーが発生した場合は、今日のメッセージが CLI に表示されます。また、API 呼び出しを使用してエラーを確認することもできます。

```
GET https://<nsx-mgr>/api/v1/node/status
```

これらのエラーは、ソフト エラーとハード エラーに分類されます。必要に応じて API 呼び出しを使用して、ソフト エラーを解決します。API 呼び出しを使用して、今日のメッセージをクリアできます。

```
POST /api/v1/node/status?action=clear_bootup_error
```

- 13 自律 NSX Edge アプライアンスをパワーオンします。

- 14 自律 NSX Edge クライアントにログインします。
 - 15 [L2VPN] - [セッションの追加] の順に選択し、次の値を入力します。
 - a セッション名を入力します。
 - b ローカル IP アドレスとリモート IP アドレスを入力します。
 - c L2 VPN サーバからピア コードを入力します。ピア コードの取得方法については、[リモート側の L2 VPN 構成ファイルのダウンロード](#)を参照してください。
 - 16 [保存] をクリックします。
 - 17 [ポート] - [ポートの追加] の順に選択して、L2 拡張ポートを作成します。
 - 18 名前と VLAN を入力し、終了インターフェイスを選択します。
 - 19 [保存] をクリックします。
 - 20 [L2 VPN] - [ポートに接続] の順に選択し、次の値を入力します。
 - a 作成した L2 VPN セッションを選択します。
 - b 作成した L2 拡張ポートを選択します。
 - c トンネル ID を入力します。
 - 21 [接続] をクリックします。
- 複数の L2 ネットワークを拡張する場合は、追加の L2 拡張ポートを作成してセッションに接続できます。
- 22 ブラウザを使用して自律 NSX Edge にログインするか、API 呼び出しを使用して L2 VPN セッションの状態を表示します。

注： L2 VPN サーバの設定が変更された場合は、ピア コードを再度ダウンロードして、新しいピア コードでセッションを更新してください。

IPsec VPN セッションの認識された状態の確認

IPsec VPN セッションに対する設定更新要求を送信した後に、要求された状態がトランスポート ノードの NSX-T Data Center のローカル制御プレーンで正常に処理されたかどうかを確認できます。

IPsec VPN セッションを作成するときに、IKE プロファイル、DPD プロファイル、トンネル プロファイル、ローカル エンドポイント、IPsec VPN サービス、IPsec VPN セッションなどの複数のエンティティが作成されます。これらすべてのエンティティで同じ `IPSecVPNSession SPAN` が共有されるため、同じ GET API 呼び出しを使用して、IPsec VPN セッションのすべてのエンティティの認識状態を取得することができます。API のみを使用して認識状態を確認することができます。

前提条件

- IPsec VPN について理解しておく必要があります。[IPsec VPN の理解](#) を参照してください。
- IPsec VPN が正常に設定されていることを確認します。[IPsec VPN サービスの追加](#) を参照してください。
- NSX Manager API にアクセスできる

手順

- 1 POST、PUT、または DELETE 要求 API 呼び出しを送信します。

次はその例です。

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
      "id": "1026",
      "sources": [
        {
          "subnet": "1.1.1.0/24"
        }
      ],
      "logged": true,
      "destinations": [
        {
          "subnet": "2.1.4..0/24"
        }
      ],
      "action": "PROTECT",
      "enabled": true,
      "_revision": 1
    }
  ]
}
```

- 2 返された応答ヘッダー内で x-nsx-requestid の値を検索して、コピーします。

次はその例です。

```
x-nsx-requestid    e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 次の GET 呼び出しを使用して、IPsec VPN セッションの認識状態を要求します。

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

次の API 呼び出しでは、以前の手順で使用した例の id と x-nsx-requestid の値を使用します。

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?
request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

次に、認識状態が `in_progress` の場合に受信する応答の例を示します。

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebe174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ],
  "state": "in_progress",
  "failure_message": "The state realization is in progress at transport nodes."
}
```

次に、認識状態が `in_sync` の場合に受信する応答の例を示します。

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ],
  "state": "in_sync"
}
```

次に、認識状態が `unknown` の場合に受信する可能性のある応答の例を示します。

```
{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation after some time."
}
```

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable to get response from the node. Please retry operation after some time."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",

```

```

        "state": "in_sync"
    }
],
"state": "unknown",
"failure_message": "The state realization is unknown at transport nodes"
}

```

エンティティの DELETE 操作を実行した後に、次の例のような NOT_FOUND の状態を受信する可能性があります。

```

{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}

```

セッションに関連付けられている IPsec VPN サービスが無効な場合は、次の例のような BAD_REQUEST 応答を受信します。

```

{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization status."
}

```

VPN セッションの監視とトラブルシューティング

IPsec または L2 VPN のセッションを設定した後に、NSX Manager ユーザー インターフェイスを使用して VPN トンネルの状態を監視し、報告されたトンネルに関するすべての問題のトラブルシューティングを行うことができます。

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 [ネットワーク] - [VPN] - [IPsec セッション] または [ネットワーク] - [VPN] - [L2 VPN セッション] タブに移動します。
- 3 監視またはトラブルシューティングを行う VPN セッションの行を展開します。
- 4 VPN トンネルの状態を表示するには、情報アイコンをクリックします。
[状態] ダイアログ ボックスが開き、状態が表示されます。
- 5 VPN トンネルのトラフィック統計情報を表示するには、[状態] 列で [統計情報の表示] をクリックします。
[統計情報] ダイアログ ボックスに、VPN トンネルのトラフィック統計情報が表示されます。
- 6 エラーの統計情報を表示するには、[統計情報] ダイアログ ボックスの [詳細を表示] リンクをクリックします。

- 7 [統計情報] ダイアログ ボックスを閉じるには、[閉じる] をクリックします。

ネットワーク アドレス変換

6

ネットワーク アドレス変換 (NAT) は、IP アドレス空間を別の IP アドレス空間にマッピングします。NAT は、Tier-0 と Tier-1 ゲートウェイ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。

■ ゲートウェイでの NAT の設定

ゲートウェイでの NAT の設定

Tier-0 または Tier-1 ゲートウェイに送信元 NAT (SNAT)、宛先 NAT (DNAT)、または再帰 NAT を設定できます。

Tier-0 ゲートウェイがアクティブ/アクティブモードで実行されている場合、非対称のパスがあると問題が生じる可能性があるため、SNAT または DNAT を設定できません。設定できるのは、再帰 NAT (別名、ステートレス NAT) のみです。Tier-0 ゲートウェイがアクティブ/スタンバイ モードで実行されている場合は、SNAT、DNAT、または再帰 NAT を設定できます。

また、IP アドレスやアドレス範囲の SNAT または DNAT を無効にすることもできます。アドレスに複数の NAT ルールが設定されている場合は、優先順位が最も高いルールが適用されます。

注： DNAT は、ポリシーベースの IPsec VPN が設定されている Tier-1 ゲートウェイでサポートされていません。

Tier-0 ゲートウェイの外部インターフェイスに設定された SNAT は、Tier-1 ゲートウェイからのトラフィックと、Tier-0 ゲートウェイの別の外部インターフェイスからのトラフィックを処理します。

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 [ネットワーク] - [NAT] の順に選択します。
- 3 ゲートウェイを選択します。
- 4 [NAT ルールを追加] をクリックします。
- 5 アクションを選択します。

Tier-1 ゲートウェイで使用できるアクションは、[SNAT]、[DNAT]、[再帰]、[SNAT なし]、および [DNAT なし] です。

アクティブ/スタンバイ モードの Tier-O ゲートウェイで使用するアクションは、[SNAT]、[DNAT]、[SNAT なし]、および [DNAT なし] です。

アクティブ/アクティブ モードの Tier-O ゲートウェイで使用するアクションは、[再帰] です。

6 [サービス] 列で [設定] をクリックして、サービスを選択します。

7 (必須) [送信元の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。

このフィールドを空白にしておくと、この NAT ルールはローカル サブネットの外部のすべての送信元に適用されます。

8 [宛先の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。

9 [変換された IP アドレス] に、IP アドレスまたは IP アドレスの範囲を CIDR 形式で指定します。

10 [変換されたポート] に値を入力します。

11 次のオプションからファイアウォール設定を選択します。

- [外部アドレスと一致]：パケットは、変換された IP アドレスとポートの組み合わせに一致するファイアウォール ルールによって処理されます。
 - SNAT の場合、NAT 実行後の変換された送信元アドレスが外部アドレスになります。
 - DNAT の場合、NAT 実行前の元の宛先アドレスが外部アドレスになります。
 - 再帰の場合、出力方向トラフィックに対しては、NAT 完了後の変換された送信元アドレスにファイアウォールが適用されます。入力方向トラフィックの場合は、NAT 完了前の元の宛先アドレスにファイアウォールが適用されます。
- [内部アドレスと一致]：パケットは、元の IP アドレスとポートの組み合わせに一致するファイアウォール ルールによって処理されます。
 - SNAT の場合、NAT 実行前の元の送信元アドレスが内部アドレスになります。
 - DNAT の場合、NAT 実行後の変換された宛先アドレスが内部アドレスになります。
 - 再帰の場合、出力方向トラフィックに対しては、NAT 完了前の元の送信元アドレスにファイアウォールが適用されます。入力方向トラフィックの場合は、NAT 完了後の変換された宛先アドレスにファイアウォールが適用されます。
- [バイパス]：パケットは、ファイアウォール ルールをバイパスします。

12 (必須) ログの収集状態を変更します。

13 (必須) [適用先] には、このルールが適用されるオブジェクトを選択します。

使用可能なオブジェクトは、[Tier-O ゲートウェイ]、[インターフェイス]、[ラベル]、[サービス インスタンスのエンドポイント]、および [仮想エンドポイント] です。

14 優先順位を指定します。

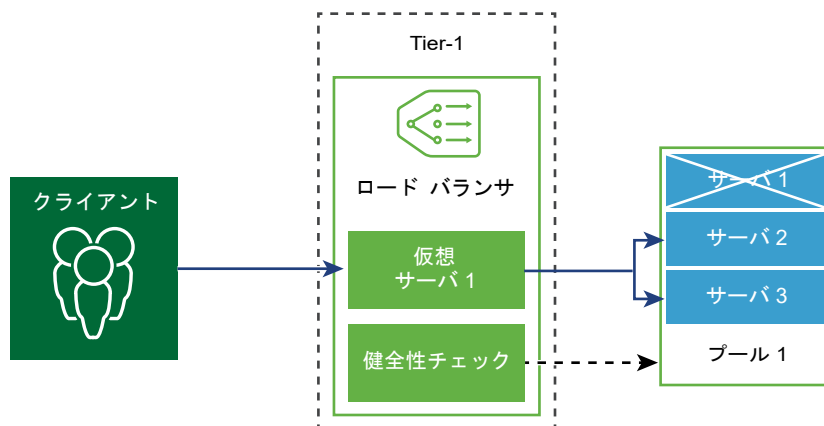
小さい値ほど、優先順位が高くなります。デフォルトは 100 です。

15 [保存] をクリックします。

ロード バランシング

7

NSX-T Data Center 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、最適ナ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 ゲートウェイ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 ゲートウェイ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。

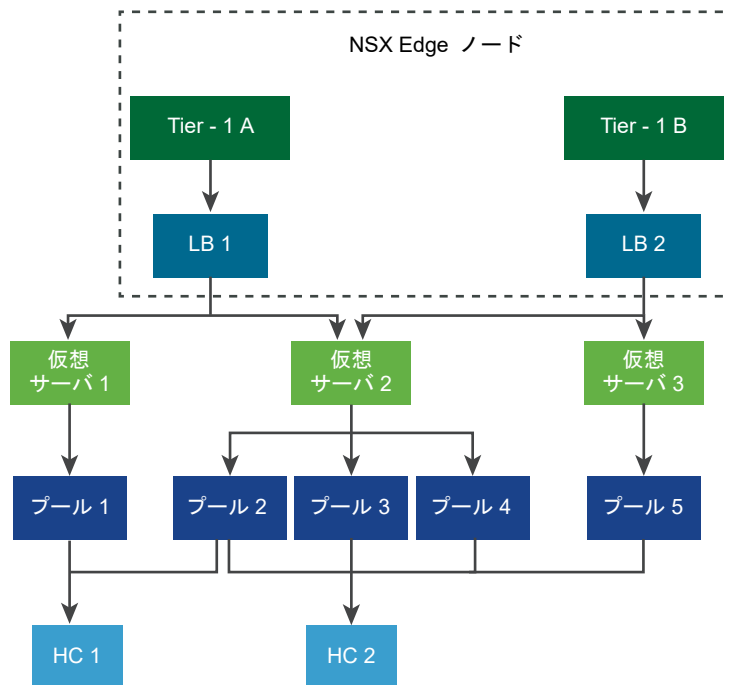
- キー ロード バランサの概念
- ロード バランサ コンポーネントの設定
- サーバ プールと仮想サーバに作成されたグループ

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 バランサを構成するときに、サイズ (Small, Medium, Large のいずれか) を指定できます。このサイズにより、ロード バランサがサポートできる仮想サーバ、サーバ プール、プール メンバーの数が決まります。

ロード バランサは Tier-1 ゲートウェイで実行されます。このゲートウェイはアクティブ/スタンバイ モードである必要があります。ゲートウェイは NSX Edge ノードで実行されます。NSX Edge ノード (ベアメタル、Small、Medium、または Large) のフォーム ファクタに、NSX Edge ノードがサポートできるロード バランサの数が決まります。[ネットワークとセキュリティの詳細設定] タブでは、ゲートウェイを表す用語として、論理ルーターが使用されています。

ロード バランシングの規模と NSX Edge フォーム ファクタでサポートされる内容については、<https://configmax.vmware.com> を参照してください。

本番環境の場合、Small NSX Edge ノードで Small ロード バランサを実行することはおすすめしません。

API を呼び出して、NSX Edge ノードのロード バランサの使用量に関する情報を取得できます。[ネットワーク] タブを使用してロード バランシングを構成する場合は、次のコマンドを実行します。

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

[ネットワークとセキュリティの詳細設定] タブを使用してロード バランシングを構成する場合は、次のコマンドを実行します。

```
GET /api/v1/loadbalancer/usage-per-node/<node-id>
```

使用量の情報には、ノードで設定されているロード バランサ オブジェクト（ロード バランサ サービス、仮想サーバ、サーバ プール、プール メンバーなど）の数が含まれます。詳細については、『NSX-T Data Center API ガイド』を参照してください。

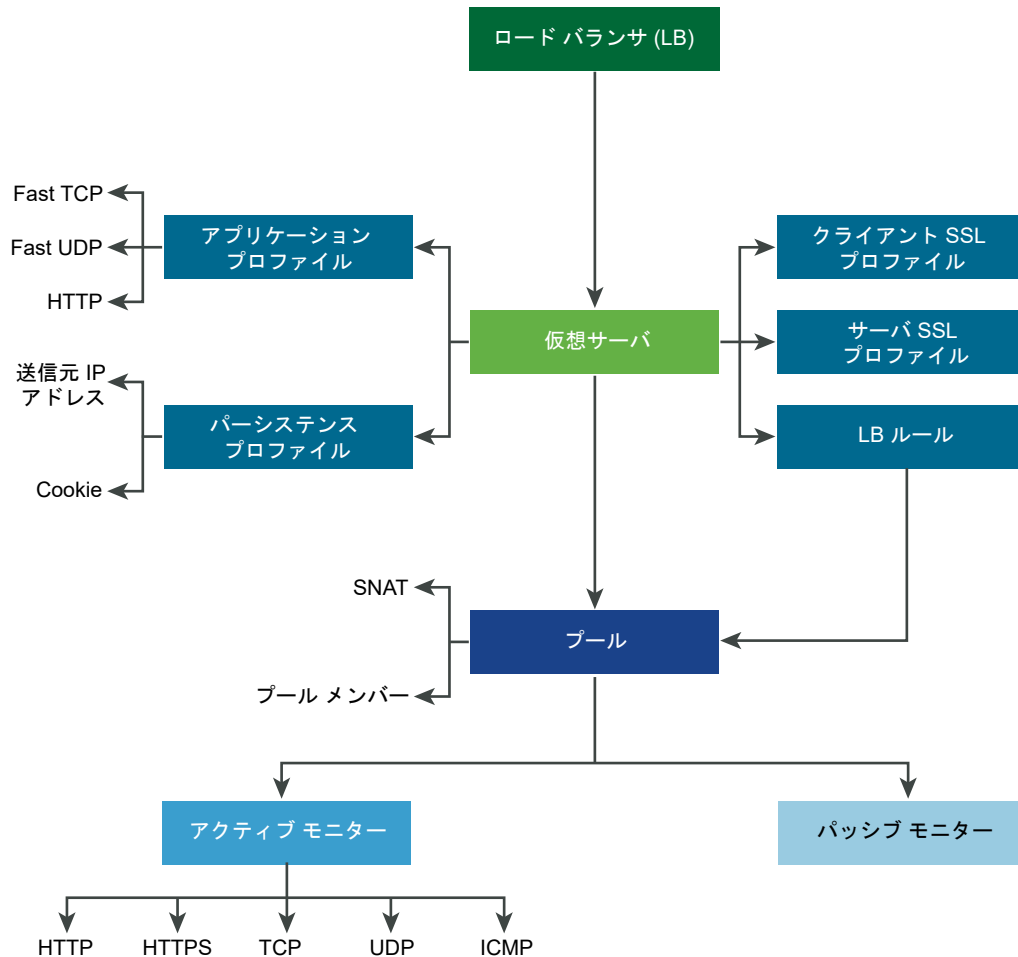
サポートされているロード バランサの機能

NSX-T Data Center 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（NS グループを使用）
- 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 リスト
- HTTP アップグレード - WebSocket など、HTTP アップグレードを使用するアプリケーションの場合は、クライアントまたはサーバによって HTTP アップグレードが要求されますが、この動作はサポートされています。デフォルトでは、NSX-T Data Center は HTTP アプリケーション プロファイルを使用して、クライアントによる HTTPS アップグレード要求をサポートし、受け入れます。

ロード バランサでは、非アクティブなクライアント通信またはサーバ通信を検出するために、60 秒に設定された HTTP アプリケーション プロファイルの応答タイムアウト機能を使用します。サーバから 60 秒間隔でトラフィックが送信されない場合、NSX-T Data Center ではクライアント側とサーバ側で接続を終了します。

注：SSL - NSX-T Data Center Limited Export Release 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。

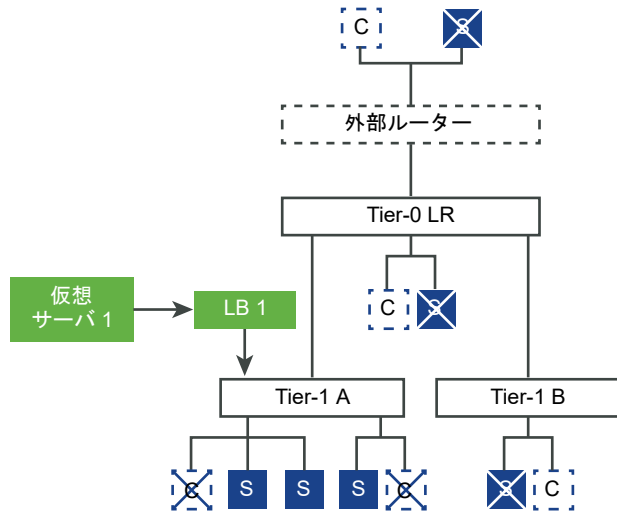


ロード バランサ トポロジ

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。ワンアーム モードでは仮想サーバの送信元 NAT (SNAT) 構成が必要ですが、インライン モードでは必要ありません。

インライン トポロジ

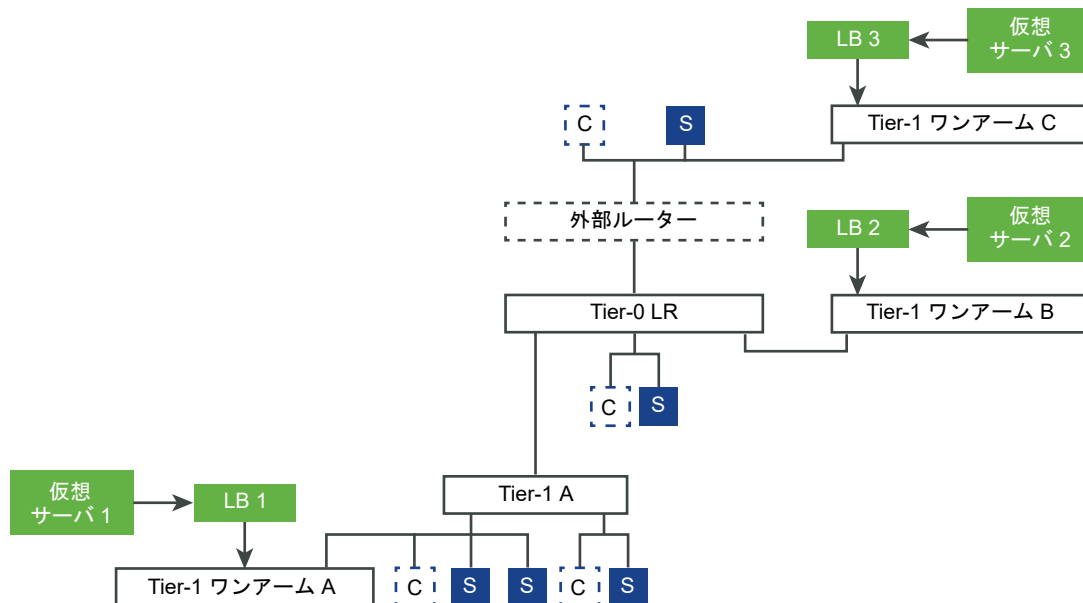
インライン モードでは、ロード バランサはクライアントとサーバ間のトラフィック パスに配置します。ロード バランサで SNAT を使用しない場合は、クライアントとサーバを同じ Tier-1 論理ルーターのオーバーレイ セグメントに接続しないようにします。クライアントとサーバを同じ Tier-1 論理ルーターのオーバーレイ セグメントに接続する場合は、SNAT が必要です。



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ます。ロード バランサがその応答をクライアントに転送します。



Tier-1 サービス チェーン

Tier-1 ゲートウェイまたは論理ルーターが、NAT、ファイアウォール、ロード バランサなどの異なるサービスをホストしている場合、サービスは次の順序で適用されます。

■ 入力方向 (Ingress)

DNAT - ファイアウォール - ロード バランサ

注：DNAT でファイアウォールの回避が設定されている場合、ファイアウォールはスキップされますが、ロード バランサはスキップされません。

■ 出力方向

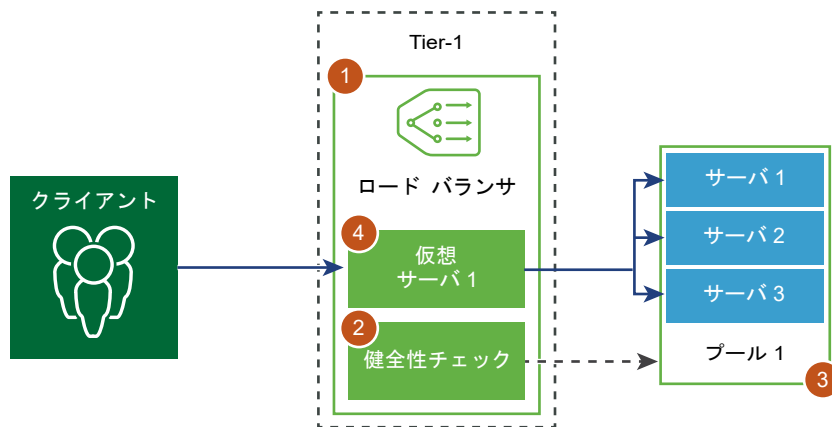
ロード バランサ - ファイアウォール - SNAT

ロード バランサ コンポーネントの設定

論理ロード バランサを使用するには、最初にロード バランサを設定して、Tier-1 ゲートウェイに接続する必要があります。

注： [詳細とセキュリティ] タブでは、Tier-1 ゲートウェイを表すのに、Tier-1 論理ルーターという用語が使用されています。

次に、サーバに対する健全性チェック監視を設定します。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 バランサのレイヤー 4 またはレイヤー 7 仮想サーバを作成し、新しく作成した仮想サーバをロード バランサに接続する必要があります。



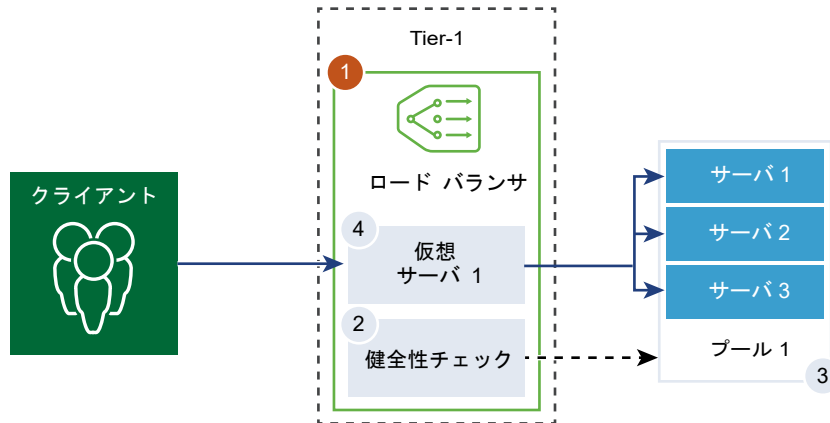
ロード バランサの追加

ロード バランサが作成され、Tier-1 ゲートウェイに接続されています。

注： [詳細とセキュリティ] タブでは、Tier-1 ゲートウェイを表すのに、Tier-1 論理ルーターという用語が使用されています。

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 ゲートウェイが設定されていることを確認します。3 章 [Tier-1 ゲートウェイ](#) 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [ロード バランサの追加] を選択します。
- 3 ロード バランサの名前と説明を入力します。
- 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 メニューからこのロード バランサに接続する構成済みの Tier-1 ゲートウェイを選択します。

Tier-1 ゲートウェイはアクティブ/スタンバイ モードにする必要があります。

- 6 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。

- 7 (オプション) タグを入力して検索しやすくします。

タグを指定して、タグの範囲を設定できます。

- 8 [保存] をクリックします。

ロード バランサの作成やロード バランサと Tier-1 ゲートウェイの接続には 3 分ほどかかり、完了すると、設定の状態は緑で [稼動中] と表示されます。

状態が [停止] になっている場合は、情報アイコンをクリックし、エラーを解決してから続行してください。

9 (オプション) ロード バランサを削除します。

- a 仮想サーバおよび Tier-1 ゲートウェイからロード バランサを接続解除します。
- b ロード バランサを選択します。
- c 垂直方向の省略記号ボタンをクリックします。
- d [削除] を選択します。

アクティブ モニターの追加

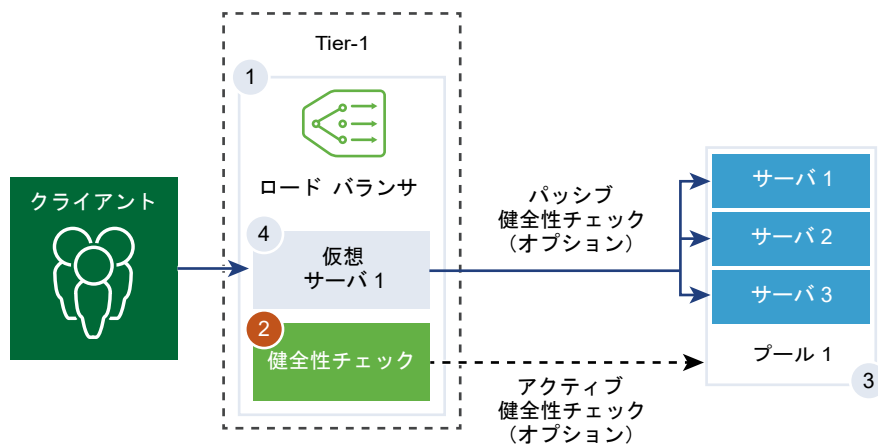
アクティブ健全性モニターは、サーバが使用可能かどうかをテストする際に使用します。アクティブ健全性モニターでは、基本的なサーバへの ping 送信や高度な HTTP の要求などのさまざまなタイプのテストを使用してアプリケーションの健全性を監視します。

注： [詳細とセキュリティ] タブでは、Tier-1 ゲートウェイを表すのに、Tier-1 論理ルーターという用語が使用されています。

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、この仮想サーバが Tier-1 ゲートウェイに接続された後に、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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [モニター] - [アクティブ] - [アクティブ モニターの追加] を選択します。

3 ドロップダウン メニューからサーバの プロトコルを選択します。

NSX Manager に事前定義されたプロトコル（HTTP、HTTPS、ICMP、TCP、および UDP）を使用することもできます。

4 [HTTP] プロトコルを選択します。

5 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
名前と説明	アクティブ健全性モニターの名前と説明を入力します。
モニタリング ポート	モニタリング ポートの値を設定します。
モニタリング間隔	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。
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。
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。
起動回数	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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

たとえば、モニタリング間隔が 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見なされます。

6 [設定] をクリックします。

7 HTTP 要求および応答の設定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 メニューからサーバの状態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 を受け入れることもできます。
HTTP 応答ヘッダー	[追加] をクリックして、HTTP 応答ヘッダーの名前および対応する値を入力します。 デフォルトのヘッダー値は 4,000 です。ヘッダーの最大値は 64,000 です。
HTTP 要求 Body	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。

オプション	説明
HTTP 応答コード	HTTP 応答本文の状態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 [HTTPS] プロトコルを選択します。
- 9 手順 5 を実行します。
- 10 [設定] をクリックします。
- 11 HTTP 要求/応答および SSL 設定の詳細を入力します。

オプション	説明
名前と説明	アクティブ健全性モニターの名前と説明を入力します。
HTTP メソッド	ドロップダウン メニューからサーバの状態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 を受け入れることもできます。
HTTP 応答ヘッダー	[追加] をクリックして、HTTP 応答ヘッダーの名前および対応する値を入力します。 デフォルトのヘッダー値は 4,000 です。ヘッダーの最大値は 64,000 です。
HTTP 要求 Body	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 応答本文の状態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。
サーバ SSL	ボタンを切り替えて、SSL サーバを有効にします。
クライアント証明書	(オプション) ドロップダウン メニューから、サーバが同じ IP アドレスの複数のホスト名に対応していない場合、またはクライアントが SNI 拡張機能をサポートしていない場合に使用される証明書を選択します。
サーバ SSL のプロファイル	(オプション) ドロップダウン メニューから、再利用可能であり、アプリケーションに依存しないクライアント側 SSL プロパティを定義するデフォルトの SSL プロファイルを割り当てます。 垂直方向の省略記号をクリックして、カスタム SSL プロファイルを作成します。
信頼されている CA (認証局) 証明書	(オプション) クライアントに認証用の CA 証明書を保持するよう要求することができます。
必須のサーバ認証	(オプション) ボタンを切り替えて、サーバ認証を有効にします。
証明書チェーンの階層の深さ	(オプション) クライアント証明書チェーンの認証の深さを設定します。
証明書失効リスト	(オプション) クライアント側の SSL プロファイルで、不正なクライアント証明書を拒否するための証明書失効リスト (CRL) を設定します。

12 [ICMP] プロトコルを選択します。

13 手順 5 を実行し、ICMP 健全性チェック パケットのデータ サイズをバイト単位で割り当てます。

14 [TCP] プロトコルを選択します。

15 手順 5 を実行します。TCP データのパラメータは空白のまま設定できます。

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、このデータは文字列である必要があります。正規表現はサポートされません。

16 [UDP] プロトコルを選択します。

17 手順 5 を実行して、UDP データを設定します。

必須オプション	説明
UDP 送信データ	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。
UDP 予測データ	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、サーバが稼動状態と見なされます。

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。[サーバ プールの追加](#) を参照してください。

パッシブ モニターの追加

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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [モニター] - [パッシブ] - [パッシブ モニターの追加] を選択します。
- 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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

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。

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。[サーバ プールの追加](#) を参照してください。

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。

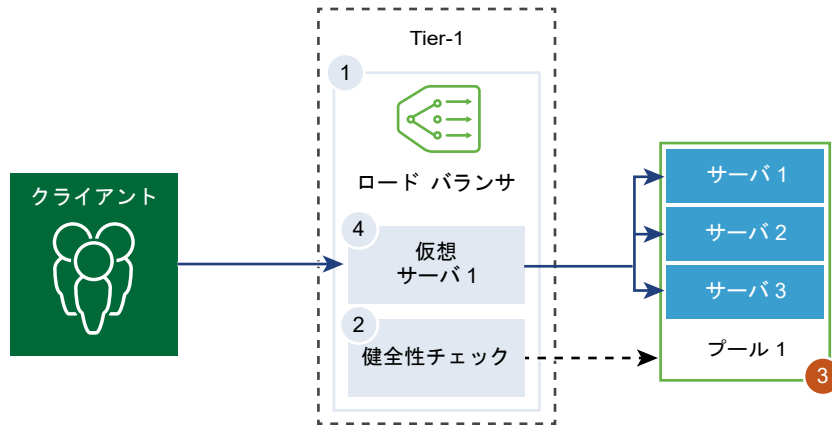
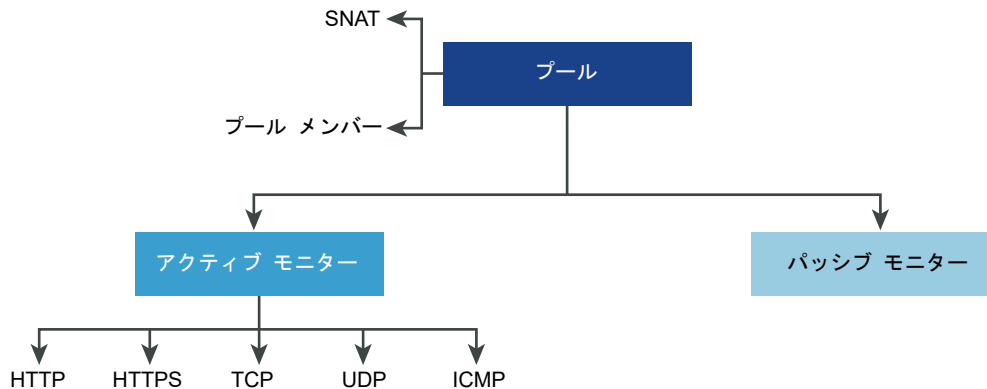


図 7-1. サーバ プール パラメータの設定



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。
- 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。[パッシブ モニターの追加](#) 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [サーバ プール] - [サーバ プールの追加] を選択します。
- 3 ロード バランサのサーバ 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数の上限に達した

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。
WEIGHTED_LEAST_CONNECTION	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、重み値を使用して、使用可能なサーバ リソース間で負荷を分散する処理に特化しています。 値が設定されず、スロー スタートが有効になっている場合、デフォルトで重み値は 1 となります。
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 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。

オプション	説明
個別メンバーの入力	<p>プール メンバー名、IP アドレス、およびポートを入力します。</p> <p>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。</p> <p>サーバ プールの管理状態を設定できます。サーバ プール メンバーの追加時に、このオプションはデフォルトで有効になっています。</p> <p>オプションが無効になっている場合は、アクティブな接続が処理され、新しい接続に対してサーバ プール メンバーは選択されていません。新しい接続は、プールの他のメンバーに割り当てられます。</p> <p>正常に無効に設定されると、メンテナンス用のサーバを削除できます。この状態のサーバ プール内のメンバーへの既存の接続が引き続き処理されます。</p> <p>アクティブ/スタンバイ状態を提供する健全性モニターと連携するバックアップ メンバーとしてプール メンバーを指定するには、ボタンで切り替えます。アクティブ メンバーの健全性チェックに失敗した場合は、バックアップ メンバーへのトラフィック フェイルオーバーが実行されます。バックアップ メンバーは、サーバの選択時にスキップされます。サーバ プールがアクティブでない場合、受信接続は、アプリケーションが使用できないことを示すソーリー ページとともに、設定されているバックアップ メンバーのみに送信されます。</p> <p>最大同時接続数の値は、サーバ プール メンバーがオーバーロードせず、サーバ選択時にスキップされないように割り当てられます。値が指定されていないと、接続は制限されません。</p>
グループの選択	<p>サーバ プール メンバーの事前設定済みのグループを選択します。</p> <p>グループ名を入力します。オプションで説明を入力できます。</p> <p>既存のリストからコンピュート メンバーを設定するか、新たにコンピュート メンバーを作成します。メンバーシップ基準を指定し、グループのメンバーを選択し、グループのメンバーとして IP アドレスと MAC アドレスを追加し、Active Directory グループを追加できます。ID メンバーとコンピュート メンバーとの組み合わせでグループのメンバーシップを定義します。</p> <p>タグを入力して検索しやすくします。タグを指定して、タグの範囲を設定できます。</p> <p>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。</p>

6 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な健全性チェック モニターを選択します。

ロード バランサは、定期的に ICMP Ping を送信し、データ トラフィックに依存することなく健全性をチェックしています。サーバ プールごとに 1 つだけのアクティブ健全性チェック モニターを設定できます。

7 送信元 NAT (SNAT) 変換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
自動マップ モード	<p>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。</p> <p>SNAT が必要です。</p> <p>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。</p> <p>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。</p>
無効	SNAT 変換モードを無効にします。
IP アドレス プール	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>

8 ボタンを切り替えて、TCP 最適化を有効にします。

TCP 最適化では、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。

9 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。

10 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。

11 ドロップダウン メニューで、サーバ プールに対してパッシブ健全性モニターを選択します。

12 タグを入力して検索しやすくします。

タグを指定して、タグの範囲を設定できます。

仮想サーバ コンポーネントの設定

レイヤー 4 およびレイヤー 7 仮想サーバを設定し、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 ルールなど、いくつかの仮想サーバ コンポーネントを設定できます。

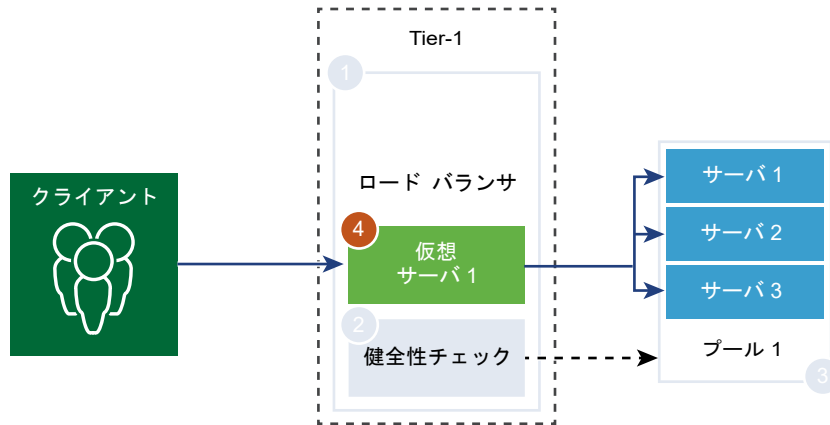
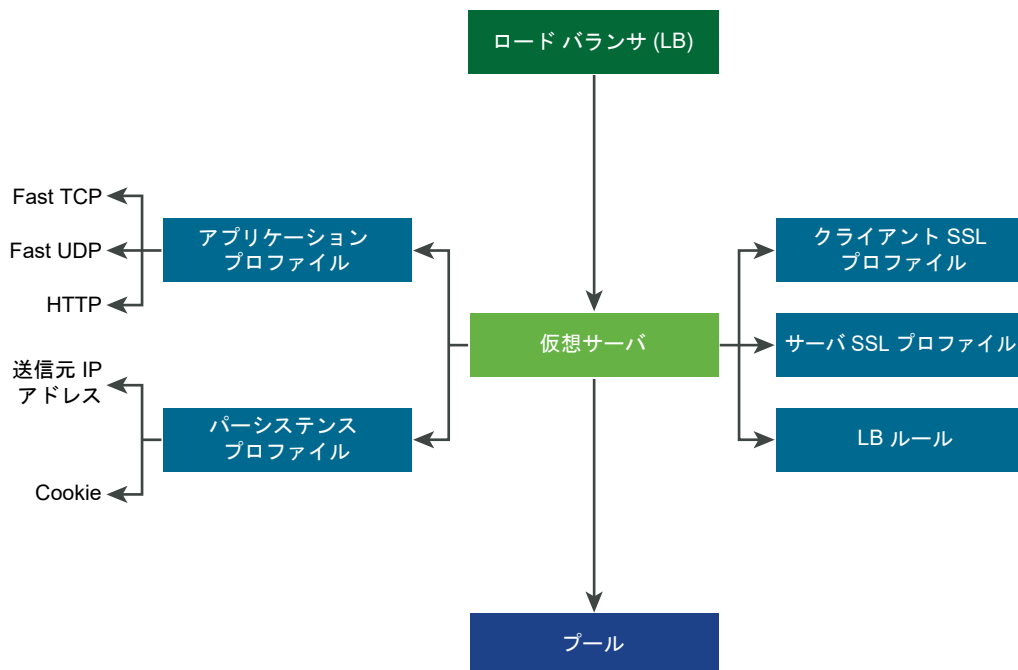


図 7-2. 仮想サーバ コンポーネント



アプリケーション プロファイルの追加

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。このプロファイルが使用されるのは、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必要があるときです。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 7-3. 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

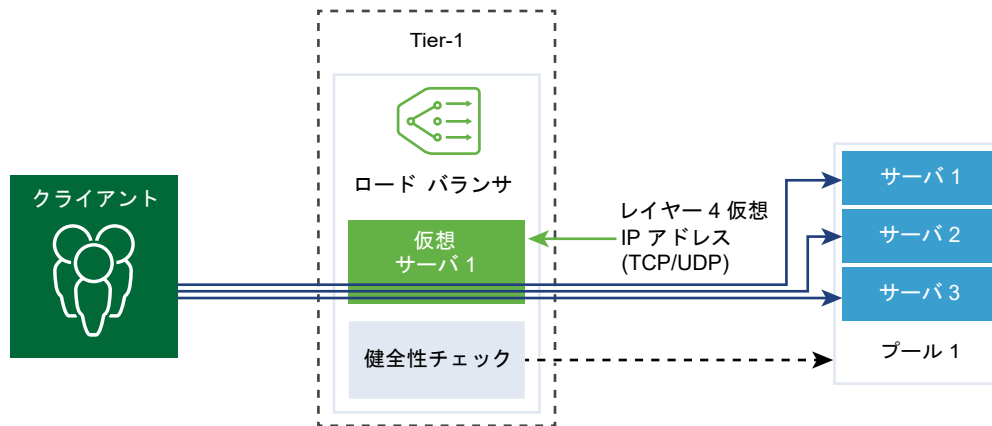
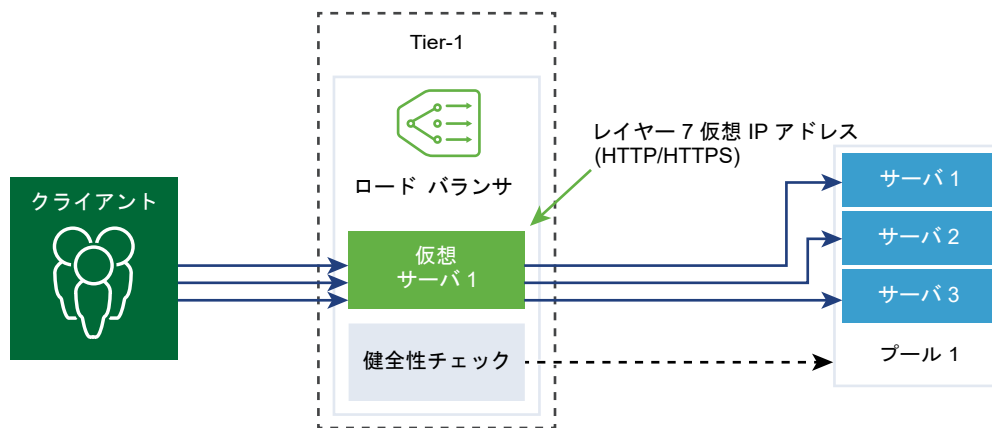


図 7-4. レイヤー 7 の HTTPS アプリケーション プロファイル



手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [プロファイル] - [アプリケーション] - [アプリケーション プロファイルの追加] を選択します。

3 [高速 TCP] アプリケーション プロファイルを選択して、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
名前と説明	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。
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。
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。
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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

4 [高速 UDP] アプリケーション プロファイルを選択して、プロファイルの詳細を入力します。

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。

オプション	説明
名前と説明	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。
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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

5 [HTTP] アプリケーション プロファイルを選択して、プロファイルの詳細を入力します。

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。

オプション	説明
名前と説明	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。
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。
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ [挿入] - 受信した要求に 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。受信された要求に XFF HTTP ヘッダーが存在する場合は、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 ヘッダーを追加します。 ■ [置き換え] - 受信した要求に 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ます。 <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>
要求本文のサイズ	HTTP 要求の本文を格納するために使用されるバッファの最大サイズを入力します。 サイズが指定されていない場合、要求の本文のサイズは無制限になります。
リダイレクト	<ul style="list-style-type: none"> ■ [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。 ■ [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。 <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"> ■ [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。 <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>

オプション	説明
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> <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>
タグ	<p>タグを入力して検索しやすくします。</p> <p>タグを指定して、タグの範囲を設定できます。</p>

パーシステンス プロファイルの追加

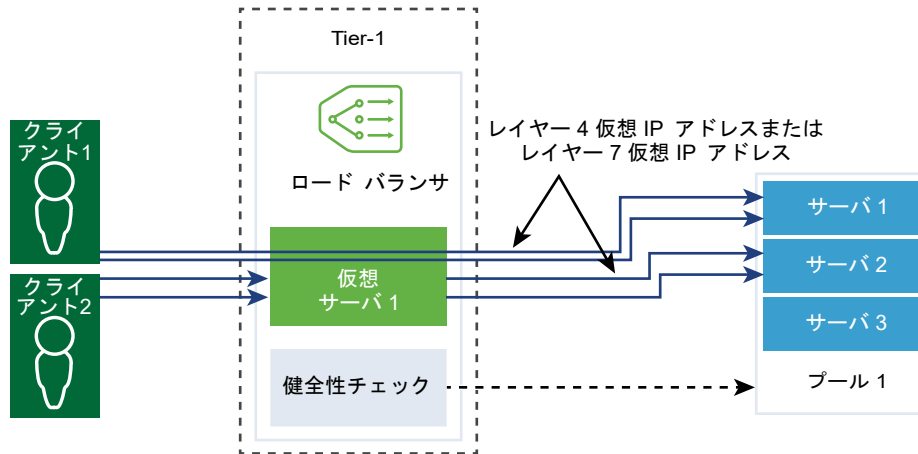
ステートフル アプリケーションの安定性を確保するため、ロード バランサには、関連するすべての接続を同じサーバに転送するパーシステンス機能が実装されています。アプリケーションによるさまざまな種類のニーズに対応できるように、さまざまな種類のパーシステンス機能がサポートされています。

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 のパーシステンス 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 のパーシステンス 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 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 パーシステンスを提供します。レイヤー 7 仮想サーバは、Cookie パーシステンス プロファイルのみを使用できます。Cookie 名に空白は使用[できません]。

汎用のパーシステンス プロファイルは、HTTP 要求の HTTP ヘッダー、Cookie または URL に基づいてパーシステンスをサポートします。このため、セッション ID が URL の一部である場合、アプリケーション セッションのパーシステンスがサポートされます。このプロファイルは、仮想サーバに直接関連付けられていません。要求の転送と応答の書き換えにロード バランサ ルールを設定するときに、このプロファイルを指定できます。



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 [ネットワーク] - [ロード バランシング] - [プロファイル] - [パーシステンス] - [パーシステンス プロファイルの追加] を選択します。
- 3 [送信元 IP] を選択して、送信元 IP のパーシステンス プロファイルを追加し、プロファイルの詳細を入力します。

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
名前と説明	送信元 IP のパーシステンス プロファイルの名前と説明を入力します。
パーシステンスの共有	<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 のパーシステンス 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> <p>新しいクライアント IP からの最初の接続は、ロード バランシング アルゴリズムに基づいてプール メンバーにロード バランシングされます。NSX は、このパーシステンス エントリを LB パーシステンス テーブルに保存します。このテーブルは、アクティブな T1-LB をホストしている Edge ノードで表示できます。表示するには、CLI コマンド <code>get load-balancer <LB-UUID> persistence-tables</code> を使用します。</p> <ul style="list-style-type: none"> ■ このクライアントから仮想 IP アドレスへの接続がある場合、パーシステンス エントリは保持されます。 ■ クライアントから仮想 IP アドレスへの接続がなくなると、「パーシステンス エントリのタイムアウト」値に従ってパーシステンス エントリのタイマーがカウントダウンを開始します。タイマーの期限切れになるまでにクライアントから仮想 IP アドレスへの新しい接続が確立されないと、そのクライアント IP アドレスのパーシステンス エントリは削除されます。エントリが削除されると、クライアントは再びロード バランシング アルゴリズムに基づいてプール メンバーにロード バランシングされます。

オプション	説明
テーブルがフルになるとエントリを消去	<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。このオプションを有効にした場合、新しいエントリを受け入れるために最も古いエントリが削除されます。</p> <p>このオプションを無効にした場合、送信元 IP のパーシステンス テーブルがいっぱいになると、新しいクライアント接続が拒否されます。</p>
HA パーシステンス ミラーリング	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。HA パーシステンス ミラーリングを有効にすると、ロード バランサのフェイルオーバーでクライアント IP のパーシステンスが維持されます。
タグ	<p>タグを入力して検索しやすくします。</p> <p>タグを指定して、タグの範囲を設定できます。</p>

4 [Cookie] パーシステンス プロファイルを選択して、プロファイルの詳細を入力します。

オプション	説明
名前と説明	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。
パーシステンスの共有	<p>このボタンを切り替えて、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します。</p> <p>Cookie パーシステンス プロファイルでは、<code><name>.<profile-id>.<pool-id></code> という形式を持つ Cookie が挿入されます。</p> <p>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、<code><name>.<virtual_server_id>.<pool_id></code> という形式を持つ Cookie が挿入されます。</p>
Cookie モード	<p>ドロップダウン メニューからモードを選択します。</p> <ul style="list-style-type: none"> ■ [挿入] - セッションを識別する一意の Cookie を追加します。 ■ [プリフィックス] - 既存の HTTP Cookie 情報に新しい情報を追加します。 ■ [書き換え] - 既存の HTTP Cookie 情報を書き換えます。
Cookie 名	Cookie 名を入力します。Cookie 名に空白は使用[できません]。
Cookie ドメイン	<p>ドメイン名を入力します。</p> <p>HTTP Cookie ドメインは、挿入モードの場合にのみ設定できます。</p>
Cookie のフォールバック	<p>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。</p> <p>Cookie で無効状態または停止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。</p>
Cookie のパス	<p>Cookie の URL パスを入力します。</p> <p>HTTP Cookie のパスは、挿入モードの場合にのみ設定できます。</p>
Cookie の暗号化	<p>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。</p> <p>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 サーバの IP アドレスとポート情報を暗号化します。</p>
Cookie のタイプ	<p>ドロップダウン メニューから Cookie のタイプを選択します。</p> <p>[セッション Cookie] - 保存されません。ブラウザを閉じると、失われます。</p> <p>[パーシステンス Cookie] - ブラウザによって保存されます。ブラウザを閉じてでも失われません。</p>

オプション	説明
最大アイドル時間	Cookie が期限切れになるまでのこの Cookie タイプの最大アイドル時間を秒単位で入力します。
Cookie の最大経過時間	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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

- 5 [汎用] を選択して、汎用パーシステンス プロファイルを追加し、プロファイルの詳細を入力します。

オプション	説明
名前と説明	送信元 IP のパーシステンス プロファイルの名前と説明を入力します。
パーシステンスの共有	ボタンを切り替えて、仮想サーバ間でプロファイルを共有します。
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> <p>新しいクライアント IP からの最初の接続は、ロード バランシング アルゴリズムに基づいてプール メンバーにロード バランシングされます。NSX は、このパーシステンス エントリを LB パーシステンス テーブルに保存します。このテーブルは、アクティブな T1-LB をホストしている Edge ノードで表示できます。表示するには、CLI コマンド <code>get load-balancer <LB-UUID> persistence-tables</code> を使用します。</p> <ul style="list-style-type: none"> このクライアントから仮想 IP アドレスへの接続がある場合、パーシステンス エントリは保持されます。 クライアントから仮想 IP アドレスへの接続がなくなると、「パーシステンス エントリのタイムアウト」値に従ってパーシステンス エントリのタイマーがカウントダウンを開始します。タイマーの期限切れになるまでにクライアントから仮想 IP アドレスへの新しい接続が確立されないと、そのクライアント IP アドレスのパーシステンス エントリは削除されます。エントリが削除されると、クライアントは再びロード バランシング アルゴリズムに基づいてプール メンバーにロード バランシングされます。
HA パーシステンス ミラーリング	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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

SSL プロファイルの追加

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 Data Center Limited Export Release 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 接続を停止するロード 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 7-5. SSL オフロード

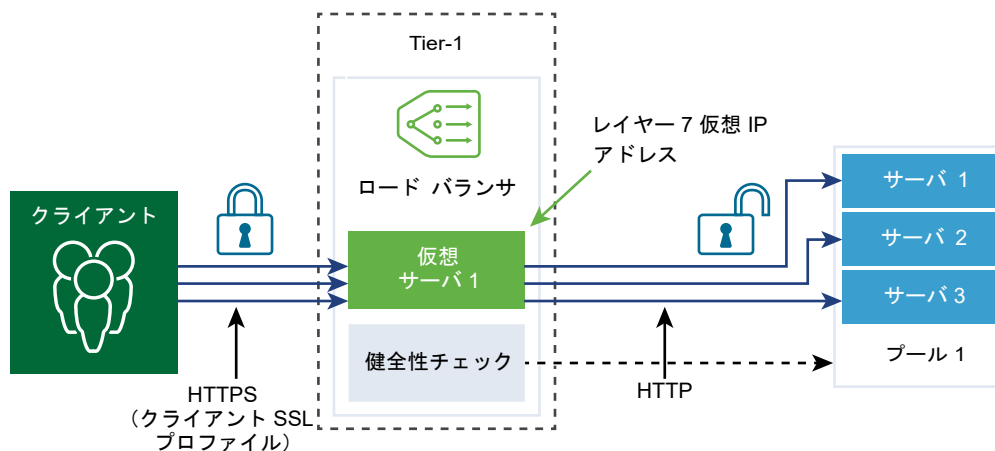
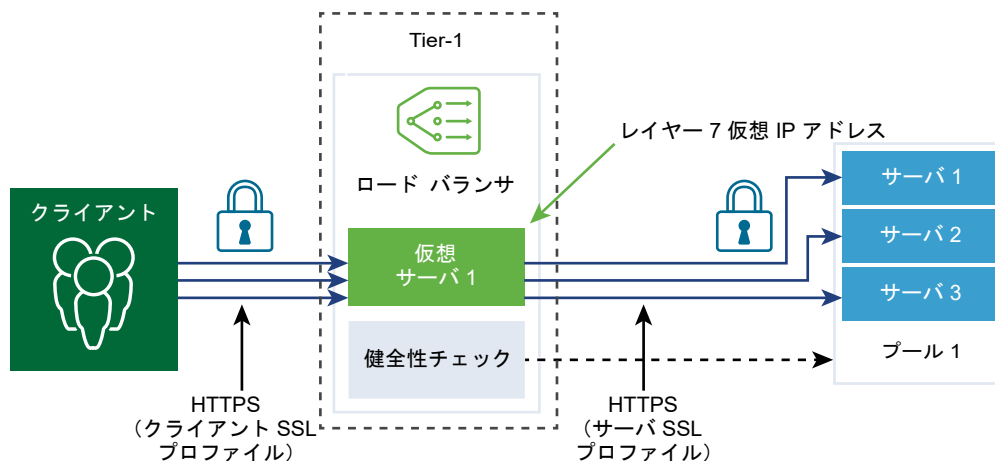


図 7-6. エンド ツー エンドの SSL



手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [プロファイル] - [SSL プロファイル] を選択します。

3 [クライアント SSL のプロファイル] を選択して、プロファイルの詳細を入力します。

オプション	説明
名前と説明	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。
SSL Suite	ドロップダウン メニューから SSL 暗号グループを選択します。クライアント SSL プロファイルに含まれる SSL 暗号および SSL プロトコルが入力されます。 デフォルトは、分散 SSL 暗号グループです。
セッションのキャッシュ	このボタンを切り替えると、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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。
サポートされている SSL 暗号	SSL スイートに応じて、ユーザーが割り当てたサポート対象の SSL 暗号がここに入力されます。[詳細を表示] をクリックして、リスト全体を表示します。 [カスタム] を選択した場合は、ドロップダウン メニューから [SSL 暗号] を選択する必要があります。
サポートされている SSL プロトコル	SSL スイートに応じて、ユーザーが割り当てたサポート対象の SSL プロトコルがここに入力されます。[詳細を表示] をクリックして、リスト全体を表示します。 [カスタム] を選択した場合は、ドロップダウン メニューから [SSL 暗号] を選択する必要があります。
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。

4 [サーバ SSL のプロファイル] を選択して、プロファイルの詳細を入力します。

オプション	説明
名前と説明	サーバ SSL プロファイルの名前と説明を入力します。
SSL Suite	ドロップダウン メニューから SSL 暗号グループを選択します。サーバ SSL プロファイルに含めることができる SSL 暗号および SSL プロトコルが入力されています。 デフォルトは、分散 SSL 暗号グループです。
セッションのキャッシュ	このボタンを切り替えると、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。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。
サポートされている SSL 暗号	SSL スイートに応じて、ユーザーが割り当てたサポート対象の SSL 暗号がここに入力されます。[詳細を表示] をクリックして、リスト全体を表示します。 [カスタム] を選択した場合は、ドロップダウン メニューから [SSL 暗号] を選択する必要があります。

オプション	説明
サポートされている SSL プロトコル	SSL スイートに応じて、ユーザーが割り当てたサポート対象の SSL プロトコルがここに入力されます。[詳細を表示] をクリックして、リスト全体を表示します。 [カスタム] を選択した場合は、ドロップダウン メニューから [SSL 暗号] を選択する必要があります。
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。

レイヤー 4 仮想サーバの追加

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。

仮想サーバの状態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 プロファイルの追加](#) 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 プロファイルの追加](#) 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 プロファイルの追加](#) 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。[サーバ プールの追加](#) を参照してください。
- ロード バランサが使用可能であることを確認します。[ロード バランサの追加](#) 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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [ロード バランシング] - [仮想サーバ] - [仮想サーバの追加] を選択します。
- 3 [L4 TCP] プロトコルを選択し、プロトコルの詳細を入力します。

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。

オプション	説明
名前と説明	レイヤー 4 仮想サーバの名前と説明を入力します。
IP アドレス	仮想サーバの IP アドレスを入力します。
ポート	仮想サーバのポート番号を入力します。
ロード バランサ	ドロップダウン メニューからこのレイヤー 4 仮想サーバに接続する既存のロード バランサを選択します。
サーバ プール	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。 縦型の楕円形をクリックすると、サーバ プールを作成できます。
アプリケーション プロファイル	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。 縦型の楕円形をクリックすると、アプリケーション プロファイルを作成できます。
パーシステンス	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。 仮想サーバでパーシステンス プロファイルを有効にすると、送信元 IP アドレスに関連するクライアント接続を同じサーバに送信できます。
最大同時接続	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。
最大新規接続レート	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。
ソーリー サーバ プール	ドロップダウン メニューから既存のソーリー サーバ プールを選択します。 ソーリー サーバ プールは、ロード バランサがデフォルト プールからの要求を処理するバックエンド サーバを選択できない場合に要求を処理します。 縦型の楕円形をクリックすると、サーバ プールを作成できます。
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。
管理状態	ボタンを切り替え、レイヤー 4 仮想サーバの管理状態を無効にします。
アクセス ログ	ボタンを切り替え、レイヤー 4 仮想サーバのログを有効にします。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

4 [L4 UDP] プロトコルを選択し、プロトコルの詳細を入力します。

オプション	説明
名前と説明	レイヤー 4 仮想サーバの名前と説明を入力します。
IP アドレス	仮想サーバの IP アドレスを入力します。

オプション	説明
ポート	仮想サーバのポート番号を入力します。
ロード バランサ	ドロップダウン メニューからこのレイヤー 4 仮想サーバに接続する既存のロード バランサを選択します。
サーバ プール	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。 縦型の楕円形をクリックすると、サーバ プールを作成できます。
アプリケーション プロファイル	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。 縦型の楕円形をクリックすると、アプリケーション プロファイルを作成できます。
パーシステンス	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。 仮想サーバでパーシステンス プロファイルを有効にすると、送信元 IP アドレスに関連するクライアント接続を同じサーバに送信できます。
最大同時接続	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。
最大新規接続レート	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。
ソーリー サーバ プール	ドロップダウン メニューから既存のソーリー サーバ プールを選択します。 ソーリー サーバ プールは、ロード バランサがデフォルト プールからの要求を処理するバックエンド サーバを選択できない場合に要求を処理します。 縦型の楕円形をクリックすると、サーバ プールを作成できます。
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。
管理状態	ボタンを切り替え、レイヤー 4 仮想サーバの管理状態を無効にします。
アクセス ログ	ボタンを切り替え、レイヤー 4 仮想サーバのログを有効にします。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

レイヤー 7 HTTP 仮想サーバの追加

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。

注： レイヤー 7 SSL パススルーは、NSX-T Data Center 3.0 以降でサポートされます。

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。

仮想サーバの状態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。

注： SSL プロファイルは NSX-T Data Center Limited Export Release ではサポートされていません。

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

- 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 プロファイルの追加](#) 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 プロファイルの追加](#) 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 プロファイルの追加](#) 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。[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。
- ロード バランサが使用可能であることを確認します。[ロード バランサの追加](#) 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>>) に管理者権限でログインします。

2 [ネットワーク] - [ロード バランシング] - [仮想サーバ] - [仮想サーバの追加] を選択します。

3 [L7 HTTP] プロトコルを選択し、プロトコルの詳細を入力します。

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。

オプション	説明
名前と説明	レイヤー 7 仮想サーバの名前と説明を入力します。
IP アドレス	仮想サーバの IP アドレスを入力します。
ポート	仮想サーバのポート番号を入力します。
ロード バランサ	ドロップダウン メニューからこのレイヤー 4 仮想サーバに接続する既存のロード バランサを選択します。
サーバ プール	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。 縦型の楕円形をクリックすると、サーバ プールを作成できます。
アプリケーション プロファイル	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。 縦型の楕円形をクリックすると、アプリケーション プロファイルを作成できます。
パーシステンス	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。 仮想サーバでパーシステンス プロファイルを有効にすると、送信元 IP アドレスおよび Cookie に関連するクライアント接続を同じサーバに送信できます。

4 [設定] をクリックし、レイヤー 7 仮想サーバ SSL を構成します。

クライアント SSL およびサーバ SSL を設定できます。

5 クライアント SSL を構成します。

オプション	説明
クライアント 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。
デフォルトの証明書	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。
クライアント SSL のプロファイル	ドロップダウン メニューからクライアント側 SSL プロファイルを選択します。
SNI 証明書	ドロップダウン メニューから利用可能な SNI 証明書を選択します。
信頼されている CA (認証局) 証明書	利用可能な CA 証明書を選択します。
必須のクライアント認証	ボタンを切り替えて、このメニュー項目を有効にします。
証明書チェーンの階層の深さ	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。
証明書失効リスト	利用可能な CRL を選択し、侵害されたサーバの証明書を禁止します。

6 サーバ SSL を構成します。

オプション	説明
サーバ SSL	ボタンを切り替えてプロファイルを有効にします。
クライアント証明書	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。
サーバ SSL のプロファイル	ドロップダウン メニューからサーバ側 SSL プロファイルを選択します。
信頼されている CA (認証局) 証明書	利用可能な CA 証明書を選択します。
必須のサーバ認証	ボタンを切り替えて、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、信頼する CA の 1 つによって署名されている必要があります。
証明書チェーンの階層の深さ	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。
証明書失効リスト	利用可能な CRL を選択し、侵害されたサーバの証明書を禁止します。 サーバ側では、OCSP および OCSP Stapling はサポートされていません。

7 追加のレイヤー 7 仮想サーバ プロパティを構成します。

オプション	説明
最大同時接続	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。
最大新規接続レート	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。
ソーリー サーバ プール	ドロップダウン メニューから既存のソーリー サーバ プールを選択します。 ソーリー サーバ プールは、ロード バランサがデフォルト プールからの要求を処理するバックエンド サーバを選択できない場合に要求を処理します。 縦型の楕円形をクリックすると、サーバ プールを作成できます。
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。
管理状態	ボタンを切り替え、レイヤー 7 仮想サーバの管理状態を無効にします。
アクセス ログ	ボタンを切り替え、レイヤー 7 仮想サーバのログを有効にします。
タグ	タグを入力して検索しやすくします。 タグを指定して、タグの範囲を設定できます。

8 [保存] をクリックします。

ロード バランサ ルールの追加

レイヤー 7 HTTP 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。

ロード バランサのルールは、一致のタイプとして正規表現をサポートします。高度な使用方法ではいくつかの制限があります。PCRE スタイルの正規表現パターンがサポートされています。一致条件に正規表現を使用する場合、名前付きキャプチャ グループがサポートされます。

正規表現には以下の制限事項があります。

- 文字を和集合および共通部分で表現することはサポートされません。たとえば、`[a-z[0-9]]` および `[a-z&&[aeiou]]` と表現せず、それぞれ `[a-z0-9]` および `[aeiou]` と表現します。
- 後方参照は 9 までサポートされ、`\1` ~ `\9` を使用して参照できます。
- 8 進数に一致させるには、`\ddd` 形式ではなく `\Odd` 形式を使用します。
- 最上位のレベルでは組み込みフラグはサポートされません。グループ内でのみサポートされます。たとえば、「`Case (?i:s)ensitive`」は使用せずに、「`Case ((?i:s)ensitive)`」を使用します。
- 前処理演算子 `\l`、`\u`、`\L`、`\U` はサポートされません。ここで、`\l` は次の文字を小文字にする演算子、`\u` は次の文字を大文字にする演算子、`\L` は `\E` までの文字を小文字にする演算子、`\U` は `\E` までの文字を大文字にする演算子です。
- `(?(condition)X)`、`(? {code})`、`(??{Code})` および `(?#comment)` はサポートされません。
- 事前定義済みの Unicode 文字クラス `\X` はサポートされません。
- Unicode 文字の名前付き構文を使用した参照はサポートされません。たとえば、`\N{name}` は使用せずに `\u2018` を使用します。

一致条件に正規表現を使用する場合、名前付きキャプチャ グループがサポートされます。たとえば、正規表現による一致パターン「`/news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+)/?(<article>.*))`」は、「`/news/2018-06-15/news1234.html`」のような URI との一致に使用されます。

ここで変数を以下のように設定します：`$year = "2018" $month = "06" $day = "15" $article = "news1234.html"`。設定後の変数は、ロード バランサ ルールのアクションで使用できます。たとえば、URI は一致する変数を使用して「`/news.py?year=$year&month=$month&day=$day&article=$article`」のように書き換えることができます。したがって URI は「`/news.py?year=2018&month=06&day=15&article=news1234.html`」と書き換えられます。

書き換えアクションにより、名前付きキャプチャ グループと組み込みの変数を組み合わせて使用できます。たとえば、URI は「`/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr`」と記述できます。したがって例の URI は「`/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1`」と書き換えられます。

注： 名前付きキャプチャ グループの名前は、「`_`」文字で開始できません。

名前付きキャプチャ グループのほか、書き換えアクションでは次の組み込みの変数も使用できます。組み込みの変数の名前はすべて「`_`」で始まります。

- `$ _args` : 要求からの引数

- `$_arg_<name>` : 要求行の `<name>` 引数
- `$_cookie_<name>` : `<name>` Cookie の値
- `$_upstream_cookie_<name>` : アップストリーム サーバによって送信された Cookie。Set-Cookie 応答ヘッダー フィールドに名前が指定されます。
- `$_upstream_http_<name>` : 任意の応答ヘッダー フィールドで、`<name>` は小文字に変換され、ダッシュをアンダースコアで置き換えたフィールド名
- `$_host` : 優先順位で、要求行からのホスト名、「Host」要求のヘッダーフィールドからのホスト名、または要求に一致するサーバ名
- `$_http_<name>` : 任意の要求のヘッダー フィールドで、`<name>` は小文字に変換され、ダッシュをアンダースコアで置き換えたフィールド名
- `$_https` : 接続が SSL モードで機能している場合は "on"、それ以外の場合は ""
- `$_is_args` : 要求行に引数がある場合は "?" それ以外の場合は ""
- `$_query_string` : `$_args` と同じ
- `$_remote_addr` : クライアント アドレス
- `$_remote_port` : クライアント ポート
- `$_request_uri` : 元の完全な要求 URI (引数を含む)
- `$_scheme` : 要求のスキーム、"http" または "https"
- `$_server_addr` : 要求を承認したサーバのアドレス
- `$_server_name` : 要求を承認したサーバの名前
- `$_server_port` : 要求を承認したサーバのポート
- `$_server_protocol` : 申請プロトコル、通常、"HTTP/1.0" または "HTTP/1.1"
- (NSX-T Data Center 2.5.0 のみ) `$_ssl_client_cert` : 確立された SSL 接続に対し、クライアント証明書を最初の行以外の各行で先頭にタブ文字を追加した PEM 形式で返します。
- (NSX-T Data Center 2.5.1 以降) `$_ssl_client_escaped_cert` : 確立された SSL 接続のクライアント証明書を PEM 形式で返します。
- `$_ssl_server_name` : SNI で要求されたサーバ名を返します
- `$_uri` : 要求内の URI パス
- `$_ssl_ciphers` : クライアントの SSL 暗号を返します
- `$_ssl_client_i_dn` : RFC 2253 に従って確立された SSL 接続のクライアント証明書の issuer DN 文字列を返します
- `$_ssl_client_s_dn` : RFC 2253 に従って確立された SSL 接続のクライアント証明書の subject DN 文字列を返します
- `$_ssl_protocol` : 確立された SSL 接続のプロトコルを返します
- `$_ssl_session_reused` : SSL セッションが再利用された場合は 「r」、それ以外の場合は 「.」 を返します

前提条件

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

手順

- 1 レイヤー 7 HTTP 仮想サーバを開きます。
- 2 [ロード バランサ ルール] セクションで、[設定] - [ルールの追加] の順にクリックし、HTTP 要求の書き換えフェーズのロード 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 要求の Cookie	任意の HTTP 要求 cookie と一致します。 http_request.cookie_value : 一致する値
HTTP 要求の本文	HTTP 要求の本文の内容に一致します。 http_request.body_value : 一致する値
クライアント SSL	クライアント SSL プロファイル ID と一致します。 ssl_profile_id : 一致する値
TCP ヘッダー ポート	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 ソース	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

サポートされている一致条件	説明
変数	変数を作成し、この変数に値を割り当てます。
大文字と小文字を区別	HTTP ヘッダー値を比較する場合、大文字と小文字が区別されるフラグを設定します。

操作	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
HTTP 要求ヘッダーの削除	HTTP ヘッダーを削除します。 http_request.header_delete : ヘッダー名 http_request.header_delete : 書き込む値

- 3 [要求の転送] - [ルールの追加] の順にクリックし、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 要求の Cookie	任意の HTTP 要求 cookie と一致します。 http_request.cookie_value : 一致する値
HTTP 要求の本文	HTTP 要求の本文の内容に一致します。 http_request.body_value : 一致する値
クライアント SSL	クライアント SSL プロファイル ID と一致します。 ssl_profile_id : 一致する値
TCP ヘッダー ポート	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 ソース	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

サポートされている一致条件	説明
変数	変数を作成し、この変数に値を割り当てます。
大文字と小文字を区別	HTTP ヘッダー値を比較する場合、大文字と小文字が区別されるフラグを設定します。
アクション	説明
HTTP 拒否	たとえば、状態を 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 状態コード http_forward.reply_message - HTTP 却下メッセージ
HTTP リダイレクト	要求をリダイレクトします。状態コードは、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 状態コード 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
変数パーシステンス検査	汎用パーシステンス プロファイルを選択し、変数名を入力します。 また、[ハッシュ変数] を有効にすることもできます。変数の値が非常に長い場合、変数のハッシュ値を使用することで、変数をパーシステンス テーブルに正しく格納できます。[ハッシュ変数] が有効になっていない場合、非常に長い変数値は、固定プリフィックス部分のみがパーシステンス テーブルに格納されます。その結果、プリフィックス部分が同じ変数値が複数存在すると、異なるバックエンド サーバにディスパッチするときに、長い変数値を含む 2 つの異なる要求が同じバックエンド サーバにディスパッチされる場合があります。
応答の状態	応答の状態を表示します。
応答メッセージ	サーバは、確認済みのアドレスと設定が含まれる応答メッセージを返します。

- 4 [応答の書き換え] - [ルールの追加] の順にクリックし、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
HTTP 応答メソッド	HTTP 応答メソッドに一致します。 http_response.method : 一致する値
HTTP 応答 URI	HTTP 応答 URI に一致します。 http_response.uri : 一致する値
HTTP 応答の URI 引数	HTTP 応答の URI 引数に一致します。 http_response.uri_args : 一致する値
HTTP 応答バージョン	HTTP 応答バージョンに一致します。 http_response.version : 一致する値
HTTP 応答 Cookie	任意の HTTP 応答 cookie に一致します。 http_response.cookie_value : 一致する値

サポートされている一致条件	説明
クライアント SSL	クライアント SSL プロファイル ID と一致します。 ssl_profile_id : 一致する値
TCP ヘッダー ポート	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 ソース	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
変数	変数を作成し、この変数に値を割り当てます。
大文字と小文字を区別	HTTP ヘッダー値を比較する場合、大文字と小文字が区別されるフラグを設定します。
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
HTTP 応答ヘッダーの削除	HTTP ヘッダーを削除します。 http_request.header_delete : ヘッダー名 http_request.header_delete : 書き込む値
変数パーシステンス学習	汎用パーシステンス プロファイルを選択し、変数名を入力します。 また、[ハッシュ変数] を有効にすることもできます。変数の値が非常に長い場合、変数のハッシュ値を使用することで、変数をパーシステンス テーブルに正しく格納できます。[ハッシュ変数] が有効になっていない場合、非常に長い変数値は、固定プリフィックス部分のみがパーシステンス テーブルに格納されます。その結果、プリフィックス部分が同じ変数値が複数存在すると、異なるバックエンド サーバにディスパッチするときに、長い変数値を含む 2 つの異なる要求が同じバックエンド サーバにディスパッチされる場合があります。

サーバ プールと仮想サーバに作成されたグループ

NSX Manager は、ロード バランサ サーバ プールと VIP ポートのグループを自動的に作成します。

ロード バランサが作成したグループは、[インベントリ] - [グループ] に表示されます。

サーバ プール グループは、NLB.PoolLB.Pool_Name LB_Name という名前で作成され、グループ メンバーの IP アドレスが割り当てられます。

- NO LB-SNAT (透過モード) で構成されたプール : 0.0.0.0/0
- NO LB-SNAT (自動マップ) で構成されたプール : T1-Uplink IP 100.64.x.y、T1-ServiceInterface IP
- NO LB-SNAT (IP プール) で構成されたプール : LB-SNAT IP-Pool

VIP グループは、NLB.VIP.virtual server name という名前で作成されます。VIP グループ メンバーの IP アドレスは VIP IP@ です。

サーバ プール グループの場合、ロード バランサ (NLB.PoolLB.Pool_Name LB_Name) からのトラフィックを許可する分散ファイアウォール ルールを作成できます。Tier-1 ゲートウェイ ファイアウォールの場合、LB VIP NLB.VIP.virtual server name からのトラフィックを許可するルールを作成できます。

転送ポリシー

8

この機能は、NSX Cloud に関連しています。

転送ポリシーまたはポリシー ベース ルーティング (PBR) ルールには、NSX-T が NSX 管理対象仮想マシンからのトラフィックを処理する方法を定義します。このトラフィックは、NSX-T オーバーレイに設定することも、クラウド プロバイダ（アンダーレイ）ネットワーク経由でルーティングすることもできます。

注： NSX-T Data Center を使用してパブリック クラウド ワークロード仮想マシンを管理する方法については、[22 章 NSX Cloud の使用](#)を参照してください。

トランジット VPC/VNet に PCG を展開するか、コンピュート VPC/VNet とトランジットをリンクすると、次の 3 つのデフォルト転送ポリシーが自動的に設定されます。

- 1 つの[ルートからアンダーレイへ]。トランジット/コンピュート VPC/VNet 内で解決されるすべてのトラフィックに使用されます。
- 別の[ルートからアンダーレイへ]。パブリック クラウドのメタデータ サービスに送信されるすべてのトラフィックに使用されます。
- 1 つの[ルートからオーバーレイへ]。それ以外のトラフィックに使用されます。たとえば、トランジット/コンピュート VPC/VNet の外部に送信されるトラフィック。このようなトラフィックは、NSX-T オーバーレイ トンネルを介して PCG にルーティングされ、宛先に転送されます。

注： [同じ PCG が管理する他の VPC/VNET へのトラフィック]：トラフィックは、送信元の NSX 管理対象 VPC/VNet から NSX-T オーバーレイ トンネルを経由して PCG にルーティングされ、さらに宛先の VPC/VNet に転送されます。

[別の PCG が管理する他の VPC/VNet へのトラフィック]：トラフィックは、NSX 管理対象 VPC/VNet の 1 つから NSX オーバーレイ トンネル経由で送信元の VPC/VNet の PCG にルーティングされ、宛先の NSX 管理対象 VPC/VNet の PCG に転送されます。

トラフィックがインターネットに送信される場合は、PCG がインターネット上の宛先にルーティングします。

アンダーレイへのルーティング中のマイクロセグメンテーション

トラフィックがアンダーレイ ネットワークにルーティングされるワークロード仮想マシンの場合でも、マイクロセグメンテーションが適用されます。

NSX 管理対象ワークロード仮想マシンから管理対象 VPC/VNet の外部にある宛先に直接接続している場合に、PCG をバイパスするには、この仮想マシンからアンダーレイ経由でトラフィックをルーティングするように転送ポリシーを設定します。

トラフィックがアンダーレイ ネットワークを経由してルーティングされると、PCG がバイパスされるため、トラフィックは North-South ファイアウォールを検出しません。ただし、これらのルールは PCG に到達する前に仮想マシン レベルで適用されるため、East-West または分散ファイアウォール (DFW) のルールは引き続き管理する必要があります。

サポートされている転送ポリシーと一般的な使用事例

ドロップダウン メニューに転送ポリシーのリストが表示されますが、このリリースでサポートされるのは次の転送ポリシーだけです。

- ルートからアンダーレイへ
- アンダーレイからルートへ
- ルートからオーバーレイへ

転送ポリシーが役立つ一般的なシナリオは次のとおりです。

- [ルートからアンダーレイへ]: NSX 管理対象仮想マシンからサービスまたはアンダーレイにアクセスします。たとえば、AWS アンダーレイ ネットワーク上の AWS S3 サービスにアクセスします。
- [オーバーレイからのルート]: アンダーレイ ネットワークから NSX 管理対象仮想マシンにホストされているサービスにアクセスします。たとえば、AWS ELB から NSX 管理対象仮想マシンにアクセスします。

この章には、次のトピックが含まれています。

- [転送ポリシーの追加または編集](#)

転送ポリシーの追加または編集

自動作成された転送ポリシーを編集したり、新しいポリシーを追加したりできます。

たとえば、AWS の S3 など、パブリック クラウドで提供されるサービスを使用するは、一連の IP アドレスがアンダーレイ経由でルーティングされ、このサービスにアクセスできるようにポリシーを手動で作成できます。

前提条件

ここに展開された PCG には、VPC または VNet が必要です。

手順

- 1 [セクションを追加] をクリックします。**AWS Services** など、適切な名前をセクションに付けます。
- 2 このセクションの横にあるチェック ボックスを選択し、[ルールを追加] をクリックします。**S3 Rules** などの名前をルールに付けます。

- 3 [ソース] タブで、AmazonVPC など、サービス アクセスを提供するワークロード仮想マシンが配置された VPC または VNet を選択します。またここでは、1 つ以上の条件に一致する複数の仮想マシンが含まれるように [グループ] を作成することもできます。
- 4 [宛先] タブでは、AWS で S3 サービスの IP アドレスが含まれている [グループ] など、サービスがホストされている VPC または VNet を選択します。
- 5 [サービス] タブで、ドロップダウン メニューからサービスを選択します。サービスがない場合は、サービスを追加することができます。また、[宛先] でルーティングの詳細を指定できるため、この選択肢を [任意] のままにすることもできます。
- 6 [アクション] タブで、AWS S3 サービスのこのポリシーを設定する場合は、[ルートからアンダーレイへ] を選択するなど、ルーティング方法を選択します。
- 7 [発行] をクリックし、転送ポリシーの設定を完了します。

IP アドレス管理 (IPAM)

9

IP アドレスを管理するには、DNS (Domain Name System)、DHCP (Dynamic Host Configuration Protocol)、IP アドレス プール、および IP アドレス ブロックを構成します。

注： IP アドレス ブロックは、NSX Container Plug-in (NCP) で使用されます。NCP の詳細については、『NSX Container Plug-in for Kubernetes and Cloud Foundry：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。

- DNS ゾーンの追加
- DNS フォワーダ サービスの追加
- DHCP サーバの追加
- Tier-0 または Tier-1 の DHCP リレー サーバの設定
- IP アドレス プールの追加
- IP アドレス ブロックの追加

DNS ゾーンの追加

DNS サービス用の DNS ゾーンを設定できます。DNS ゾーンとは、DNS 内のドメイン ネームスペース内の、他と区別できる範囲のことです。

DNS ゾーンを設定するときに、DNS クエリをアップストリーム DNS サーバに転送する際に使用する DNS フォワーダの送信元 IP を指定できます。送信元 IP を指定しないと、DNS クエリ パケットの送信元 IP が DNS フォワーダのリスナー IP になります。リスナー IP が、外部のアップストリーム DNS サーバからアクセスできない内部アドレスの場合は、送信元 IP を指定する必要があります。DNS 応答パケットがフォワーダに確実にルーティングされるようにするには、専用の送信元 IP が必要です。また、論理ルーターで SNAT を設定し、リスナー IP をパブリック IP に変換することもできます。この場合、送信元 IP を指定する必要はありません。

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 [ネットワーク] - [IP アドレス管理] - [DNS] の順に選択します。
- 3 [DNS ゾーン] タブをクリックします。

- 4 デフォルト ゾーンを追加するには、[DNS ゾーンの追加] - [デフォルト ゾーンを追加] の順に選択します。
 - a 名前を入力します。必要に応じて説明も入力します。
 - b 最大 3 つの DNS サーバの IP アドレスを入力します。
 - c (オプション) [送信元の IP アドレス] フィールドに IP アドレスを入力します。
- 5 FQDN ゾーンを追加するには、[DNS ゾーンの追加] - [FQDN ゾーンを追加] の順に選択します。
 - a 名前を入力します。必要に応じて説明も入力します。
 - b ドメインの FQDN を入力します。
 - c 最大 3 つの DNS サーバの IP アドレスを入力します。
 - d (オプション) [送信元の IP アドレス] フィールドに IP アドレスを入力します。
- 6 [保存] をクリックします。

DNS フォワーダ サービスの追加

DNS クエリを外部 DNS サーバに転送するように、DNS フォワーダを設定できます。

DNS フォワーダを設定する前に、デフォルトの DNS ゾーンを設定する必要があります。必要に応じて、1 つ以上の FQDN DNS ゾーンを設定できます。各 DNS ゾーンは、最大 3 台までの DNS サーバに関連付けることができます。FQDN DNS ゾーンを設定する場合は、1 つ以上のドメイン名を指定します。DNS フォワーダは、デフォルトの DNS ゾーンと、最大 5 つまでの FQDN DNS ゾーンに関連付けられます。DNS クエリを受信すると、DNS フォワーダはクエリ内のドメイン名を FQDN DNS ゾーンのドメイン名と比較します。一致が見つかったら、FQDN DNS ゾーンで指定された DNS サーバにクエリを転送します。一致が見つからない場合、デフォルトの DNS ゾーンで指定された DNS サーバにクエリを転送します。

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 [ネットワーク] - [IP アドレス管理] - [DNS] の順に選択します。
- 3 [DNS サービスの追加] をクリックします。
- 4 名前を入力します。必要に応じて説明も入力します。
- 5 Tier-0 または Tier-1 ゲートウェイを選択します。
- 6 DNS サービスの IP アドレスを入力します。

クライアントは、この IP アドレスに DNS クエリを送信します。これは DNS フォワーダのリスナー IP ともいいます。

- 7 デフォルトの DNS ゾーンを選択します。
- 8 ログ レベルを選択します。
- 9 最大 5 つの FQDN ゾーンを選択します。
- 10 [管理状態] 切り替えボタンをクリックして、DNS サービスを有効または無効にします。

- 11 [保存] をクリックします。

DHCP サーバの追加

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 サーバを作成して DHCP 要求を処理できます。

注： この手順で作成された DHCP サーバは、VLAN によってバックアップされるセグメントでサポートされません。VLAN でバックアップされた論理スイッチでサポートされる DHCP サーバを作成するには、[ネットワークとセキュリティの詳細設定] で DHCP 機能を使用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>>) に管理者権限でログインします。
- 2 [ネットワーク] - [IP アドレス管理] - [DHCP] の順に選択します。
- 3 [サーバを追加] をクリックします。
- 4 サーバタイプとして [DHCP サーバ] を選択します。
- 5 サーバの名前を入力します。
- 6 サーバの IP アドレスを CIDR 形式で入力します。

この手順では、2 つの論理ポートを作成します（論理インターフェイス用に 1 つ、DHCP サーバ用に 1 つ）。さらに、DHCP サーバを特定の DHCP 論理スイッチに接続します。このインターフェイスは、接続済みのインターフェイスとして Tier-0 または Tier-1 ゲートウェイに表示されます。そのため、DHCP サーバを割り当てる Tier-0 または Tier-1 ゲートウェイには、重複していないサブネットを選択してください。この目的では、<IP アドレス>/30 を指定できます。ここで使用するサブネット範囲は、接続された Tier-0 ゲートウェイにアドバタイズされませんが、Tier-1 ゲートウェイのフォワーディング テーブルに表示されます。

- 7 リース時間を入力します。
- 8 NSX Edge クラスタを選択します。
- 9 [保存] をクリックします。
- 10 DHCP サーバを Tier-0 または Tier-1 ゲートウェイに割り当てるには、次のようにします。
 - a [ネットワーク] - [Tier-0 ゲートウェイ] の順にクリックするか、[ネットワーク] - [Tier-1 ゲートウェイ] の順に移動します。
 - b 既存のゲートウェイを編集します。
 - c [IP アドレス管理] フィールドで、[IP アドレスを割り当てない] をクリックします。
 - d [タイプ] ドロップダウン リストから [DHCP ローカル サーバ] を選択します。
 - e DHCP サーバを選択します。
 - f [保存] をクリックします。
 - g [保存] をクリックします。

- 11 DHCP サーバをセグメントに割り当てるには、次のようにします。
 - a [ネットワーク] - [セグメント] の順に移動します。
 - b セグメントを追加または編集します。
セグメントは、Tier-0 または Tier-1 ゲートウェイに関連付けられている必要があります。
 - c 新しいセグメントを追加するには [サブネット] をクリックします。サブネットの追加または変更を行うには、[サブネット] の下にある数字をクリックします。
 - d 適切な DHCP の範囲を入力します。
 - e [適用] をクリックします。
 - f [保存] をクリックします。

Tier-0 または Tier-1 の DHCP リレー サーバの設定

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 リレー サーバを作成して、外部の DHCP サーバに DHCP トラフィックを中継できます。

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 [ネットワーク] - [IP アドレス管理] - [DHCP] の順に選択します。
- 3 [サーバを追加] をクリックします。
- 4 サーバタイプとして [DHCP リレー] を選択します。
- 5 リレー サーバの名前を入力します。
- 6 サーバの IP アドレスを 1 つ以上入力します。
- 7 [保存] をクリックします。
- 8 [ネットワーク] - [Tier-0 ゲートウェイ] の順に移動するか、[ネットワーク] - [Tier-1 ゲートウェイ] の順に移動して、ゲートウェイの DHCP リレー サーバを設定します。
- 9 適切なゲートウェイを編集します。
- 10 [IP アドレス管理] フィールドで、[IP を割り当てない] (Tier-0 ゲートウェイの場合) または [IP 割り当てを設定しない] (Tier-1 ゲートウェイの場合) をクリックします。
- 11 [タイプ] フィールドで、[DHCP リレー] を選択します。
- 12 [DHCP リレー] フィールドで、以前に作成した DHCP リレー サーバを選択します。
- 13 [保存] をクリックします。

- 14** リレーが機能するように、この DHCP リレー サービスを使用するゲートウェイに接続するセグメントごとに DHCP 範囲を指定する必要があります。

- a [ネットワーク] - [セグメント] の順に移動します。
- b セグメントを追加または編集します。
- c 新しいセグメントを追加するには、[サブネット] をクリックします。サブネットを変更するには、[サブネット] の下にある数字をクリックします。
- d 1 つ以上の DHCP 範囲を指定します。

これは、リレーを機能させるために必要です。

- e [適用] をクリックします。
- f [保存] をクリックします。

IP アドレス プールの追加

DHCP などのコンポーネントで使用する IP アドレス プールを設定できます。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワーク] - [IP アドレス管理] - [IP アドレス プール] の順に選択します。
- 3 [IP アドレス プールの追加] をクリックします。
- 4 名前を入力します。必要に応じて説明も入力します。
- 5 [サブネット] 列の [設定] をクリックして、サブネットを追加します。
- 6 アドレス ブロックを指定するには、[サブネットの追加] - [IP ブロック] の順に選択します。
 - a IP ブロックを選択します。
 - b サイズを指定します。
 - c [ゲートウェイを自動割り当て] をクリックして、ゲートウェイ IP の自動割り当てを有効または無効にします。
 - d [追加] をクリックします。
- 7 IP 範囲を指定するには、[サブネットの追加] - [IP 範囲] の順に選択します。
 - a IPv4 または IPv6 の IP 範囲を入力します。
 - b IP 範囲を CIDR 形式で入力します。
 - c [ゲートウェイ IP アドレス] にアドレスを入力します。
 - d [追加] をクリックします。
- 8 [保存] をクリックします。

IP アドレス ブロックの追加

他のコンポーネントで使用する IP アドレス ブロックを設定できます。

注： [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [IP アドレス管理] の順に移動し、IP アドレス ブロックを追加することもできます。

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 [ネットワーク] - [IP アドレス管理] - [IP アドレス プール] の順に選択します。
- 3 [IP アドレス ブロック] タブをクリックします。
- 4 [IP アドレス ブロックの追加] をクリックします。
- 5 名前を入力します。必要に応じて説明も入力します。
- 6 IP アドレス ブロックを CIDR 形式で入力します。
- 7 [保存] をクリックします。

このセクションのトピックでは、分散ファイアウォール ルール、ID ファイアウォール、ネットワーク イントロスペクション、ゲートウェイ ファイアウォール、エンドポイント保護ポリシーの North-South および East-West セキュリティについて説明します。

この章には、次のトピックが含まれています。

- セキュリティ設定の概要
- セキュリティに関する用語
- Identity Firewall
- レイヤー 7 コンテキスト プロファイル
- 分散ファイアウォール
- East-West ネットワーク セキュリティ：サードパーティ サービスのチェーン
- ゲートウェイ ファイアウォールの設定
- North-South ネットワーク セキュリティ：サードパーティ サービスの挿入
- エンドポイントの保護
- セキュリティ プロファイル

セキュリティ設定の概要

使用環境に事前に定義されたカテゴリで、East-West および North-South ファイアウォール ポリシーを設定します。

分散ファイアウォール (East-West) およびゲートウェイ ファイアウォール (North-South) は通常、カテゴリに分かれた複数の設定可能なルール セットを提供します。ファイアウォールを適用しない論理スイッチ、論理ポート、またはグループを含む除外リストを設定できます。

セキュリティ ポリシーは次のように適用されます。

- ルールは、左から右に、カテゴリ単位で処理されます。
- ルールは上から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。

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、詳細なポリシーが適用されるようになります。

セキュリティに関する用語

分散ファイアウォール全体で、次の用語が使用されます。

表 10-1. セキュリティ関連の用語

構造	定義
ポリシー	セキュリティ ポリシーには、ファイアウォール ルールやサービスの設定などのさまざまなセキュリティ要素が含まれています。ポリシーは、以前はファイアウォール セクションと呼ばれていました。
ルール	フローの評価に使用され、一致したときの対処方法を定義する一連のパラメータです。ルールには、送信元と宛先、サービス、コンテキスト プロファイル、ログ、タグなどのパラメータが含まれます。
グループ	<p>グループには静的および動的に追加されたさまざまなオブジェクトが含まれていて、ファイアウォール ルールの送信元および宛先フィールドとして使用できます。また、仮想マシン、IP セット、MAC セット、論理ポート、論理スイッチ、Active Directory ユーザー グループ、およびその他のネストされたグループの組み合わせを含むように設定できます。グループの動的な追加は、タグ、マシン名、OS 名、またはコンピュータ名に基づいて行うことができます。</p> <p>グループを作成するときに、グループが属するドメインを含める必要があります。デフォルトでは、これがデフォルト ドメインになります。</p> <p>グループは、以前は NSGroup またはセキュリティ グループと呼ばれていました。</p>
サービス	ポートとプロトコルの組み合わせを定義します。ポートとプロトコルに基づいてトラフィックを分類する場合に使用します。ファイアウォール ルールでは、事前定義されたサービスおよびユーザー定義のサービスを使用できます。
コンテキスト プロファイル	アプリケーション ID とドメイン名を含むコンテキスト対応属性を定義します。アプリケーションのバージョンや暗号設定などのサブ属性も含まれています。ファイアウォール ルールには、レイヤー 7 ファイアウォール ルールを有効にするためのコンテキスト プロファイルを含めることができます。

Identity Firewall

Identity Firewall (IDFW) 機能を使用すると、NSX 管理者は Active Directory ユーザーベースの分散ファイアウォール (DFW) ルールを作成できます。

IDFW は、仮想デスクトップ (VDI) またはリモート デスクトップ セッション (RDSH サポート) で使用できます。複数のユーザーによる同時ログインや、要件に基づくアプリケーションへのユーザー アクセスを可能にし、独立したユーザー環境を維持できます。VDI 管理システムは、VDI 仮想マシンへのアクセス権を付与するユーザーを制御します。NSX-T は、送信元の仮想マシン (VM) から宛先サーバへのアクセスを制御します。ここでは IDFW が有効になっています。RDSH を使用して、管理者は Active Directory (AD) 内のさまざまなユーザーを含むセキュリティ グループを作成し、そのユーザーのロールに基づいてアプリケーション サーバへのアクセスを許可または拒否します。たとえば、人事およびエンジニアリングは同じ RDSH サーバに接続し、このサーバから異なるアプリケーションにアクセスできます。

IDFW は、サポート対象のオペレーティング システムが実行されている仮想マシンでも使用できます。[Identity Firewall でサポートされる構成](#) を参照してください。

IDFW 構成のワークフローの概要は次のとおりです。ワークフローは、インフラストラクチャの準備から始まります。この段階では、NSX が Active Directory のユーザーおよびグループを利用できるようにするため、管理者が保護対象の各クラスタに必要なコンポーネントをインストールし、Active Directory の同期を設定します。次に、IDFW ルールを適用するため、Active Directory ユーザーがログインするデスクトップを IDFW が識別できるようにする必要があります。ネットワーク イベントがユーザーによって生成されると、仮想マシン上に VMware Tools でインストールされたシン エージェントは情報を収集して転送し、コンテキスト エンジンに送信します。この情報は、分散ファイアウォールに適用するために使用されます。

IDFW は、分散ファイアウォール ルールでのみ、送信元でユーザー ID を処理します。ID ベースのグループは、DFW ルールの宛先として使用できません。

注： IDFW は、ゲスト OS のセキュリティと整合性に依存します。悪意のあるローカル管理者がファイアウォール ルールを回避するために ID を偽装する方法は 1 つではありません。ユーザー ID 情報は、ゲスト仮想マシン内の NSX ゲスト イントロスペクション シン エージェントによって提供されます。セキュリティ管理者は、シン エージェントが各ゲスト仮想マシンにインストールされ、実行されていることを確認する必要があります。ログイン ユーザーには、エージェントの削除または停止を行う権限を付与してはなりません。

サポートされている IDFW 構成については、[Identity Firewall でサポートされる構成](#)を参照してください。

IDFW ワークフロー：

- 1 ユーザーは仮想マシンにログインし、Skype や Outlook を起動してネットワーク接続を開始します。
- 2 ユーザーのログイン イベントはシン エージェントによって検出され、接続情報と ID 情報が収集され、コンテキスト エンジンに送信されます。
- 3 コンテキスト エンジンでは、接続情報と ID 情報を該当するルール環境の分散ファイアウォールに転送します。

Identity Firewall のワークフロー

IDFW はユーザー ID に基づいてファイアウォールを許可することにより、従来のファイアウォールを強化します。たとえば、管理者は単一のファイアウォール ポリシーを使用して、カスタマー サポートのスタッフに人事データベースへのアクセスを許可または禁止することができます。

ID ベースのファイアウォール ルールは、Active Directory (AD) グループのメンバーシップによって決定されます。[Identity Firewall でサポートされる構成](#)を参照してください。

IDFW は、分散ファイアウォール ルールでのみ、送信元でユーザー ID を処理します。ID ベースのグループは、DFW ルールの宛先として使用できません。

注： Identity Firewall ルールを適用する場合、Active Directory を使用するすべての仮想マシンで Windows Time サービスを [有効] にする必要があります。これにより、Active Directory と仮想マシン間で日付と時刻が同期されるようになります。ユーザーの有効化や削除などの Active Directory グループ メンバーシップの変更は、ログインしているユーザーにすぐに反映されません。ユーザーに変更を反映させるには、ログオフして再度ログインする必要があります。グループ メンバーシップが変更されたときに、Active Directory 管理者がログアウトを強制的に実行することをおすすめします。これは、Active Directory の制限が原因で発生しています。

前提条件

仮想マシンで Windows 自動ログインが有効になっている場合は、[ローカル コンピューター ポリシー] - [コンピューターの構成] - [管理テンプレート] - [システム] - [ログオン] の順に移動して、[コンピューターの起動およびログオンで常にネットワークを待つ] を有効にします。

サポートされている IDFW 構成については、[Identity Firewall でサポートされる構成](#)を参照してください。

手順

- 1 NSX ファイル イントロスペクション ドライバと NSX ネットワーク イントロスペクション ドライバを有効にします。VMware Tools の完全インストールを行うと、これらがデフォルトで追加されます。
- 2 クラスタまたはスタンドアローン ホストで IDFW を有効にします ([Identity Firewall の有効化](#))。
- 3 Active Directory ドメインを構成します ([Active Directory の追加](#))。
- 4 Active Directory 同期操作を構成します ([Active Directory の同期](#))。
- 5 Active Directory グループ メンバーを含むセキュリティ グループ (SG) を作成します ([グループの追加](#))。
- 6 Active Directory グループ メンバーを含む SG を分散ファイアウォール ルールに割り当てます ([分散ファイアウォールの追加](#))。

Identity Firewall の有効化

Identity Firewall は、IDFW ファイアウォール ルールを適用するために有効にする必要があります。

手順

- 1 [セキュリティ] - [分散ファイアウォール] の順に選択します。
- 2 左上隅で、[アクション] - [全般設定] の順にクリックします。
- 3 状態ボタンを切り替えて IDFW を有効にします。

IDFW を機能させるには、分散ファイアウォールも有効にする必要があります。

- 4 スタンドアローン ホストまたはクラスタで IDFW を有効にするには、[Identity Firewall の設定] タブを選択します。
- 5 [有効] バーを切り替えて、スタンドアローン ホストを選択するか、IDFW ホストを有効にするクラスタを選択します。
- 6 [保存] をクリックします。

Identity Firewall のベスト プラクティス

次のベスト プラクティスに従うことで、Identity Firewall ルールを最大限に活用することができます。

- IDFW は次のプロトコルをサポートしています：
 - シングル ユーザー (VDI または非 RDSH サーバ) のユースケース サポート - TCP、UDP、ICMP
 - マルチユーザー (RDSH) の使用事例のサポート - TCP、UDP
 - 。

- 1つの ID ベースのグループは、分散ファイアウォール ルール内の送信元としてのみ使用できます。ソースで IP ベースと ID ベースのグループが必要な場合は、それぞれのグループにファイアウォール ルールを作成します。
- ドメイン名の変更など、ドメインの変更が発生すると、Active Directory との完全同期がトリガーされます。完全同期が完了するまでに時間がかかる場合があるため、オフピーク時または営業時間外に同期することをおすすめします。
- ローカルのドメイン コントローラの場合、デフォルトの LDAP ポート 389 と LDAPS ポート 636 は Active Directory の同期に使用されます。デフォルト値は変更できません。

Identity Firewall でサポートされる構成

仮想マシン (VM) の IDFW では、次の構成がサポートされています。物理デバイスの IDFW はサポートされていません。

ゲスト OS	適用タイプ
Windows 8	デスクトップ - デスクトップ ユーザーの使用事例をサポート
Windows 10	デスクトップ - デスクトップ ユーザーの使用事例をサポート
Windows 2012	サーバ - サーバ ユーザーの使用事例をサポート
Windows 2012R2	サーバ - サーバ ユーザーの使用事例をサポート
Windows 2016	サーバ - サーバ ユーザーの使用事例をサポート
Windows 2012R2	RDSH - リモート デスクトップ セッション ホストをサポート
Windows 2016	RDSH - リモート デスクトップ セッション ホストをサポート

Active Directory ドメイン コントローラ :

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

ホスト OS : ESXi

VMware Tools - バージョン 11

- VMCI ドライバ
- NSX ファイル イントロスペクション ドライバ
- NSX ネットワーク イントロスペクション ドライバ

レイヤー 7 コンテキスト プロファイル

レイヤー 7 アプリケーション ID は、コンテキスト プロファイルの一部として設定されます。

コンテキスト プロファイルでは、1つ以上の **属性** を指定できます。また、分散ファイアウォール (DFW) ルールやゲートウェイ ファイアウォール ルールで使用するサブ属性を指定することもできます。TLS バージョン 1.2 などのサブ属性が定義されている場合、複数のアプリケーション ID 属性はサポートされません。属性だけでなく、DFW は完全修飾ドメイン名 (FQDN) や URL をサポートしています。これらは、FQDN のホワイトリスト登録またはブラックリスト登録のコンテキスト プロファイルに指定できます。現在は、事前定義済みのドメインのリストがサポートされています。FQDN は、コンテキスト プロファイルの属性とともに設定することも、別のコンテキスト プロファイルで個別に設定することもできます。コンテキスト プロファイルを定義すると、1つまたは複数の分散ファイアウォール ルールに適用できます。

現在は、事前定義済みのドメインのリストがサポートされています。属性タイプ「ドメイン (FQDN) 名」の新しいコンテキスト プロファイルを追加する場合、FQDN のリストを表示できます。API 呼び出し `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` を実行して FQDN のリストを表示することもできます。

注：

- ゲートウェイ ファイアウォール ルールでは、コンテキスト プロファイルに FQDN 属性または他のサブ属性は使用できません。
 - コンテキスト プロファイルは、Tier-0 ゲートウェイ ファイアウォール ポリシーでサポートされていません。ゲートウェイ ファイアウォール ルールでは、FQDN 属性または他のサブ属性は使用できません。
-

コンテキスト プロファイルをルール内で使用すると、仮想マシンとの送受信トラフィックが、5-tuple に基づいてルール テーブルと照合されます。ルールがフローと一致し、レイヤー 7 コンテキスト プロファイルも含まれる場合、このパケットは、vDPI エンジンというユーザー空間コンポーネントにリダイレクトされます。それ以降の各フローでこの vDPI エンジンにパントされるパケットの数は少なくなり、アプリケーション ID と判断されると、この情報はカーネル内のコンテキスト テーブルに保存されます。フローの次のパケットを受信すると、コンテキスト テーブル内の情報はルール テーブルと再度比較され、5-tuple およびレイヤー 7 アプリケーション ID に基づいて照合されます。完全に一致したルールで定義されている適切なアクションが実行されます。許可ルールの場合、フローの後続のすべてのパケットはカーネルで処理され、接続テーブルと照合されます。完全に一致するドロップ ルールの場合、拒否パケットが生成されます。このフローが DPI にパントされた場合、ファイアウォールで生成されたログにはレイヤー 7 アプリケーション ID と該当する URL が含まれます。

受信パケットの処理ルール：

- 1 DFW またはゲートウェイ フィルタを入力すると、フロー テーブルで 5-tuple に基づいてパケットが検索されます。
- 2 フロー/状態が見つからない場合、5-tuple に基づいてルール テーブルにフローが照合され、フロー テーブルにエントリが作成されます。
- 3 フローがレイヤー 7 サービス オブジェクトのルールと一致すると、フロー テーブルの状態が「DPI 処理中」とマークされます。
- 4 トラフィックが DPI エンジンにパントされます。DPI エンジンにより、アプリケーション ID が決まります。
- 5 アプリケーション ID が決まると、DPI エンジンが属性を送信し、このフローのコンテキスト テーブルに挿入されます。「DPI 処理中」フラグが削除され、トラフィックが DPI エンジンにパントされなくなります。

- 6 アプリケーション ID 付きのフローがアプリケーション ID に一致するすべてのルールで再評価され、5-tuple ベースで一致した元のルールから開始され、最初に L4/L7 ルールに完全一致したフローが選択されます。適切なアクション（許可/拒否/却下）が実行され、フロー テーブルのエントリが更新されます。

レイヤー 7 ファイアウォール ルールのワークフロー

レイヤー 7 アプリケーション ID は、分散ファイアウォール ルールまたはゲートウェイ ファイアウォール ルールで使用されるコンテキスト プロファイルの作成に使用されます。属性に基づくルールを適用すると、ユーザーは任意のポートで実行するアプリケーションを許可/拒否できます。

NSX-T では、共通のインフラストラクチャおよびエンタープライズ アプリケーション用に組み込みの属性が提供されています。アプリケーション ID には、バージョン (SSL/TLS および CIFS/SMB) と暗号スイート (SSL/TLS) が含まれています。分散ファイアウォールの場合、アプリケーション ID は、コンテキスト プロファイル中のルールで使用され、FQDN のホワイト リスト登録やブラックリスト登録と組み合わせることができます。アプリケーション ID は、ESXi および KVM ホストでサポートされます。

注：

- ゲートウェイ ファイアウォール ルールでは、コンテキスト プロファイルに FQDN 属性または他のサブ属性は使用できません。
- コンテキスト プロファイルは、Tier-0 ゲートウェイ ファイアウォール ポリシーでサポートされていません。ゲートウェイ ファイアウォール ルールでは、FQDN 属性または他のサブ属性は使用できません。

サポートされているアプリケーション ID と FQDN:

- FQDN の場合、ユーザーは、指定された DNS サーバの DNS アプリケーション ID を使用して、ポート 53 に高優先度のルールを設定する必要があります。
- ALG アプリケーション ID (FTP、ORACLE、DCERPC、TFTP) では、ファイアウォール ルールに対応する ALG サービスが必要です。
- SYSLOG アプリケーション ID は標準ポートでのみ検出されます。

KVM がサポートするアプリケーション ID と FQDN :

- KVM では、サブ属性はサポートされません。
- KVM では、FTP と TFTP の ALG アプリケーション ID がサポートされます。

レイヤー 7 と ICMP の組み合わせ、または他のプロトコルを使用している場合は、レイヤー 7 ファイアウォール ルールを最後に設定する必要があります。レイヤー 7 any/any ルールより上のルールは実行されません。

手順

- 1 カスタム コンテキスト プロファイルを作成します。[コンテキスト プロファイルの追加](#)を参照してください。

- 2 分散ファイアウォール ルールまたはゲートウェイ ファイアウォール ルールでコンテキスト プロファイルを使用します。[分散ファイアウォールの追加](#) または [ゲートウェイ ファイアウォールのポリシーおよびルールの追加](#) を参照してください。

サービスが [任意] に設定されたファイアウォール ルールには、複数のアプリケーション ID コンテキスト プロファイルを使用できます。ALG プロファイル (FTP、ORACLE、DCERPC、TFTP) の場合、1 つのルールでサポートされるコンテキスト プロファイルは 1 つだけです。

属性

レイヤー 7 属性 (アプリケーション ID) は、使用するポートは問わず、特定のバケットまたはフローがどのアプリケーションで生成されたのかを識別するものです。

アプリケーション ID に基づいて適用することで、ユーザーは任意のポートを使用するアプリケーションの実行を許可または拒否することができます。さらに、標準ポートを使用してアプリケーションを強制的に実行することもできます。vDPI では、定義済みのパターンとバケット ペイロードを比較できます。このパターンは署名とも呼ばれています。署名ベースの識別および適用により、フローが所属する特定のアプリケーション/プロトコルに一致するだけでなく、TLS バージョン 1.0、TLS バージョン 1.2、または CIFS トラフィックの異なるバージョンなど、このプロトコルのバージョンにも一致できます。これにより、すべての展開済みアプリケーションおよびデータセンター内の E-W フローについて、既知の脆弱性を持つプロトコルを可視化し、その使用を制限できるようになります。

レイヤー 7 アプリケーション ID、は、分散ファイアウォール ルールとゲートウェイ ファイアウォール ルールのコンテキスト プロファイルで使用されます。この ID は ESXi と KVM ホストでサポートされます。

注： NFS バージョン 4 はサポートされる属性ではありません。

注：

- ゲートウェイ ファイアウォール ルールでは、コンテキスト プロファイルに FQDN 属性または他のサブ属性は使用できません。
 - コンテキスト プロファイルは、Tier-0 ゲートウェイ ファイアウォール ポリシーでサポートされていません。ゲートウェイ ファイアウォール ルールでは、FQDN 属性または他のサブ属性は使用できません。
-

サポートされているアプリケーション ID と FQDN:

- FQDN の場合、ユーザーは、指定された DNS サーバの DNS アプリケーション ID を使用して、ポート 53 に高優先度のルールを設定する必要があります。
- ALG アプリケーション ID (FTP、ORACLE、DCERPC、TFTP) では、ファイアウォール ルールに対応する ALG サービスが必要です。
- SYSLOG アプリケーション ID は標準ポートでのみ検出されます。

KVM がサポートするアプリケーション ID と FQDN :

- KVM では、サブ属性はサポートされません。
- KVM では、FTP と TFTP の ALG アプリケーション ID がサポートされます。

属性 (アプリケーション ID)	説明	タイプ
360ANTIV	360 Safeguard は、中国の IT 企業である Qihoo 360 が開発したプログラムです。	Web サービス
ACTIVDIR	Microsoft Active Directory	ネットワーク
AMQP	Advanced Message Queueing Protocol。アプリケーション間または組織間のビジネス メッセージ通信をサポートするアプリケーション層プロトコルです。	ネットワーク
AVAST	Avast.com の公式サイト (Avast! アンチウイルスのダウンロード) の閲覧で生成されるトラフィック	Web サービス
AVG	AVG アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
AVIRA	Avira アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
BLAST	データセンターでデータの圧縮、暗号化、エンコードを行い、VMware Horizon デスクトップの標準 IP ネットワーク間で転送するリモート アクセス プロトコルです。	リモート アクセス
BDEFENDER	BitDefender アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
CA_CERT	認証局 (CA) が、メッセージ暗号化のパブリック キーの所有者を証明するデジタル証明書を発行します。	ネットワーク
CIFS	CIFS (Common Internet File System) は、ネットワークのノード間のディレクトリ、ファイル、プリンタ、シリアル ポート、その他の通信に共有アクセスを提供するために使用します。	ファイル転送
CLDAP	Connectionless Lightweight Directory Access Protocol (CLDAP) は、UDP を使用してインターネット プロトコル (IP) ネットワーク上の分散型ディレクトリ情報サービスにアクセスし、これを保持するためのアプリケーション プロトコルです。	ネットワーク
CTRXCGP	Citrix Common Gateway Protocol は、UDP を使用してインターネット プロトコル (IP) ネットワーク上の分散型ディレクトリ情報サービスにアクセスし、これを保持するためのアプリケーション プロトコルです。	データベース
CTRKGOTO	Citrix GoToMeeting または GoToMeeting プラットフォーム ベースの類似セッションをホストします。通話、ビデオ、制限付きの混雑管理機能が含まれています。	コラボレーション
CTXICA	ICA (Independent Computing Architecture) は、Citrix Systems によって開発された、アプリケーション サーバ システムの専用プロトコルです。	リモート アクセス
DCERPC	分散コンピューティング環境/リモート プロシージャ コール。分散コンピューティング環境 (DCE) 用に開発されたリモート プロシージャ コール システムです。	ネットワーク
DIAMETER	コンピュータ ネットワークの認証/承認/課金プロトコル	ネットワーク
DHCP	Dynamic Host Configuration Protocol (DHCP) は、ネットワーク内の IP アドレスの割り当てを管理するプロトコルです。	ネットワーク
DNS	TCP または UDP 経由で DNS サーバにクエリを送信します。	ネットワーク

属性 (アプリケーション ID)	説明	タイプ
EPIC	Epic EMR は、患者の管理情報と医療情報を提供する電子医療記録アプリケーションです。	クライアント サーバ
ESET	Eset アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
FPROT	F-Prot アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
FTP	FTP (File Transfer Protocol) は、ファイル サーバとローカル マシン間のファイル転送に使用されます。	ファイル転送
GITHUB	Web ベースの Git またはバージョン管理リポジトリとインターネット ホスティング サービス	コラボレーション
HTTP	HyperText Transfer Protocol。World Wide Web の基本的な転送プロトコルです。	Web サービス
HTTP2	HTTP 2.0 プロトコル対応の Web サイトを参照したときに生成されるトラフィック	Web サービス
IMAP	IMAP (Internet Message Access Protocol) は、リモート サーバ上の Eメールにアクセスするためのインターネット標準プロトコルです。	メール
KASPRSKY	Kaspersky アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
KERBEROS	Kerberos は、秘密鍵暗号を使用してクライアント/サーバ アプリケーションに堅牢な認証機能を提供するネットワーク認証プロトコルです。	ネットワーク
LDAP	LDAP (Lightweight Directory Access Protocol) は、IP ネットワーク経由でディレクトリの読み取りと編集を行うためのプロトコルです。	データベース
MAXDB	MaxDB SQL サーバに対する SQL 接続とクエリ	データベース
MCAFEE	McAfee アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデート	ファイル転送
MSSQL	Microsoft SQL Server は、リレーショナル データベースです。	データベース
NFS	クライアント コンピュータのユーザーが、ローカル ストレージにアクセスする場合と同様にネットワーク上のファイルにアクセスできます。 注： NFS バージョン 4 はサポートされる属性ではありません。	ファイル転送
NNTP	ニュース サーバ間で Usenet ニュース記事 (netnews) を転送したり、エンドユーザーのクライアント アプリケーションから記事を閲覧したり投稿したりするためのインターネット アプリケーション プロトコルです。	ファイル転送
NTBIOSNS	NetBIOS ネーム サービス。アプリケーションは、セッションを開始したり、データグラムを配布するため、ネーム サービスを使用して NetBIOS 名を登録する必要があります。	ネットワーク
NTP	NTP (Network Time Protocol) は、ネットワーク経由でコンピュータ システムの時刻を同期するために使用されます。	ネットワーク
OCSP	ユーザーのプライベート キーの侵害や失効を確認する OCSP レスポンド。	ネットワーク
ORACLE	Oracle Corporation のオブジェクト/リレーショナル データベース管理システム (ORDBMS)	データベース

属性 (アプリケーション ID)	説明	タイプ
PANDA	Panda アンチウイルス/セキュリティ ソフトウェアのダウンロードとアップデ ート	ファイル転送
PCOIP	データセンターでデータの圧縮、暗号化、エンコードを行い、標準の IP ネット ワーク間で転送するリモート アクセス プロトコルです。	リモート アクセス
POP2	POP (Post Office Protocol) は、ローカルのメール クライアントがリモート サーバからメールを取得するためのプロトコルです。	メール
POP3	Microsoft 社が実装する NetBIOS ネーム サービス (NBNS)、ネーム サー バ、サービスです。	メール
RADIUS	コンピュータがネットワーク サービスに接続して使用できるように、認証/承 認/課金 (AAA) を統合管理します。	ネットワーク
RDP	RDP (Remote Desktop Protocol) は、別のコンピュータのグラフィカル インターフェイスへのアクセスを可能にします。	リモート アクセス
RTCP	RTCP (Real-Time Transport Control Protocol) は、RTP (Real-time Transport Protocol) と一緒に使用するプロトコルです。RTCP は、RTP フ ローにアウトオブバンドの制御情報を提供します。	メディア ストリーミング
RTP	RTP (Real-Time Transport Protocol) は主にリアルタイム オーディオ/ビ デオの配信に使用されます。	メディア ストリーミング
RTSP	RTSP (Real Time Streaming Protocol) は、エンドポイント間のメディア セッションの確立と制御に使用されます。	メディア ストリーミング
SIP	SIP (Session Initiation Protocol) は、音声通話/ビデオ通話の設定と制御を 行う一般的な制御プロトコルです。	メディア ストリーミング
SMTP	SMTP (Simple Mail Transfer Protocol) は、インターネット プロトコル (IP) ネットワーク間で E メール転送を行うインターネット標準規格です。	メール
SNMP	SNMP (Simple Network Management Protocol) は、IP ネットワーク 上のデバイスを管理するインターネット標準プロトコルです。	ネットワーク監視
SSH	SSH (Secure Shell) は、ネットワークに接続している 2 台のデバイス間でセ キュア チャネルを使用してデータの交換を行うためのネットワーク プロトコ ルです。	リモート アクセス
SSL	SSL (Secure Sockets Layer) は、インターネット経由で保護された通信を可 能にする暗号プロトコルです。	Web サービス
SYMUPDAT	Symantec LiveUpdate のトラフィック。スパイウェアの定義、ファイアウ オール ルール、アンチウイルス シグネチャ ファイル、ソフトウェア アップデ ートなどが転送されます。	ファイル転送
SYSLOG	SYSLOG は、ネットワーク デバイスがイベント メッセージをログ サーバに送 信できるようにするプロトコルです。	ネットワーク監視
TELNET	インターネットまたはローカル エリア ネットワークで、仮想ターミナル接続に より、双方向にインタラクティブなテキスト指向の通信機能を提供するためのネ ットワーク プロトコル。	リモート アクセス
TFTP	TFTP (Trivial File Transfer Protocol) は、WinAgents TFTP クライアン トなどのクライアントを使用して、SolarWinds TFTP サーバなどの TFTP サーバにファイルのリスト、ダウンロード、アップロードを行うために使用され ます。	ファイル転送

属性 (アプリケーション ID)	説明	タイプ
VNC	仮想ネットワーク コンピューティングのトラフィック。	リモート アクセス
WINS	Microsoft 社が実装する NetBIOS ネーム サービス (NBNS)、ネーム サーバ、サービスです。	ネットワーク

分散ファイアウォール

分散ファイアウォールでは、ファイアウォール ルールにカテゴリが事前に定義されています。ルールは、上から下、左から右に評価されます。

表 10-2. 分散ファイアウォール ルールのカテゴリ

カテゴリ	説明
イーサネット	レイヤー 2 ベースのルールで使われます
緊急	ルールの検疫と許可で使われます
インフラストラクチャ	共有サービスへのアクセスを定義します。グローバル ルール：Active Directory、DNS、NTP、DHCP、バックアップ、管理サーバ
環境	ゾーン間のルール：本番と開発、ビジネス部門間のルール
アプリケーション	アプリケーション、アプリケーション層、またはマイクロ サービス間のルール

ファイアウォール ドラフト

ドラフトは、ポリシー セクションとルールが設定された分散ファイアウォールの完全な構成です。ドラフトはすぐに発行することも、後で発行するために保存することもできます。保存は自動または手動で行うことができます。

手動ドラフトのファイアウォール構成を保存するには、分散ファイアウォール画面の右上に移動し、[アクション] - [保存] の順にクリックします。保存後、[アクション] - [表示] の順に選択すると、構成を表示できます。デフォルトでは、自動ドラフトが有効になっています。自動ドラフトを無効にするには、[アクション] - [全般設定] の順に移動します。自動ドラフトが有効になっているときに、ファイアウォールの構成を変更すると、システムによって自動ドラフトが生成されます。最大で、100 個の自動ドラフトと 10 個の手動ドラフトを保存できます。自動ドラフトを編集して手動ドラフトとして保存できます。このドラフトはすぐに発行することも、後で発行することもできます。同じドラフトを複数のユーザーが開いて編集しないように、手動ドラフトをロックできます。ドラフトを発行すると、現在の構成がドラフトの構成に置き換わります。

ファイアウォール ドラフトの保存と表示

ドラフトは、後で発行するために保存されているか、すでに発行されている分散ファイアウォールの設定です。ドラフトは自動的に作成されます。また、手動で作成することもできます。

手動ドラフトは、編集して保存できます。自動ドラフトの場合は、そのクローンを作成し、手動ドラフトとして保存すると編集が可能になります。最大で、100 個の自動ドラフトと 10 個の手動ドラフトを保存できます。

手順

- 1 [セキュリティ] - [分散ファイアウォール] をクリックします。

- 2 ファイアウォールの設定を手動で保存するには、[アクション] - [保存] の順に移動します。

手動ドラフトは、保存、編集、保存が可能です。保存した後、元の設定に戻すことができます。

- 3 [名前] に構成名を入力します。

- 4 複数のユーザーが手動ドラフトを同時に開いて編集できないようにするには、[ロック] を選択して設定をロックし、コメントを追加します。

- 5 [保存] をクリックします。

- 6 保存済みの構成を表示するには、[アクション] - [ビュー] の順にクリックします。

タイムラインを開き、保存済みのすべての設定を表示します。ドラフトの名前、日付、時刻、保存者などの詳細を表示するには、ドラフトのドット アイコンまたはスター アイコンをポイントします。保存済みの構成は時間でフィルタリングされます。1 日、1 週間、30 日間または過去 3 か月のすべてのドラフトが表示されます。これにより、自動ドラフトでフィルタリングし、保存することができます。また、右上の検索ツールを使用して、名前でフィルタリングすることもできます。

- 7 ドラフトの上にカーソルを置くと、保存した設定の名前、日付、時刻の詳細が表示されます。名前をクリックして詳細を表示します。

ドラフトの詳細ビューには、このドラフトと同期するために、現在のファイアウォールの設定に必要な変更が表示されます。このドラフトが発行されている場合、このビューに表示されるすべての変更が現在の設定に適用されます。

下向き矢印をクリックすると、各セクションが展開され、セクションに追加、変更または削除された変更が表示されます。追加されたルールの場合、ボックスの左側に緑色のバーが表示されます。変更された要素（名前の変更など）には黄色のバーが、削除された要素には赤色のバーが表示されます。

- 8 選択したドラフトの名前または説明を編集するには、[ドラフトの詳細を表示] 画面からメニュー アイコン（3 つのドット）をクリックし、[編集] を選択します。

手動のドラフトはロックできます。ロックする場合は、ドラフトのコメントを指定する必要があります。

エンタープライズ管理者などの一部のロールにはフル アクセスの認証情報があるため、ロックアウトできません。[ロールベースのアクセス コントロール](#) を参照してください。

- 9 [クローン作成] をクリックすると、自動ドラフトと手動ドラフトのクローンを作成して保存できます。

[保存済みの構成] 画面で、デフォルトの名前をそのまま使用することも、編集することもできます。設定をロックすることもできます。ロックする場合は、ドラフトのコメントを指定する必要があります。

- 10 ドラフトの設定のクローン バージョンを保存するには、[保存] をクリックします。これで、[保存済みの構成] セクションにドラフトが表示されます。

次のステップ

表示されたドラフトを読み込み、発行できます。その後、このドラフトがアクティブなファイアウォール構成になります。

ファイアウォール ドラフトの発行と取り消し

自動ドラフトと手動ドラフトの両方を読み込んで発行し、アクティブな構成にすることができます。

発行時に、新しい自動ドラフトが作成されます。この自動ドラフトは、以前の構成に戻すために発行できます。

手順

- 1 保存済みの構成を表示するには、[アクション] - [ビュー] の順にクリックします。

タイムラインを開き、保存済みのすべての設定を表示します。ドラフトの名前、日付、時刻、保存者などの詳細を表示するには、ドラフトのドット アイコンをポイントします。保存済みの構成は時間でフィルタリングされます。1 日、1 週間、30 日間または過去 3 か月に作成されたすべてのドラフトが表示されます。

- 2 ドラフト名をクリックすると、[ドラフトの詳細を表示] ウィンドウが表示されます。

- 3 [ロード] をクリックします。新しいファイアウォール構成がメイン ウィンドウに表示されます。

注： ファイアウォール フィルタが使用されている場合、または現在の構成に保存されていない変更がある場合は、ドラフトをロードできません。

- 4 ドラフト構成を確定して有効にするには、[発行] をクリックします。以前に発行した構成に戻すには、[元に戻す] をクリックします。

発行後、ドラフトの変更がアクティブな構成に表示されます。

- 5 発行前にドラフトの内容を編集するには、[ロード] をクリックした後に構成を編集します。

- 6 ドラフト構成の編集済みバージョンを保存するには、[アクション] - [保存] の順にクリックします。

手動ドラフトは、新しい構成または既存の構成の更新として保存できます。自動ドラフトは、新しい構成として保存されます。

- 7 [名前] に名前を入力します。必要であれば、[説明] に説明を入力します。[ロック] を選択して、ドラフトをロックすることもできます。ロックする場合は、ドラフトのコメントを指定する必要があります。

- 8 [保存] をクリックします。

- 9 ドラフト構成を確定して有効にするには、[発行] をクリックして、以前に発行した構成に戻すには、[元に戻す] をクリックします。

分散ファイアウォールの追加

分散ファイアウォール (DFW) は、仮想マシンですべての East-West トラフィックを監視します。

前提条件

DFW で保護するゲスト仮想マシンの vNIC は、トランスポート ゾーンに関連付けられた N-VDS 論理スイッチに接続されている必要があります。

Identity Firewall ルールを作成する場合はまず、Active Directory のメンバーを持つグループを作成します。IDFW でサポートされるのは、TCP ベースのファイアウォール ルールのみです。

注： Identity Firewall ルールを適用する場合、Active Directory を使用するすべての仮想マシンで Windows Time サービスを [有効] にする必要があります。これにより、Active Directory と仮想マシン間で日付と時刻が同期されるようになります。ユーザーの有効化や削除などの Active Directory グループ メンバーシップの変更は、ログインしているユーザーにすぐに反映されません。ユーザーに変更を反映させるには、ログオフして再度ログインする必要があります。グループ メンバーシップが変更されたときに、Active Directory 管理者がログアウトを強制的に実行することをおすすめします。これは、Active Directory の制限が原因で発生しています。

レイヤー 7 と ICMP の組み合わせ、または他のプロトコルを使用している場合は、レイヤー 7 ファイアウォール ルールを最後に設定する必要があります。レイヤー 7 any/any ルールより上のルールは実行されません。

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 [セキュリティ] - [分散ファイアウォール] の順に選択します。
- 3 [アクション] - [全般設定] の順に選択し、分散ファイアウォールの状態を切り替え、分散ファイアウォールを有効にします。[保存] をクリックします。
- 4 正しい事前定義済みカテゴリであることを確認し、[ポリシーの追加] をクリックします。カテゴリの詳細については、[分散ファイアウォール](#) を参照してください。
- 5 [名前] に、新しいポリシー セクションを入力します。

6 (オプション) 次のポリシーを構成するには、歯車アイコンをクリックします。

オプション	説明
TCP Strict	<p>3 ウェイ ハンドシェイク (SYN、SYN ACK、ACK) で TCP 接続が開始し、通常、2 方向の交換 (FIN、ACK) で接続が終了します。特定の状況では、分散ファイアウォール (DFW) に特定のフローの 3 ウェイ ハンドシェイクが検証されない場合があります (トラフィックが非対称であったり、フローの存在中に分散ファイアウォールが有効になっている場合など)。デフォルトでは、分散ファイアウォールは 3 ウェイ ハンドシェイクを検証する必要がないため、すでに確立されているセッションをピックアップします。TCP Strict をセッションごとに有効にして、中間セッションのピックアップをオフにし、3 ウェイ ハンドシェイクの要件を適用できます。</p> <p>特定の DFW ポリシーで TCP Strict モードを有効にし、デフォルトの ANY-ANY Block ルールを使用すると、3 ウェイ ハンドシェイクの接続要件を満たしていないパケットと、このセクションの TCP ベースのルールに一致するパケットはドロップします。Strict はステートフル TCP ルールにのみ適用され、分散ファイアウォールポリシー レベルで有効になります。TCP Strict は、TCP サービスが指定されていないデフォルトの ANY-ANY Allow と一致するパケットには適用されません。</p>
ステートフル	<p>ステートフル ファイアウォールは、アクティブな接続の状態を監視し、この情報を使用してファイアウォールの通過を許可するパケットを決定します。</p>
ロック済み	<p>複数のユーザーが同じセクションを編集できないように、ポリシーをロックできます。セクションをロックする場合は、コメントを含める必要があります。</p> <p>エンタープライズ管理者などの一部のロールにはフル アクセスの認証情報があるため、ロックアウトできません。ロールベースのアクセス コントロール を参照してください。</p>

7 [発行] をクリックします。複数のポリシーを追加し、まとめて一度に発行できます。

新しいポリシーは画面に表示されます。

8 ポリシーのセクションを選択し、[ルールの追加] をクリックします。

9 ルールの名前を入力します。

10 [送信元] 列で、編集アイコンをクリックし、ルールのソースを選択します。Active Directory のメンバーを持つグループは、IDFW ルールの送信元フィールドに使用できます。詳細については[グループの追加](#)を参照してください。

IPv4、IPv6、マルチキャスト アドレスがサポートされています。

注：IPv6 ファイアウォールでは、接続されたセグメントで IPv6 に対して IP 検出を有効にする必要があります。詳細については、[IP アドレス検出セグメント プロファイルの理解](#)を参照してください。

11 [宛先] 列で、編集アイコンをクリックし、ルールの宛先を選択します。定義しない場合、宛先は [すべて] に一致します。詳細については[グループの追加](#)を参照してください。IPv4、IPv6、マルチキャスト アドレスがサポートされています。

- 12 [サービス] 列で編集アイコンをクリックし、サービスを選択します。サービスを定義しない場合は、[すべて] と一致します。

- 13 イーサネット カテゴリにルールを追加する場合、[プロファイル] 列は使用できません。他のルール カテゴリの場合は、[プロファイル] 列で編集アイコンをクリックしてコンテキスト プロファイルを選択するか、[新しいコンテキスト プロファイルの追加] をクリックします。 [コンテキスト プロファイルの追加](#) を参照してください。

コンテキスト プロファイルは、分散ファイアウォール ルールとゲートウェイ ファイアウォール ルールでレイヤー 7 アプリケーション ID 属性を使用します。サービスが [任意] に設定されたファイアウォール ルールには、複数のアプリケーション ID コンテキスト プロファイルを使用できます。ALG プロファイル (FTP と TFTP) の場合、1 つのルールでサポートされるコンテキスト プロファイルは 1 つだけです。

- 14 [適用] をクリックして、ルールにコンテキスト プロファイルを適用します。

- 15 デフォルトで、[適用先] の列は分散ファイアウォールに設定されており、ルールはすべてのワークロードに適用されます。また、選択したグループにルールまたはポリシーを適用することもできます。[適用先] はルールあたりの適用スコープを定義します。また、ESXi および KVM ホストの最適化またはリソースに主に使用されます。特定のゾーンとテナントのターゲットとなるポリシーを定義するのに役立ち、その他のテナントとゾーンに定義されている他のポリシーに干渉することはありません。

IP アドレス、MAC アドレス、または Active Directory グループのみで構成されるグループは、[適用先] テキスト ボックスで使用できません。

- 16 [アクション] 列で、アクションを選択します。

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。

- 17 状態の切り替えボタンをクリックし、ルールを有効または無効にします。

- 18 (オプション) 歯車アイコンをクリックし、次のルールのオプションを構成します。

オプション	説明
ログの記録	ログの記録はデフォルトで無効になっています。ログは ESXi および KVM ホストの /var/log/dfwlogs.log ファイルに保存されます。
方向	このフィールドは、ゲートウェイのアップリンク インタフェースまたはサービス インタフェースから見たトラフィックの方向を示します。受信はアップリンク インタフェースまたはサービス インタフェースから入ってくるトラフィックのみ、送信はアップリンク インタフェースまたはサービス インタフェースから出ていくトラフィックのみ、受信/送信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	IPv4、IPv6、または IPv4 と IPv6 の両方に基づくルールを適用します。
ログ ラベル	ログを有効にすると、ログ ラベルがファイアウォール ログに記録されます。

- 19 [発行] をクリックします。複数のルールを追加し、まとめて一度に発行できます。

- 20 各ルールで、[情報] アイコンをクリックして、ルール ID 番号とその適用場所を表示します。

ルールを発行するまで、このアイコンはグレー表示になります。フィルタ アイコンをクリックしたときに、フィルタ条件を満たすポリシーとルールのみが表示されるように、ルール ID を指定することもできます。

- 21 セキュリティ ポリシー レベルで認識の状態 API が強化され、認識の状態の追加情報が提供されます。これを実現するには、*intent_path* と一緒にクエリ パラメータ *include_enforced_status=true* を指定します。次の API 呼び出しを実行します。

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/
infra/domains/default/security-policies/<security-policy-
id>&include_enforced_status=true
```

分散ファイアウォール パケット ログ

ファイアウォール ルールのログが有効な場合は、ファイアウォール パケット ログを確認して問題のトラブルシューティングを行うことができます。

ESXi ホストと KVM ホストのログ ファイルはどちらも /var/log/dfwlogs.log です。

以下に、分散ファイアウォール ルールの通常ログのサンプルを示します。

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainrs/1024 IN 52 TCP 192.168.4.3/49627->192.168.4.4/49153 SEW

2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainrs/1024 OUT 52 TCP 192.168.4.3/49676->192.168.4.4/135 SEW

2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1

2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP
fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:0:1:2/547
```

DFW ログ ファイルには次の要素が含まれます。各要素はスペースで区切られます。

- タイムスタンプ：

- インターフェイスの VIF ID の最後の 8 桁
- INET タイプ (v4 または v6)
- 理由 (match)
- アクション (PASS、DROP、REJECT)
- ルール セット名/ルール ID
- パケットの方向 (IN/OUT)
- パケット サイズ
- プロトコル (TCP、UDP、または PROTO #)
- netx ルール ヒットの SVM 方向
- 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
- TCP フラグ (SEW)

渡された TCP パケットの場合、セッション終了時に終了ログが記録されます。

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

TCP 終了ログには次の要素が含まれます。各要素はスペースで区切られます。

- タイムスタンプ :
- インターフェイスの VIF ID の最後の 8 桁
- INET タイプ (v4 または v6)
- アクション (TERM)
- ルールセット名/ルール ID
- パケットの方向 (IN/OUT)
- プロトコル (TCP、UDP、または PROTO #)
- TCP RST フラグ
- netx ルール ヒットの SVM 方向
- 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
- 受信パケット数/送信パケット数 (すべて累計)
- 受信パケット サイズ/送信パケット サイズ

以下に、分散ファイアウォール ルールの FQDN ログ ファイルのサンプルを示します。

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

FQDN ログには次の要素が含まれます。各要素はスペースで区切られます。

- タイムスタンプ :

- インターフェイスの VIF ID の最後の 8 桁
- INET タイプ (v4 または v6)
- 理由 (match)
- アクション (PASS、DROP、REJECT)
- ルールセット名/ルール ID
- パケットの方向 (IN/OUT)
- パケット サイズ
- プロトコル (TCP、UDP、または PROTO #)
- 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
- ドメイン名/UUID。UUID はドメイン名のバイナリ内部表現です。

以下に、分散ファイアウォール ルールのレイヤー 7 ログ ファイルのサンプルを示します。

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

レイヤー 7 ログには次の要素が含まれます。各要素はスペースで区切られます。

- タイムスタンプ :
- インターフェイスの VIF ID の最後の 8 桁
- INET タイプ (v4 または v6)
- 理由 (match)
- アクション (PASS、DROP、REJECT)
- ルールセット名/ルール ID
- パケットの方向 (IN/OUT)
- パケット サイズ
- プロトコル (TCP、UDP、または PROTO #)
- 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
- APP_XXX は、検出されたアプリケーションです。

デフォルトの接続方法の選択

セキュリティ モデルを適用するデフォルトの接続方法を選択できます。

デフォルトの接続方法では、個々のルールを修正する代わりに、作成した他のファイアウォール ルールよりも上位に、すべて許可（ブラックリスト）またはすべて拒否（ホワイトリスト）のいずれかのファイアウォール ポリシーを作成します。デフォルトの接続方法を設定するには、[分散ファイアウォール] に移動します。ページの上部にある接続状態をクリックして、別のオプションを選択します。

デフォルトで選択されている接続方法を変更し、すぐに有効にするには、ファイアウォール ポリシーとルールがすでに作成されている必要があります。ポリシーやルールが作成されていない場合、ポリシーとルールが作成されるまでデフォルトの接続方法が維持されます。

次のオプションを設定できます。

- [ブラックリスト（ログありまたはなし）]: これはデフォルトのオプションで、DFW にすべて許可ルールを作成します。
- [ホワイトリスト（ログ付きまたはログなし）]: すべてのトラフィックを拒否するファイアウォール ルールを作成します。ファイアウォール ルールで定義されたサイトまたはアプリケーションからの通信のみが許可され、他のすべての通信は拒否されます。DHCP トラフィックも対象になります。
- [なし]: このオプションを選択すると、ファイアウォール ルールのブラックリスト登録とホワイトリスト登録の両方が無効になります。これは、以前のバージョンの NSX-T Data Center を使用してすでに設定されているルール セットがある場合に便利です。

ファイアウォール除外リストの管理

ファイアウォール除外リストは、グループ メンバーシップに基づいてファイアウォール ルールから除外するグループから構成されます。

グループはファイアウォール ルールから除外できます。また、最大で 100 個のグループがリストに表示されます。IP セット、MAC セット、Active Directory グループは、ファイアウォール除外リストにあるグループのメンバーとして追加できません。

注: NSX-T Data Center は、NSX Manager と NSX Edge ノードの仮想マシンを自動的にファイアウォール除外リストに追加します。

手順

- 1 [セキュリティ] - [分散ファイアウォール] - [アクション] - [除外リスト] の順に移動します。
ウィンドウが表示され、使用可能なグループが表示されます。
- 2 グループを除外リストに追加するには、グループの横にあるチェックボックスをクリックします。[適用] をクリックします。
- 3 グループを作成するには、[グループの追加] をクリックします。[グループの追加](#) を参照してください。
- 4 グループを編集するには、グループの横にある 3 つのドット メニューをクリックして、[編集] を選択します。
- 5 グループを編集するには、3 つのドット メニューをクリックして、[削除] を選択します。
- 6 グループの詳細を表示するには、[すべてを表示] を をクリックします。

特定のドメインのフィルタリング (FQDN/URL)

分散ファイアウォール ルールを設定し、*.office365.com など、FQDN/URL で識別される特定のドメインをフィルタリングします。

現在は、事前定義済みのドメインのリストがサポートされています。属性タイプ「ドメイン (FQDN) 名」の新しいコンテキスト プロファイルを追加する場合、FQDN のリストを表示できます。API 呼び出し `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` を実行して FQDN のリストを表示することもできます。

最初に DNS ルールを設定し、その下に FQDN の許可リスト ルールまたは拒否リスト ルールを設定する必要があります。NSX-T Data Center は、DNS 応答 (DNS サーバから仮想マシンに送信) の TTL 時間を使用して、仮想マシン (VM) の DNS から IP アドレスへのマッピング キャッシュ エントリを保持します。DNS セキュリティ プロファイルを使用して DNS の TTL をオーバーライドするには、[DNS セキュリティの構成](#)を参照してください。FQDN フィルタリングを有効にするには、仮想マシンでドメイン解決に (静的 DNS エントリではなく) DNS サーバを使用する必要があります。また、DNS 応答で受信した TTL も考慮する必要があります。NSX-T Data Center は、DNS スヌーピングを使用して IP アドレスと FQDN のマッピングを取得します。DNS スプーフィング攻撃から保護するため、すべての論理ポートのスイッチ全体で SpoofGuard を有効にする必要があります。DNS スプーフィング攻撃では、悪意のある仮想マシンが偽の DNS 応答を挿入し、トラフィックを悪意のあるエンドポイントにリダイレクトしたり、ファイアウォールをバイパスしたりします。SpoofGuard の詳細については、[SpoofGuard セグメント プロファイルの理解](#)を参照してください。

この機能はレイヤー 7 で動作しますが、ICMP は対象外です。example.com のすべてのサービスに対して拒否リスト ルールを作成した場合、ping example.com から応答があり、curl example.com からの応答がなければ、この機能は意図したとおり機能しています。

サブドメインが含まれるため、ワイルドカード FQDN を選択するのがベスト プラクティスです。たとえば、*example.com を選択すると、americas.example.com や emea.example.com などのサブドメインも含まれます。example.com の場合、サブドメインは含まれません。

ESXi ホストの vMotion では、FQDN ベースのルールが保持されます。

注： ESXi および KVM ホストがサポートされています。KVM ホストは、FQDN 許可リストのみをサポートします。FQDN フィルタリングは、TCP および UDP トラフィックでのみ使用できます。

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 [セキュリティ] - [分散ファイアウォール] の順に移動します。
- 3 [分散ファイアウォールの追加](#) の手順を実行し、ファイアウォール ポリシー セクションを追加します。既存のファイアウォール ポリシー セクションも使用できます。
- 4 新規または既存のファイアウォール ポリシー セクションを選択し、[ルールの追加] をクリックして最初に DNS ファイアウォール ルールを作成します。

- 5 **DNS rule** など、ファイアウォール ルールの名前を入力し、次の詳細を入力します。

オプション	説明
サービス	編集アイコンをクリックし、環境に応じて適宜 DNS または DNS-UDP サービスを選択します。
プロファイル	編集アイコンをクリックし、DNS コンテキスト プロファイルを選択します。これは事前に作成されており、展開内でデフォルトで使用可能です。
適用先	必要に応じて、グループを選択します。
アクション	[許可] を選択します。

- 6 [ルールの追加] を再度クリックして、FQDN を許可リストまたは拒否リストに登録するルールを設定します。
- 7 **FQDN/URL Allowlist** など、ルールに適切な名前を付けます。このポリシー セクションの DNS のルールの下にルールをドラッグします。
- 8 次のように詳細を指定します。

オプション	説明
サービス	編集アイコンをクリックし、HTTP など、このルールと関連付けるサービスを選択します。
プロファイル	編集アイコンをクリックし、[新しいコンテキスト プロファイルの追加] をクリックします。 [属性] という列をクリックし、[ドメイン (FQDN) 名] を選択します。事前定義済みリストから属性の名前/値のリストを選択します。[追加] をクリックします。詳細については、 コンテキスト プロファイルの追加 を参照してください。
適用先	必要に応じて、分散ファイアウォールまたはグループを選択します。
アクション	[許可]、[ドロップ] または [拒否] を選択します。

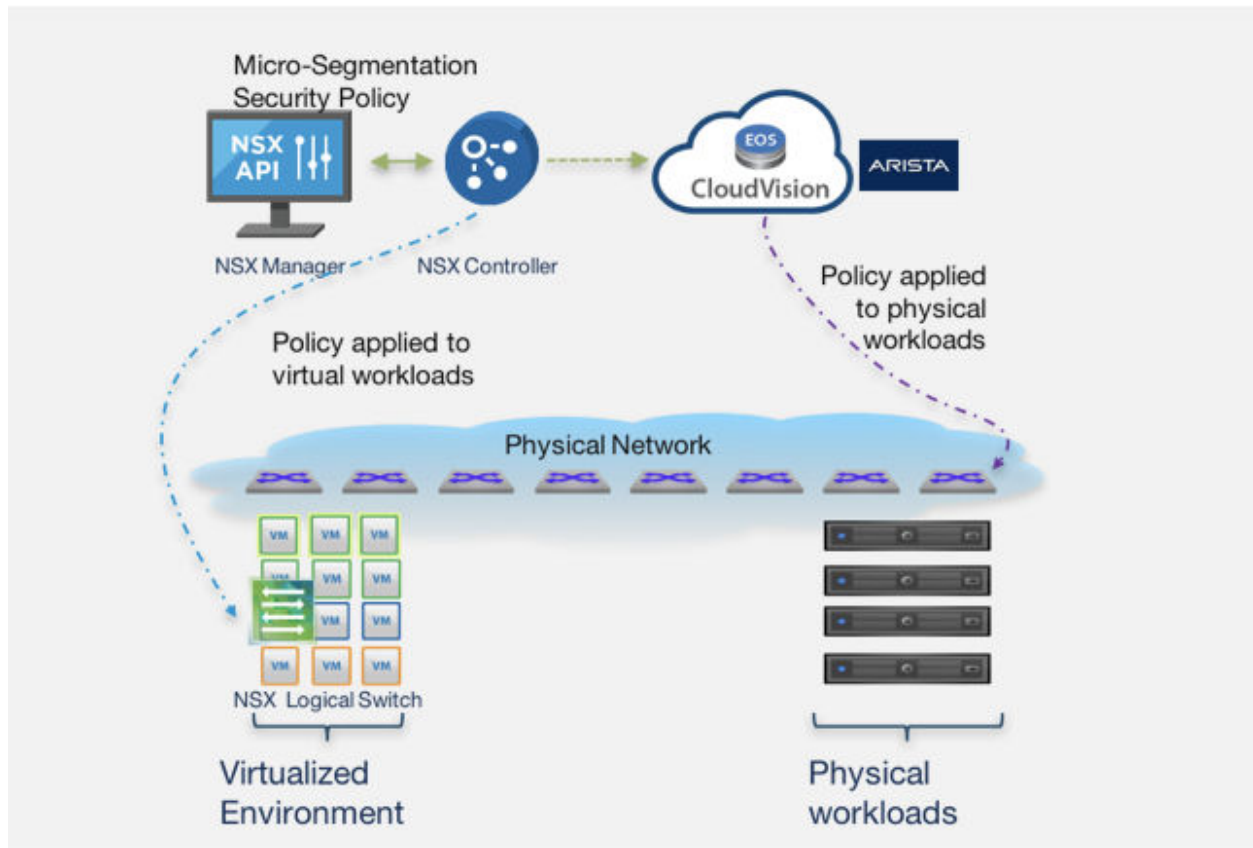
- 9 [発行] をクリックします。

物理ワークロードへのセキュリティ ポリシーの拡張

NSX-T Data Center は、仮想ワークロードと物理ワークロードの両方の単一の管理ポイントとして機能できます。

NSX-T Data Center 2.5.1 以降では、Arista CloudVision eXchange (CVX) との連携がサポートされています。この連携により、アプリケーション フレームワークや物理ネットワーク インフラストラクチャに依存せずに、仮想ワークロードと物理ワークロードに一貫したネットワーク サービスとセキュリティ サービスを提供できます。NSX-T Data Center は物理ネットワーク スイッチまたはルーターを直接プログラミングしませんが、物理 SDN コントローラ レベルで統合することで、セキュリティ管理者と物理ネットワーク管理者の自律性が維持されます。

NSX-T Data Center 2.5.1 以降では、Arista EOS 4.22.1FX-PCS 以降との連携がサポートされています。



制限事項

- Arista スイッチに接続されているエンド ホストにファイアウォール ルールが適用される前に、Arista スイッチに ARP トラフィックが存在する必要があります。そのため、トラフィックをブロックするようにファイアウォール ルールを設定する前に、パケットがスイッチを通過する可能性があります。
- スイッチがクラッシュまたは再ロードされると、許可されたトラフィックは再開されません。スイッチにファイアウォール ルールを適用するには、スイッチの起動後に ARP テーブルに再度入力する必要があります。
- Arista 物理スイッチに接続された FTP サーバに接続する FTP パッシブ クライアントでは、ファイアウォール ルールを Arista 物理スイッチに適用することはできません。
- CVX クラスタに仮想 IP アドレスを使用する CVX HA の設定では、CVX 仮想マシンの `dvpg` の無作為検出モードと偽装転送を [承諾] に設定する必要があります。デフォルト ([拒否]) に設定されている場合、CVX HA 仮想 IP アドレスには NSX Manager からアクセスできません。

NSX-T Manager との通信のための Arista CVX の設定

NSX-T Data Center を設定したら、Arista CloudVision eXchange (CVX) の構成手順を完了して、CVX が NSX-T Data Center と通信できるようにします。

前提条件

NSX-T Data Center が CVX を適用ポイントとして登録していること。

手順

- 1 root ユーザーとして NSX Manager にログインし、次のコマンドを実行して CVX が NSX Manager と通信するためのサムプリントを作成します。

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

出力例：

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 CVX CLI から次のコマンドを実行します。

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 CVX CLI から次のコマンドを実行して、構成を確認します。

```
show running-config
```

出力例：

```
cvx
    no shutdown
    source-interface Management1
    !
    service hsc
        no shutdown

    !
    service pcs
        no shutdown
        controller 192.168.2.80
        username admin
```

```
password 7 046D26110E33491F482F2800131909556B
enforcement-point cvx-default-ep
pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
notification-id a0286cb6-de4d-41de-99a0-294465345b80
```

- 4 物理サーバに接続する物理スイッチのイーサネット インターフェイスで tag を構成します。CVX で管理されている物理スイッチで次のコマンドを実行します。

```
configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.
```

- 5 次のコマンドを実行して、スイッチの tag 構成を確認します。

```
show running-config section tag
```

出力例：

```
interface Ethernet4
description connected-to-7150s-3
switchport trunk allowed vlan 1-4093
switchport mode trunk
tag sx4_app_server
```

ARP を使用してタグ付きインターフェイスで学習された IP アドレスは NSX-T Data Center と共有されます。

- 6 NSX Manager にログインして、CVX で管理される物理ワークロードのファイアウォール ルールを作成および公開します。ルール作成の詳細については、[10 章 セキュリティ](#)を参照してください。次はその例です。

ポリシーの追加

ルールを追加

クローン作成

取り消す

削除

	<input type="checkbox"/>	名前	送信元	宛先	サービス	プロファイル	適用先	アクション		
⋮	▼	<input type="checkbox"/> Firewall_Services (2)	適用先 分散ファイアウォー						●稼動中	🔄 ⓘ ⚙️
⋮		<input type="checkbox"/> vm_to_phy_server ⓘ	🌐 vm	🌐 phy_server	任意	なし	分散ファイアウォー	●許可 ▼	🟢 ⓘ ⚙️	
⋮		<input type="checkbox"/> phy_server_to_vm ⓘ	🌐 phy_server	🌐 vm	任意	なし	分散ファイアウォー	●許可 ▼	🟢 ⓘ ⚙️	

NSX-T Data Center で公開される NSX-T Data Center ポリシーとルールは、CVX で管理される物理スイッチ上の動的 ACL として表示されます。

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
  10 permit ip host 71.1.1.3 host 27.1.1.11

IP Access List et4.v4.out [dynamic]
  10 permit ip host 27.1.1.11 host 71.1.1.3
```

詳細については [CVX HA のセットアップ](#)、[CVX HA 仮想 IP アドレスのセットアップ](#)、および [物理スイッチ Mlag のセットアップ](#) を参照してください。

Arista CVX と通信するための NSX-T Data Center の設定

NSX-T Data Center での構成手順を完了して、CVX を NSX-T Data Center の適用ポイントとして追加し NSX-T Data Center が CVX と通信できるようにします。

前提条件

Arista CVX クラスターの仮想 IP アドレスを取得します。

手順

- 1 root ユーザーとして NSX Manager にログインし、次のコマンドを実行して CVX のサムプリントを取得します。

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

出力例：

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 取得されたサムプリントを編集して小文字のみを使用するようにし、サムプリントからすべてのコロンの(:)を除外します。

CVX の編集済みサムプリントの例：

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 PATCH /policy/api/v1/infra/sites/default/enforcement-points API を呼び出し、CVX サムプリントを使用して CVX の適用エンドポイントを作成します。次はその例です。

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 GET /policy/api/v1/infra/sites/default/enforcement-points API を呼び出して、エンドポイント情報を取得します。次はその例です。

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "admin",
    "password": "1q2w3e4rT",
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
  }
}
```

出力例：

```
{
  "connection_info": {
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
    "enforcement_point_address": "192.168.2.198",
    "resource_type": "CvxConnectionInfo"
  },
  "auto_enforce": false,
  "resource_type": "EnforcementPoint",
  "id": "cvx-default-ep",
  "display_name": "cvx-default-ep",
  "path": "/infra/sites/default/enforcement-points/cvx-default-ep",
  "relative_path": "cvx-default-ep",
  "parent_path": "/infra/sites/default",
  "marked_for_delete": false,
  "_system_owned": false,
  "_create_user": "admin",
  "_create_time": 1564036461953,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564036461953,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

- 5 POST /api/v1/notification-watchers/ API を呼び出し、CVX サンプリントを使用して通知 ID を作成します。次はその例です。

```
POST https://<nsx-manager>/api/v1/notification-watchers/
{
  "server": "<virtual IP address of CVX cluster>",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "use_https": true,
  "certificate_sha256_thumbprint":
    "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
```

```
"username": "cvpadmin",
"password": "1q2w3e4rT"
}
}
```

- 6 GET /api/v1/notification-watchers/ を呼び出して、通知 ID を取得します。

出力例：

```
{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
"35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
  "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
  "_create_user": "admin",
  "_create_time": 1564038044780,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564038044780,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

- 7 PATCH /policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap API を呼び出して、CVX ドメイン展開マップを作成します。次はその例です。

```
PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-
default-dmap
{

  "display_name": "cvx-deployment-map",

  "id": "cvx-default-dmap",

  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"

}
```

- 8 GET /policy/api/v1/infra/domains/default/domain-deployment-maps API を呼び出して、展開マップ情報を取得します。

共有アドレス セット

動的オブジェクトまたは論理オブジェクトに基づくセキュリティ グループを作成し、分散ファイアウォール ルールの [適用先] テキスト ボックスで 사용할 수 있습니다.

アドレス セットは仮想マシン名またはタグに基づいて動的に設定されるため、各フィルタで更新する必要があります。これにより、ホスト上で使用可能なヒープ メモリがすべて使用され、DFW ルールと IP アドレス セットを保存できない場合があります。

NSX-T Data Center バージョン 2.5 以降では、グローバル アドレス セットまたは共有アドレス セット機能で、すべてのフィルタでアドレス セットを共有할 수 있습니다。[適用先] に基づいて各フィルタに異なるルールを設定し、すべてのフィルタで同じアドレス セット メンバーを共有할 수 있습니다。この機能はデフォルトで有効になっているため、ヒープ メモリの使用量が減少합니다。無効にすることはできません。

NSX-T Data Center バージョン 2.4 以前では、グローバル アドレス セットまたは共有アドレス セットは無効になっています。このため、分散ファイアウォール ルールの処理量の多い環境では、VSIP ヒープがすべて使用される可能性があります。

East-West ネットワーク セキュリティ : サードパーティ サービスのチェーン

パートナーが侵入検知システムや侵入防止システム (IDS/IPS) などのネットワーク サービスを NSX-T Data Center に登録した後、ユーザーは管理者として、オンプレミス データセンターの仮想マシン間で移動する East-West トラフィックにイントロスペクションを行うように、ネットワーク サービスを設定할 수 있습니다.

前提条件

- パートナーが、NSX-T Data Center にサービスを登録している必要があります。
- ESXi ホストが、トランスポート ノード プロファイルを使用して NSX-T Data Center トランスポート ノードとして準備されている必要があります。

注 :

- サービス仮想マシンは、ESXi ホストでのみサポートされます。KVM ホストではサポートされません。
- NSX-T Data Center は、ESXi ホストで実行されているゲスト仮想マシンのみを保護합니다。
- NSX-T Data Center は、KVM ホストで実行されているゲスト仮想マシンを保護しません。

ネットワーク保護の主な概念 (East-West)

オンプレミス データセンターのゲスト仮想マシン間で送受信されるトラフィックは、パートナーが提供するサードパーティ サービスによって保護されます。以下の概念を把握すると、ワークフローの理解に役立ちます。

- サービス : 파트너가 NSX-T Data Center に 서비스를 등록합니다。서비스는, 파트너가 제공하는セキュリティ 기능や、서비스展開の詳細 (서비스仮想마신의 OVF URL、서비스의接続포인트、서비스의 상태など) を表합니다。

- **ベンダー テンプレート**：ネットワーク トラフィックに対してサービスが実行できる機能で構成されています。パートナーは、ベンダー テンプレートを定義します。たとえば、ベンダー テンプレートを使用して、IPsec サービスによるトンネリングなどのネットワーク操作サービスを実行できます。
- **サービス プロファイル**：ベンダー テンプレートのインスタンスです。NSX-T Data Center 管理者は、サービス仮想マシンで使用されるサービス プロファイルを作成できます。
- **ゲスト仮想マシン**：ネットワーク内のトラフィックの送信元または宛先です。受信トラフィックまたは送信トラフィックは、ルールに対して定義された、East-West ネットワーク サービスを実行するサービス チェーンによって調査されます。
- **サービス仮想マシン**：サービスによって指定された OVA または OVF アプライアンスを実行する仮想マシンです。サービス プレーンを介して接続されていて、リダイレクトされたトラフィックを受信します。
- **サービス インスタンス**：ホストにサービスが展開されたときに作成されます。各サービス インスタンスには、対応するサービス仮想マシンがあります。
- **サービス セグメント**：トランスポート ゾーンに関連付けられているサービス プレーンのセグメントです。各サービスの接続は、他のサービスの接続、および NSX-T によって提供される標準の L2 または L3 ネットワーク セグメントから分離されています。サービスの接続はサービス プレーンによって管理されます。
- **Service Manager**：一連のサービスを参照するパートナーの Service Manager です。
- **サービス チェーン**：管理者によって定義されたサービス プロファイルの論理シーケンスです。サービス プロファイルは、サービス チェーンで定義されている順序でネットワーク トラフィックのイントロスペクションを実行します。たとえば、最初のサービス プロファイルはファイアウォール、2 番目のサービス プロファイルはモニターのようになります。サービス チェーンは、トラフィックの方向（出力/入力）ごとに異なる順序でサービス プロファイルを指定します。
- **リダイレクト ポリシー**：特定のサービス チェーンに分類されているトラフィックは、そのサービス チェーンにリダイレクトされます。これは、NSX-T Data Center セキュリティ グループおよびサービス チェーンと一致するトラフィック パターンに基づいて決まります。パターンと一致するすべてのトラフィックは、サービス チェーンに沿ってリダイレクトされます。
- **サービス パス**：サービス チェーンのサービス プロファイルを実装する一連のサービス仮想マシンです。管理者は、サービス プロファイルを事前に定義された順序で並べたサービス チェーンを定義します。NSX-T Data Center は、ゲスト仮想マシンおよびサービス仮想マシンの数および場所に基づいて、サービス チェーンから複数のサービス パスを生成します。また、トラフィック フローのイントロスペクションを行う上で最適なサービス パスを選択します。各サービス パスはサービス パス インデックス (SPI) によって識別され、各ホップには、パスに沿って一意のサービス インデックス (SI) が付与されます。

East-West トラフィックに関する NSX-T Data Center の要件

NSX-T Data Center 環境では、オーバーレイ トランスポート ゾーンとオーバーレイでバックアップされる論理スイッチが存在することを確認する必要があります。

East-West のサービス挿入は、NSX-T 環境全体に適用されます。クラスタ レベルまたはホスト レベルでサービスを展開することはできません。

サービスは、GENEVE またはオーバーレイでバックアップされた論理スイッチにトラフィックを送信するため、すべてのトランスポート ノードをオーバーレイ タイプにする必要があります。オーバーレイ（または GENEVE）でバックアップされた論理スイッチは内部でプロビジョニングされ、ユーザー インターフェイスには表示されません。

VLAN でバックアップされた論理スイッチのみを使用して展開する場合でも、East-West トラフィックはオーバーレイ トランスポート ゾーンとオーバーレイでバックアップされた論理スイッチを通過します。したがって、オーバーレイ トランスポート ゾーンと GENEVE でバックアップされた論理スイッチを作成する必要があります。この要件を満たさないと、vMotion の実行中にホスト上の ゲスト仮想マシン を別のトランスポート ノードに移行できません。ゲスト仮想マシンは切断状態になり、East-West のサービスで構成エラーが発生します。

East-West ネットワーク セキュリティの手順

次の手順に従って、East-West トラフィックのネットワーク セキュリティを設定します。

表 10-3. East-West ネットワーク イントロスペクションを設定するタスクのリスト

ワークフロー タスク	個人設定	実装方法
サービスの登録	パートナー	API のみ
ベンダー テンプレートの登録	パートナー	API のみ
Service Manager の登録	パートナー	API のみ
East-West トラフィックのイントロスペクション用サービスの展開	管理者	API および NSX Manager UI
サービス プロファイルの追加	管理者	API および NSX Manager UI
サービス チェーンの追加	管理者	API および NSX Manager UI
East-West トラフィックのリダイレクト ルールの追加	管理者	API および NSX Manager UI

East-West トラフィックのイントロスペクション用サービスの展開

パートナーがサービスを登録した後に、管理者は、クラスタのメンバー ホストにサービスのインスタンスを展開する必要があります。

クラスタ内のすべての NSX-T Data Center ホストに、パートナー セキュリティ エンジンを実行するパートナー サービス仮想マシンを展開します。サービス仮想マシンを展開したら、ここで使用するポリシー ルールを作成して、ゲスト仮想マシンを保護することができます。

前提条件

- すべてのホストが、vCenter Server によって管理されていること。
- パートナー サービスが NSX-T Data Center に登録されていて、展開準備ができていないこと。
- NSX-T Data Center 管理者が、パートナー サービスおよびベンダー テンプレートにアクセスできること
- サービス仮想マシンとパートナーの Service Manager（コンソール）の両方が、管理ネットワーク レベルで相互に通信できること。

- ホストベースのサービス展開：各ホストにサービス仮想マシンを展開する前に、トランスポート ノード プロファイルを適用して、NSX-T Data Center でクラスタの各ホストを設定します。

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 [システム] - [サービス展開] - [展開] - [サービスの展開] を選択します。
- 3 [パートナー サービス] フィールドでパートナー サービスを選択します。
- 4 サービスの展開名を入力します。
- 5 [コンピュート マネージャ] フィールドで、サービスを展開する vCenter Server を選択します。
- 6 [クラスタ] フィールドで、サービスを展開する必要があるクラスタを選択します。
- 7 [データストア] ドロップ ダウン メニューで、サービス仮想マシンのリポジトリとしてデータ ストアを選択します。
- 8 [ネットワーク] 列で [設定] をクリックし、DHCP または固定 IP アドレス タイプ、およびデータ ネットワークを選択して、管理ネットワーク インターフェイスを入力します。
- 9 [サービス セグメント] フィールドのリストからサービス セグメントを選択するか、[アクション] アイコンをクリックしてサービス セグメントを追加または編集します。サービス セグメントに接続されたゲスト仮想マシンは、East-West ネットワークのトラフィックを保護します。
- 10 [展開タイプ] フィールドで、次のいずれかの展開オプションを選択します。パートナーによって登録されたサービスに応じて、複数のサービスを単一のサービス仮想マシンの一部として展開できます。
 - クラスタ化：ホスト サービス仮想マシン専用のクラスタに属するホストにサービスを展開します。
 - ホストベース：クラスタ内のすべてのホストにサービスを展開します。
- 11 [展開テンプレート] フィールドで、ゲスト仮想マシン グループで実行するワークロードを保護する属性を含むテンプレートを選択します。
- 12 (クラスタベースの展開の場合のみ) [クラスタ化された展開の数] に、クラスタに展開するサービス仮想マシンの数を入力します。サービス仮想マシンを展開するホストは、vCenter Server によって決定されます。
- 13 [保存] をクリックします。

結果

サービスを展開した後、パートナーの Service Manager に更新に関する通知が送信されます。

次のステップ

ホストに展開されたサービス インスタンスに関する展開の詳細および健全性の状態を確認します。[サービス プロファイルの追加](#) を参照してください。

サービス プロファイルの追加

サービス プロファイルは、パートナー ベンダー テンプレートのインスタンスです。管理者は、ベンダー テンプレートの属性をカスタマイズして、テンプレートのインスタンスを作成できます。

注： 1つのベンダーに複数のサービス プロファイルを作成できます。たとえば、転送パスに設定したサービス プロファイルが IDS 保護を提供し、リバース パスに設定したサービス プロファイルが IPS 保護をサポートします。ただし、1つのサービス プロファイルを転送パスとリバース パスの両方に設定できます。

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 [セキュリティ] - [East-West のセキュリティ] - [ネットワーク イントロスペクション] - [サービス プロファイル] に移動します。
- 3 [パートナー サービス] ドロップダウン フィールドから、サービスを選択します。選択したサービスのサービス プロファイルを作成できます。
- 4 サービス プロファイル名を入力し、ベンダー テンプレートを選択します。
- 5 [リダイレクト アクション] フィールドは、ベンダー テンプレートから機能を継承します。たとえば、COPY がベンダー テンプレートから提供された機能の場合、デフォルトでは、サービス プロファイルを作成するときリダイレクト アクションは COPY になります。
- 6 (オプション) サービス プロファイルを除外して管理するには、任意のタグを定義します。
- 7 [保存] をクリックします。

結果

パートナー サービスの新規サービス プロファイルが作成されます。

次のステップ

サービス チェーンを追加します。[サービス チェーンの追加](#) を参照してください。

サービス チェーンの追加

サービス チェーンは、ネットワーク管理者によって定義されたサービス プロファイルの論理的なシーケンスです。

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 [セキュリティ] - [East-West のセキュリティ] - [ネットワーク イントロスペクション] - [サービス チェーン] - [チェーンの追加] を選択します。
- 3 サービス チェーンの名前を入力します。

- 4 [サービス セグメント] フィールドで、サービス チェーンを適用するサービス セグメントを選択します。サービス セグメントは、オーバーレイ トランスポート ゾーンの複数のサービス仮想マシンを接続するサービス プレーンのセグメントです。サービス チェーン内の各サービス仮想マシンは、NSX-T Data Center で実行されている別のサービス仮想マシンおよび L2 と L3 のネットワーク セグメントから独立しています。サービス プレーンはサービス仮想マシンへのアクセスを制御します。
- 5 転送パスを設定するには、[転送パスの設定] フィールドをクリックして、[プロファイルを順番に追加] をクリックします。
- 6 サービス チェーン内に最初のプロファイルを追加して、[追加] をクリックします。
- 7 次のサービス プロファイルを指定するには、[プロファイルを順番に追加] をクリックして詳細を入力します。上下の矢印アイコンを使用して、プロファイルの順序を並べ替えることもできます。
- 8 [保存] をクリックして、サービス チェーンの転送パスの追加を完了します。
- 9 [リバース パス] 列で、転送パスに設定したサービス プロファイルを使用するサービス プレーンに [リバース パス] を選択します。
- 10 リバース パスに新しいサービス プロファイルを設定するには、[リバース パスの設定] をクリックして、サービス プロファイルを追加します。
- 11 [保存] をクリックして、サービス チェーンのリバース パスの追加を完了します。
- 12 [エラー ポリシー] フィールドで次の操作を行います。
 - [許可] を選択して、サービス仮想マシンに障害が発生した場合に、宛先仮想マシンにトラフィックを送信できるようにします。サービス仮想マシンの障害は、パートナーのみが有効にできるライブネス検出メカニズムによって検出されます。
 - [ブロック] を選択して、サービス仮想マシンに障害が発生した場合に、宛先仮想マシンにトラフィックを送信しないようにします。
- 13 [保存] をクリックします。

結果

サービス チェーンを追加した後、パートナーの Service Manager に更新に関する通知が送信されます。

次のステップ

East-West ネットワーク トラフィックのイントロスペクションを行うためのリダイレクト ルールを作成します。
[East-West トラフィックのリダイレクト ルールの追加](#) を参照してください。

East-West トラフィックのリダイレクト ルールの追加

ネットワーク イントロスペクションのために East-West トラフィックをリダイレクトするルールを追加します。

ルールはポリシーで定義されます。概念としてのポリシーは、ファイアウォールのセクションの概念と似ています。ポリシーを追加するときに、サービス チェーンのサービス プロファイルでイントロスペクションのトラフィックをリダイレクトするサービス チェーンを選択します。

ルールの定義は、トラフィックの送信元と宛先、イントロスペクション サービス、ルールを適用する NSX-T Data Center オブジェクト、およびトラフィックのリダイレクト ポリシーで構成されます。ルールを発行した後に一致するトラフィック パターンが見つかり、NSX Manager はルールをトリガします。このルールによって、トラフィックのイントロスペクションが開始されます。たとえば、イントロスペクションを行う必要があるトラフィック フローを分類するときに、NSX Manager は通常の分散ファイアウォールにトラフィックを転送せず、ポリシー内で指定されたサービス チェーンに沿ってこのトラフィックをリダイレクトします。サービス チェーン内で定義されたサービス プロファイルは、パートナーが提供するネットワーク サービスのトラフィックにイントロスペクションを実行します。サービス プロファイルによるイントロスペクションが完了しても、トラフィック内にセキュリティ上の問題が検出されなかった場合、トラフィックはサービス チェーン内の次のサービス プロファイルに転送されます。サービス チェーンの終わりに達すると、トラフィックは宛先に転送されます。

すべての通知は、パートナーの Service Manager および NSX-T Data Center に送信されます。

前提条件

サービス チェーンを使用して East-West トラフィックをリダイレクトし、ネットワーク イントロスペクションを行うことができること

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 [セキュリティ] - [East-West のセキュリティ] - [ネットワーク イントロスペクション] - [ルール] - [ポリシーの追加]。

ポリシー セクションは、トラフィック フローの仕組みを決定するルールが定義されるファイアウォール セクションと似ています。

- 3 サービス チェーンを選択します。
- 4 ポリシーを追加するには、[発行] をクリックします。
- 5 セクションにある垂直方向の省略記号 (⋮) をクリックして、[ルールの追加] をクリックします。

- 6 [送信元] フィールドを編集し、メンバーシップの基準、静的メンバー、IP/MAC アドレス、または Active Directory グループを定義してグループを追加します。
 - a 次のいずれかのエンティティを使用して、メンバーシップ基準を定義します。
 - 仮想マシン
 - 論理スイッチ
 - 論理ポート
 - IP セット
 - b 次のいずれかのエンティティを使用して、固定メンバー リストを定義します。
 - グループ
 - セグメント
 - セグメント ポート
 - 仮想ネットワーク インターフェイス
 - 仮想マシン
- 7 [保存] をクリックします。
- 8 宛先グループを追加するには、[宛先] フィールドを編集します。
- 9 [適用先] フィールドでは、次のいずれかの操作を実行できます。
 - 論理スイッチに接続されているすべての仮想 NIC にルールを適用するには、[DFW] を選択します。
 - グループのメンバー仮想マシンの仮想 NIC にルールを適用するには、[仮想マシン グループ] を選択します。メンバーは、静的リストから選択するか、動的な基準に基づいて選択することができます。サポートされている NSX-T Data Center オブジェクトは、仮想マシン、論理スイッチ、論理ポート、IP セットなどです。
- 10 サービス チェーンに沿ってトラフィックをリダイレクトするには、[アクション] フィールドで [リダイレクト] を選択します。トラフィックにネットワーク イントロスペクションを適用しない場合は、[リダイレクトしない] を選択します。
- 11 [発行] をクリックします。
- 12 発行されたルールを元に戻すには、ルールを選択して [元に戻す] をクリックします。
- 13 ポリシーを追加するには、[+ ポリシーの追加] をクリックします。
- 14 ポリシーまたはルールのクローンを作成するには、ポリシーまたはルールを選択して、[クローン作成] をクリックします。
- 15 ルールを有効にするには、[有効]/[無効] アイコンを有効にするか、ルールを選択して、メニューから [有効] > [ルールの有効化] の順にクリックします。
- 16 ルールを有効または無効にしたら、[発行] をクリックしてルールを適用します。

結果

送信元に送信されるトラフィックはサービス チェーンにリダイレクトされ、ネットワーク イントロスペクションが行われます。チェーン内のサービス プロファイルによってトラフィックのイントロスペクションが行われた後、トラフィックは宛先に送信されます。

展開中に、特定のポリシーの仮想マシン グループ メンバーシップが変更されることがあります。NSX-T Data Center からパートナーの Service Manager にこれらの更新について通知されます。

ゲートウェイ ファイアウォールの設定

ゲートウェイ ファイアウォールは、境界ファイアウォールで適用されるルールを表します。

[すべての共有ルール] ビューには事前定義されたカテゴリがあり、すべてのゲートウェイのルールが表示されます。ルールは、上から下、左から右に評価されます。API を使用すると、カテゴリ名を変更できます。

表 10-4. ゲートウェイ ファイアウォール ルールのカテゴリ

ルールのカテゴリ	目的
緊急	検疫に使用します。許可ルールにも使用できます。
システム	これらのルールは NSX-T Data Center によって自動的に生成され、BFD ルール、VPN ルールなどの内部制御プレーン トラフィックに対して固有です。 注： システム ルールは編集しないでください。
共有された事前ルール	これらのルールは、ゲートウェイ間でグローバルに適用されます。
ローカル ゲートウェイ	これらのルールは、特定のゲートウェイに対して固有です。
自動サービス ルール	これらは、データ プレーンに適用される、自動的に設定されたルールです。必要に応じて、これらのルールを編集できます。
デフォルト	これらのルールは、ゲートウェイ ファイアウォールのデフォルトの動作を定義します。

ゲートウェイ ファイアウォールのポリシーおよびルールの追加

ゲートウェイ ファイアウォール ルールを実装するには、事前に定義されたカテゴリに属するファイアウォール ポリシー セクションにこれらのルールを追加します。

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 [セキュリティ] - [North-South のセキュリティ] - [ゲートウェイ ファイアウォール] の順に選択します。
- 3 ゲートウェイ ファイアウォールを有効にするには、[アクション] - [全般設定] の順に選択し、状態ボタンを切り替えます。[保存] をクリックします。
- 4 [ポリシーの追加] をクリックします。カテゴリの詳細については、[ゲートウェイ ファイアウォールの設定](#)を参照してください。

- 5 新しいポリシー セクションの [名前] を入力します。
- 6 ポリシーの [宛先] を選択します。
- 7 歯車アイコンをクリックし、次のポリシーを構成します。

設定	説明
TCP Strict	3 ウェイ ハンドシェイク (SYN、SYN ACK、ACK) で TCP 接続が開始し、通常、2 方向の交換 (FIN、ACK) で接続が終了します。特定の状況では、ファイアウォールに特定のフローの 3 ウェイ ハンドシェイクが検証されない場合があります (たとえば、トラフィックが非対称になっている場合など)。デフォルトでは、ファイアウォールは 3 ウェイ ハンドシェイクを検証する必要がないため、すでに確立されているセッションをピックアップします。TCP Strict をセッションごとに有効にして、中間セッションのピックアップをオフにし、3 ウェイ ハンドシェイクの要件を適用できます。特定のファイアウォール ポリシーで TCP Strict モードを有効にし、デフォルトの ANY-ANY Block ルールを使用すると、3 ウェイ ハンドシェイクの接続要件を満たしていないパケットと、このポリシー セクションの TCP ベースのルールに一致するパケットがドロップされます。Strict はステートフル TCP ルールにのみ適用され、ゲートウェイファイアウォール ポリシー レベルで有効になります。TCP Strict は、TCP サービスが指定されていないデフォルトの ANY-ANY Allow と一致するパケットには適用されません。
ステートフル	ステートフル ファイアウォールは、アクティブな接続の状態を監視し、この情報を使用してファイアウォールの通過を許可するパケットを決定します。
ロック済み	複数のユーザーが同じセクションに変更を加えることを防ぐため、ポリシーをロックできます。セクションをロックする場合は、コメントを含める必要があります。

- 8 [発行] をクリックします。複数のポリシーを追加し、まとめて一度に発行できます。
新しいポリシーは画面に表示されます。
- 9 ポリシーのセクションを選択し、[ルールの追加] をクリックします。
- 10 ルールの名前を入力します。IPv4、IPv6、マルチキャスト アドレスがサポートされています。
- 11 [送信元] 列で、編集アイコンをクリックし、ルールのソースを選択します。詳細については[グループの追加](#)を参照してください。
- 12 [宛先] 列で、編集アイコンをクリックし、ルールの宛先を選択します。定義しない場合、宛先はすべてに一致します。詳細については[グループの追加](#)を参照してください。
- 13 [サービス] 列で鉛筆アイコンをクリックし、サービスを選択します。サービスを定義しない場合は、そのすべてと一致します。
- 14 [プロファイル] 列で編集アイコンをクリックしてコンテキスト プロファイルを選択するか、[新しいコンテキスト プロファイルの追加] をクリックします。[コンテキスト プロファイルの追加](#) を参照してください。
 - コンテキスト プロファイルは、Tier-0 ゲートウェイ ファイアウォール ポリシーでサポートされていません。

- ゲートウェイ ファイアウォール ルールでは、FQDN 属性または他のサブ属性を含むコンテキスト プロファイルはサポートされません。

コンテキスト プロファイルは、分散ファイアウォール ルールとゲートウェイ ファイアウォール ルールでレイヤー 7 アプリケーション ID 属性を使用します。サービスが [任意] に設定されたファイアウォール ルールには、複数のアプリケーション ID コンテキスト プロファイルを使用できます。ALG プロファイル (FTP または TFTP) の場合、1 つのルールでサポートされるコンテキスト プロファイルは 1 つだけです。

15 [適用] をクリックします。

16 [適用先] 列には、ルールごとの適用範囲を定義します。これにより、ユーザーは、1 つ以上のアップリンク インターフェイスまたはサービス インターフェイスにルールを選択的に適用できます。デフォルトでは、ゲートウェイ ファイアウォール ルールは、選択したゲートウェイで使用可能なすべてのアップリンク インターフェイスとサービス インターフェイスに適用されます。

17 [アクション] 列で、アクションを選択します。

オプション	説明
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トラフィックに、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。パケットが却下されると、宛先到達不能のメッセージが送信者に送信されます。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。接続が確立できない場合、送信元のアプリケーションに通知されます。

18 状態の切り替えボタンをクリックし、ルールを有効または無効にします。

19 歯車アイコンをクリックして、ログ作成、方向、IP プロトコル、タグ、およびメモを設定します。

オプション	説明
ログの記録	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、Edge の /var/log/syslog に保存されます。
方向	オプションは、受信、送信、および 受信/送信 です。デフォルトは 受信/送信 です。このフィールドは、ゲートウェイのアップリンク インターフェイスまたはサービス インターフェイスから見たトラフィックの方向を示します。受信 はアップリンク インターフェイスまたはサービス インターフェイスから入ってくるトラフィックのみ、送信 はアップリンク インターフェイスまたはサービス インターフェイスから出ていくトラフィックのみ、受信/送信 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。

オプション	説明
IP プロトコル	オプションは、IPv4、IPv6、および IPv4_IPv6 です。デフォルトは IPv4_IPv6 です。
タグ	ルールに追加されているタグです。

注： グラフ アイコンをクリックして、ファイアウォール ルールのフロー統計を表示します。バイト数、パケット数、セッション数などの情報を表示できます。

20 [発行] をクリックします。複数のルールを追加し、まとめて一度に発行できます。

21 各ポリシー セクションで [情報] アイコンをクリックし、Edge ノードにプッシュした Edge ファイアウォール ルールの現在の状態を確認します。ルールが Edge ノードにプッシュされたときに生成されたすべてのアラームも表示されます。

22 Edge ノードに適用されるポリシー ルールの統合の状態を表示するには、API 呼び出しを行います。

```
GET https://<policy-mgr>/policy/api/v1/infra/realized-state/status?
intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

North-South ネットワーク セキュリティ：サードパーティ サービスの挿入

NSX-T Data Center では、データセンターの Tier-0 または Tier-1 ルーターにサードパーティのサービスを挿入し、サードパーティ サービスにトラフィックをリダイレクトしてイントロスペクションを行うことができます。North-South のサービス仮想マシンの展開には、ESXi ホストのみがサポートされています。KVM ホストはサポートされません。

North-South ネットワーク セキュリティの手順

次の手順に従って、North-South トラフィックのネットワーク セキュリティを設定します。

表 10-5. North-South ネットワーク イントロスペクションを設定するタスクのリスト

ワークフロー タスク	個人設定	実装方法
NSX-T Data Center へのサービスの登録	パートナー	API のみ
North-South トラフィックのイントロスペクション用サービスの展開	管理者	API および NSX Manager UI
トラフィックのリダイレクトを設定	管理者	API および NSX Manager UI

North-South トラフィックのイントロスペクション用サービスの展開

サービスを登録した後、サービスがネットワーク トラフィックの処理を開始できるように、サービスのインスタンスを展開する必要があります。

Tier-0 または Tier-1 論理ルーターに、物理環境と vCenter Server の論理ネットワーク間のゲートウェイとして機能するパートナー サービス仮想マシンを展開します。サービス仮想マシンをスタンドアローン サービス インスタンスまたはアクティブ/スタンバイ サービス インスタンスとして展開した後に、サービス仮想マシンにトラフィックをリダイレクトするリダイレクト ルールを作成して、ネットワーク イントロスペクションを行うことができます。

前提条件

- すべてのホストが、vCenter Server によって管理されていること。
- パートナー サービスは NSX-T Data Center に登録されていて、展開する準備ができていること。
- NSX-T Data Center 管理者は、パートナー サービスにアクセスできます。
- 論理ルーターの高可用性モードは、アクティブ/スタンバイ モードにする必要があります。
- 分散リソース スケジューラ ユーティリティをオンにします。

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 [ネットワークとセキュリティの詳細設定] - [パートナー サービス] - [サービス インスタンス] - [カタログ] を選択します。
- 3 [カタログ] タブに、登録されたサービスが表示されます。
- 4 OVF フォーム ファクタに表示されているサービスを選択して、[展開] をクリックして、サービス インスタンスの展開を開始します。
- 5 [パートナー サービス挿入] ウィンドウで [続行] をクリックします。
- 6 [パートナー サービス] ウィンドウに詳細を入力します。

表 10-6. パートナー サービスの詳細

フィールド	説明
インスタンス名	サービス インスタンスを識別する名前を入力します。
説明	サービス インスタンスに関する説明です。
パートナー サービス	NSX-T Data Center に登録されているパートナー サービスを選択します。
展開の仕様	展開するフォーム ファクタを選択します。
論理ルーター	サービス インスタンスを展開する必要がある Tier-0 論理ルーターを選択します。

- 7 [次へ] をクリックします。

8 [インスタンスの設定] ウィンドウに詳細を入力します。

表 10-7. サービス インスタンスの詳細

フィールド	説明
展開モード	[スタンドアローン] を選択して、Tier-0 論理ルーターに単一のサービス インスタンスを展開します。 [高可用性] を選択して、Tier-0 論理ルーターにアクティブ/スタンバイ モードの 2 つのサービス インスタンスを展開します。
エラー ポリシー	[許可] または [ブロック] を選択します。
サービス インスタンスの IP アドレス	サービス インスタンスで使用する IP アドレスを入力します。
ゲートウェイ	ゲートウェイ アドレスを入力します。
サブネット マスク	サブネット マスクを入力します。
ネットワーク ID	管理ネットワークを接続する論理スイッチのネットワーク ID を入力します。
コンピュート マネージャ	登録された vCenter Server を選択します。
リソース プール	サービス インスタンスを展開するためのリソースを提供するリソース プールを選択します。
データストア	サービス インスタンスのデータを格納するリポジトリを選択します。

9 [次へ] をクリックします。

10 [高度な設定] ウィンドウに詳細を入力します。

表 10-8.

フィールド	説明
展開テンプレート	サービス インスタンスを展開するときに使用するテンプレートを選択します。
ライセンス	テンプレートのライセンスを入力します。

11 [終了] をクリックします。

結果

[サービス インスタンス] タブに、展開の進行状況が表示されます。展開が完了するまでに数分間かかる場合があります。展開状態を検証して、サービス インスタンスが Tier-0 論理ルーターに正常に展開されていることを確認します。

または、vCenter Server に移動して、展開の状態を確認します。

次のステップ

Tier-0 ルーターに展開されたサービス インスタンスにトラフィックをリダイレクトするルールを設定します。[トラフィックのリダイレクトを設定](#) を参照してください。

トラフィックのリダイレクトを設定

サービス インスタンスの展開後、ルーターからサービスにリダイレクトされるトラフィックのタイプを設定します。トラフィックのリダイレクトの設定は、ファイアウォールの設定と同様です。

ファイアウォールの設定の詳細については、「[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](#)」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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [パートナー サービス] - [サービス インスタンス] の順に選択します。
- 3 サービス インスタンスをクリックします。
- 4 [トラフィックのリダイレクト] タブをクリックします。
- 5 セクションを追加するには、既存のセクションを選択して、[セクションを追加] 追加をクリックします。
 - ◆ メニューから [セクションを上追加] または [セクションを下追加] を追加します。

新しいセクションが作成されます。リダイレクトされるトラフィックのタイプが [L3 リダイレクト] に設定され、サービスのタイプが [ステートレス] になります。[適用先] フィールドは、ホストで設定されている Tier-0 論理ルーターに関連付けられます。ルールを定義すると、[ルール] フィールドが自動的に入力されます。
- 6 [発行] をクリックして、セクションの詳細設定を保持します。
- 7 セクションにルールを追加するには、セクションを選択して [ルールを追加] をクリックします。
- 8 ルール行に、次の情報を入力します。
 - a ルール名を入力します。
 - b L3 トラフィックの送信元と宛先を入力します。パートナー サービス仮想マシンは、宛先の仮想マシンにリダイレクトする前に、送信元から受信したトラフィックのイントロスペクションを行います。
 - c [適用先] フィールドで、Tier-0 ルーターのアップリンクを選択します。
 - d サービス仮想マシンでトラフィックのイントロスペクションが必要な場合は、[アクション] フィールドで [リダイレクト] を選択します。North-South トラフィックのイントロスペクションが必要ない場合は、[リダイレクトしない] を選択します。
- 9 ルールごとに有効にできます。ルールを有効にすると、ルールに一致するトラフィックに適用されます。
- 10 [詳細設定] をクリックしてトラフィックの方向を設定し、ログの作成を有効にします。
- 11 セクションにルールを保持するには、ルールを含むセクションの最後にある [発行] をクリックします。操作をキャンセルする場合は、[元に戻す] をクリックします。

結果

トラフィックがネットワーク イントロスペクション ルールに送信され、ポリシー ルールが適用されます。

次のステップ

[North-South トラフィックへのリダイレクト ルールの追加](#) を参照してください。

North-South トラフィックへのリダイレクト ルールの追加

UI の [ネットワークとセキュリティの詳細設定] を使用して、North-South リダイレクト ルールを設定します。Tier-0 ルーターに挿入されたサービスでのみ、トラフィックのリダイレクトが発生します。

[トラフィックのリダイレクトを設定](#)の手順を実行します。

前提条件

- NSX-T でサードパーティのサービスを登録して、展開します。
- Tier-0 ルーターを設定します。

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 [セキュリティ] - [North South ファイアウォール] - [ネットワーク イントロスペクション (N-S)] - [ポリシーを追加]。

ポリシー セクションは、トラフィック フローの仕組みを決定するルールが定義されるファイアウォール セクションと似ています。
- 3 NSX-T に登録されたサービス インスタンスを [リダイレクト先] に設定し、送信元と宛先のエンティティ間で送受信されるトラフィックのネットワーク イントロスペクションを実行します。
- 4 ポリシーを追加するには、[発行] をクリックします。
- 5 セクションにある垂直方向の省略記号 (⋮) をクリックして、[ルールの追加] をクリックします。
- 6 [送信元] フィールドを編集し、メンバーシップの基準、静的メンバー、IP/MAC アドレス、または Active Directory グループを定義してグループを追加します。メンバーシップの基準は、仮想マシン、論理スイッチ、論理ポート、IP セットのいずれかのタイプから定義できます。静的メンバーは、グループ、セグメント、セグメント ポート、仮想ネットワーク インターフェイス、または仮想マシンのいずれかのカテゴリから選択できます。
- 7 [保存] をクリックします。
- 8 宛先グループを追加するには、[宛先] フィールドを編集します。
- 9 [適用先] フィールドでは、次のいずれかの操作を実行できます。
 - 論理スイッチに接続されているすべての仮想 NIC にルールを適用するには、[DFW] を選択します。
 - グループのメンバー仮想マシンの仮想 NIC にルールを適用するには、[仮想マシン グループ] を選択します。メンバーは、静的リストから選択するか、動的な基準に基づいて選択することができます。サポートされている NSX-T Data Center オブジェクトは、仮想マシン、論理スイッチ、論理ポート、IP セットなどです。

- 10 サービス インスタンスのトラフィックをリダイレクトするには、[アクション] フィールドで [リダイレクト] を選択します。トラフィックにネットワーク イントロスペクションを適用しない場合は、[リダイレクトしない] を選択します。
- 11 [発行] をクリックします。
- 12 発行されたルールを元に戻すには、ルールを選択して [元に戻す] をクリックします。
- 13 ポリシーを追加するには、[+ ポリシーの追加] をクリックします。
- 14 ポリシーまたはルールのクローンを作成するには、ポリシーまたはルールを選択して、[クローン作成] をクリックします。
- 15 ルールを有効にするには、[有効]/[無効] アイコンを有効にするか、ルールを選択して、メニューから [有効] > [ルールの有効化] の順にクリックします。
- 16 ルールを有効または無効にしたら、[発行] をクリックしてルールを適用します。

結果

設定されたアクションに基づいて、North-South トラフィックがサービス インスタンスにリダイレクトされ、ネットワーク イントロスペクションが実行されます。

トラフィックのリダイレクトの監視

サービス インスタンスを展開し、トラフィックのリダイレクトを設定すると、サービス インスタンスで送受信されるトラフィックの量を監視できます。

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 [ネットワークとセキュリティの詳細設定] - [パートナー サービス] - [サービス インスタンス] を選択します。
- 3 サービス インスタンスの名前をクリックします。
[概要] タブに、サービス インスタンスの構成と状態が表示されます。
- 4 [統計情報] タブをクリックします。
サービス インスタンスで送受信されるパケットの数とデータの量に関する情報が表示されます。
- 5 [更新] をクリックし、統計情報を更新します。

エンドポイントの保護

NSX-T Data Center を使用すると、エンドポイント保護サービスを提供する別のサービス仮想マシンとしてサードパーティのパートナー サービスを挿入できます。パートナー サービス仮想マシンは、NSX-T Data Center 管理者によって適用されたエンドポイント保護ポリシー ルールに基づいて、ゲスト仮想マシンのファイル、プロセス、レジストリのイベントを処理します。

エンドポイント保護について

エンドポイント保護のユースケース、ワークフロー、主な概念について説明します。

エンドポイント保護の使用事例

仮想環境では、ゲスト イントロスペクション プラットフォームを使用して、ゲスト仮想マシンにアンチウィルスやアンチマルウェアを提供します。

NSX 管理者は、サービス仮想マシン (SVM) として展開されたアンチウィルス/アンチマルウェア ソリューションを実装し、ゲスト仮想マシンでのファイル アクティビティを監視できます。ファイルを開く場合など、ファイルにアクセスすると、マルウェア対策サービス仮想マシンにこのイベントが通知されます。サービス仮想マシンにより、イベントへの対応方法が決まります。たとえば、ファイルにウィルスの署名があるかどうかを確認します。

- サービス仮想マシンがファイルにはウイルスが含まれていないと判断すると、ファイルを開くことができます。
- サービス仮想マシンがファイル内からウイルスを検出した場合、次のいずれかの方法で対応するように、ゲスト仮想マシンのシン エージェントを要求します。
 - 感染ファイルを削除するか、ファイルへのアクセスを拒否します。
 - 感染した仮想マシンには、NSX でタグを割り当てることができます。さらに、感染が完全に削除されるまでネットワークから隔離して追加のスキャンを行うため、感染した仮想マシンを隔離するセキュリティ グループに、このようなタグ付きゲスト仮想マシンを自動的に移動するルールを定義します。

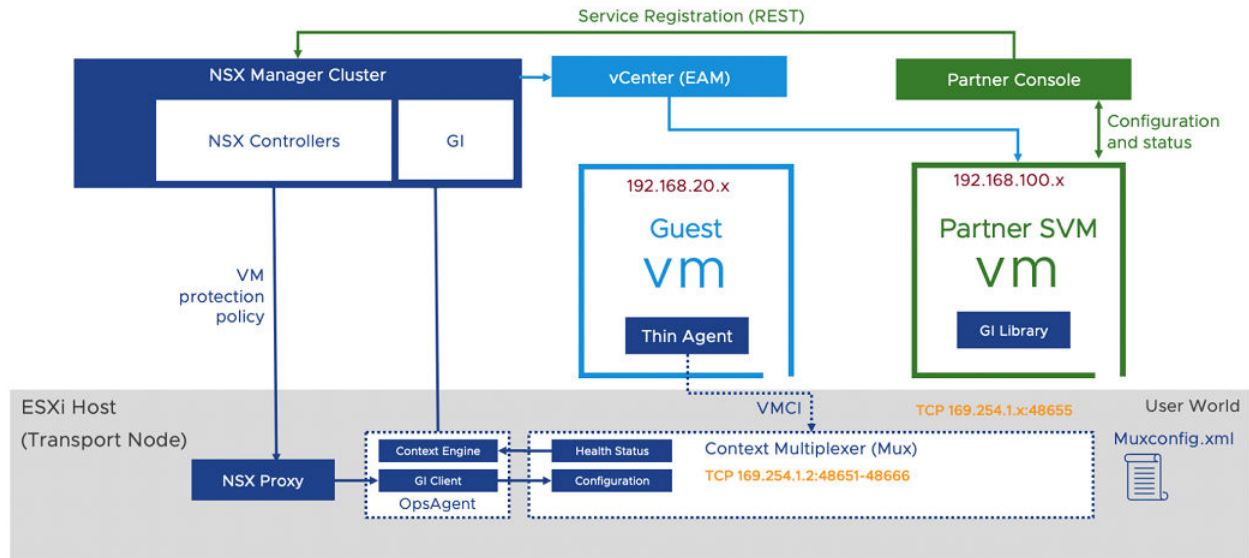
ゲスト イントロスペクション プラットフォームを使用してゲスト仮想マシンのエンドポイントを保護するメリットは次のとおりです。

- コンピューティング リソースの使用量の削減：ゲスト イントロスペクションにより、ホスト上の各エンドポイントからホスト上のサードパーティ パートナー サービス仮想マシンにウィルス シグネチャとセキュリティ スキャン ロジックがオフロードされます。ウイルス スキャンはサービス仮想マシンでのみ実行されます。ウイルス スキャンを実行するために、ゲスト仮想マシンのコンピューティング リソースを消費する必要はありません。
- 管理作業の向上：ウィルス スキャンがサービス仮想マシンにオフロードされるため、ホストごとに1つのオブジェクトのみがウィルスの署名を更新する必要があります。このようなメカニズムは、すべてのゲスト仮想マシンで同じウィルスの署名を更新するエージェント ベースのソリューションよりも優れています。
- アンチウィルスとアンチマルウェアによる継続的な保護；サービス仮想マシンが継続的に実行されるため、ゲスト仮想マシンでの最新ウイルス署名の実施は必須でなくなりました。たとえば、スナップショット仮想マシンで古いバージョンのウイルス署名が実行され、エンドポイントが従来の方法で保護されていると、攻撃を受ける可能性が高くなります。ゲスト イントロスペクション プラットフォームでは、サービス仮想マシンが最新のウィルス署名とマルウェア署名を継続的に取得しているため、新しく追加された仮想マシンも最新のウィルス署名で保護されます。
- サービス仮想マシンにオフロードされたウィルス署名：ウィル データベースのライフサイクルがゲスト仮想マシンのライフサイクルの外にあるため、ゲスト仮想マシンが停止しても、サービス仮想マシンに影響ありません。

ゲスト イントロスペクションのアーキテクチャ

NSX-T Data Center のサービス挿入とゲスト イントロスペクションのコンポーネントのアーキテクチャを理解します。

図 10-1. ゲスト イントロスペクションのアーキテクチャ



用語の説明：

- **パートナー コンソール**：ゲスト イントロスペクション プラットフォームで動作するセキュリティ ベンダーから提供される Web アプリケーションです。
- **NSX Manager**：ユーザーおよびパートナーがネットワークとセキュリティ ポリシーを設定できるように、API とグラフィカル ユーザー インターフェイスを提供する NSX の管理プレーン アプライアンスです。ゲスト イントロスペクションの場合、NSX Manager は、パートナー アプライアンスの展開および管理を行う API と GUI も提供します。
- **ゲスト イントロスペクション SDK**：セキュリティ ベンダーが使用する VMware 提供のライブラリ。
- **サービス仮想マシン**：VMware 提供のゲスト イントロスペクション SDK を使用するセキュリティ ベンダーから提供される仮想マシンです。ファイルまたはプロセス イベントをスキャンして、ゲストに潜むウィルスまたはマルウェアを検出するロジックが含まれています。要求をスキャンした後、要求に対してゲスト仮想マシンが実行したアクションに関する判定結果または通知を戻します。
- **ゲスト イントロスペクション ホスト エージェント (コンテキスト マルチプレクサ)**：エンドポイント保護ポリシーの構成を処理します。また、保護された仮想マシンからサービス仮想マシンにメッセージを多重化して転送します。ゲスト イントロスペクション プラットフォームの健全性状態をレポートし、サービス仮想マシン構成のレコードを muxconfig.xml ファイルに維持します。
- **Ops エージェント (コンテキスト エンジンとゲスト イントロスペクション クライアント)**：ゲスト イントロスペクションの設定をゲスト イントロスペクション ホスト エージェント (コンテキスト マルチプレクサ) に転送します。また、ソリューションの健全性状態を NSX Manager にリレーします。
- **EAM**：NSX Manager は、ESXi Agent Manager を使用して、保護されているクラスター上のすべてのホストにパートナー サービス仮想マシンを展開します。

- シン エージェント：ゲスト仮想マシン内で実行されるファイルまたはネットワーク イントロスペクション エージェントです。ホスト エージェントを介してサービス仮想マシンに転送されるファイルとネットワークのアクティビティをインターセプトします。このエージェントは、VMware Tools の一部です。これは、アンチウィルスまたはアンチマルウェアのセキュリティ ベンダーから提供される従来のエージェントに代わるものです。これは汎用で軽量のエージェントで、ベンダー提供のサービス仮想マシンでスキャンを行うので、ファイルとプロセスのオンボーディングが容易になります。

エンドポイントの保護の主な概念

エンドポイントの保護ワークフローを使用するには、パートナーが自身のサービスを NSX-T Data Center に登録し、管理者がこれらのサービスを使用する必要があります。以下の概念を把握すると、ワークフローの理解に役立ちます。

- サービス定義：パートナーは、名前、説明、サポートされているフォーム ファクタ、ネットワーク インターフェイスを含む展開属性、サービス仮想マシンで使用されるアプライアンス OVF パッケージの場所などの属性を使用してサービスを定義します。
- サービス挿入：NSX では、パートナーがネットワークおよびセキュリティ ソリューションを NSX プラットフォームに統合できるように、サービス挿入フレームワークを用意しています。ゲスト イントロスペクション ソリューションは、このようなサービス挿入形式の 1 つです。
- サービス プロファイルおよびベンダー テンプレート：パートナーは、ポリシーの保護レベルを公開するベンダー テンプレートを登録します。たとえば、保護レベルはゴールド、シルバー、プラチナに設定できます。サービス プロファイルは、ベンダー テンプレートから作成できます。これにより、NSX の管理者は各自のプリファレンスに従ってベンダー テンプレートに名前を設定できます。ゲスト イントロスペクション以外のサービスの場合、サービス プロファイルで属性を使用して、さらにカスタマイズすることができます。その後、サービス プロファイルをエンドポイント保護ポリシー ルールで使用し、NSX で定義されている仮想マシングループの保護を設定できます。管理者は、仮想マシンの名前、タグ、または ID に基づいてグループを作成できます。1 つのベンダー テンプレートから複数のサービス プロファイルを作成することもできます。
- エンドポイント保護ポリシー：ポリシーはルールのコレクションです。複数のポリシーがある場合は、実行順序に合わせて並べ替えます。ポリシー内で定義されるルールも同じです。たとえば、ポリシー A には 3 つのルールがあり、ポリシー B に 4 つのルールがあり、ポリシー B の前にポリシー A が適用されるように並んでいるとします。ゲスト イントロスペクションがポリシーの実行を開始すると、ポリシー B のルールの前にポリシー A のルールが実行されます。
- エンドポイント保護ルール：NSX 管理者は、保護対象の仮想マシン グループを指定するルールを作成し、各ルールにサービス プロファイルを指定して、グループの保護レベルを選択することができます。
- サービス インスタンス：ホスト上のサービス仮想マシンを表します。サービス仮想マシンは、vCenter Server で特別な仮想マシンとして扱われ、すべてのゲスト仮想マシンがパワーオンされる前に起動し、すべてのゲスト仮想マシンがパワーオフした後に停止します。ホストのサービスごとに 1 つのサービス インスタンスがあります。

重要： サービス インスタンスの数は、サービスが実行しているホストの数と同じになります。たとえば、クラスタ内に 8 台のホストがあり、パートナー サービスが 2 つのクラスタに展開されている場合、実行中のサービス インスタンスは合計で 16 台になります。

- サービス展開：Admin は、NSX-T 経由でパートナー サービス仮想マシンをクラスタごとに展開します。展開はクラスタ レベルで管理されるため、ホストがクラスタに追加されると、EAM はサービス仮想マシンを自動的に展開します。

vCenter Server クラスタで分散リソース スケジューラ (DRS) サービスが設定されている場合、サービス仮想マシンを自動的に展開する必要があります。これにより、vCenter Server は、サービス仮想マシンが展開された後にクラスタに追加された新しいホストに既存の仮想マシンを配布または再調整し、新しいホストで開始することができます。パートナー サービス仮想マシンでゲスト仮想マシンを保護するには、NSX-T プラットフォームが必要です。このため、ホストをトランスポート ノードとして準備する必要があります。

重要： 1つのサービス展開は、1つのパートナー サービスを展開および設定するために管理されている vCenter Server の1つのクラスタを表します。

- ファイル イントロスペクション ドライバ：ゲスト仮想マシンにインストールされ、ゲスト仮想マシン上のファイル アクティビティをインターセプトします。
- ネットワーク イントロスペクション ドライバ：ゲスト仮想マシンにインストールされ、ゲスト仮想マシン上のネットワーク トラフィック、プロセス、ユーザー アクティビティをインターセプトします。

エンドポイント保護の手順

ゲスト仮想マシンを保護するセキュリティ スキャン ロジックを含むサードパーティのパートナー サービスは NSX-T Data Center に登録されています。NSX 管理者が登録済みのサービスを展開し、エンドポイント保護ポリシーをゲスト仮想マシン グループに適用すると、パートナー サービスが適用されます。

エンドポイント保護のゲスト イントロスペクション ワークフローは次のとおりです。

図 10-2. エンドポイント保護ワークフロー

ワークフロー タスク	ロール/個人	実装方法
サービスの NSX-T Data Center への登録	パートナーの管理者	パートナー コンソール
サービスの NSX-T Data Center への登録	パートナーの管理者	パートナー コンソール
サービスの NSX-T Data Center への登録	パートナーの管理者	パートナー コンソール
サービスの展開	NSX 管理者	API および NSX Manager UI
サービス インスタンスの詳細の表示	NSX 管理者	API および NSX Manager UI
サービス インスタンスの起動	NSX 管理者	API および NSX Manager UI
サービス プロファイルの追加	NSX 管理者	API および NSX Manager UI
ゲスト イントロスペクション ポリシーの使用	NSX 管理者	API および NSX Manager UI
エンドポイント保護ルールの追加および発行	NSX 管理者	API および NSX Manager UI
エンドポイント保護状態のモニタリング	NSX 管理者	API および NSX Manager UI

エンドポイントの保護の設定

サードパーティ パートナーのセキュリティ サービスを使用して、NSX-T Data Center 環境で実行されているゲスト仮想マシンを保護します。

エンドポイント保護ポリシーを設定するためのおおまかな手順は、次のとおりです。

- 1 ゲスト仮想マシンでエンドポイント保護を設定する前に、[エンドポイント保護を設定するための前提条件](#)の要件を満たしていることを確認します。
- 2 サポート対象のソフトウェア。[サポート対象のソフトウェア](#) を参照してください。
- 3 Linux 仮想マシンのファイル イントロスペクション ドライバをインストールします。[Linux 仮想マシンへのゲスト イントロスペクション シン エージェントのインストール](#) を参照してください。
- 4 Windows 仮想マシンのファイル イントロスペクション ドライバをインストールします。[Linux 仮想マシンへのゲスト イントロスペクション シン エージェントのインストール](#) を参照してください。
- 5 Linux 仮想マシンのネットワーク イントロスペクション ドライバをインストールします。[ネットワーク イントロスペクション用の Linux シン エージェントのインストール](#) を参照してください。
- 6 ゲスト イントロスペクション パートナーの管理者ロールを持つユーザーを作成します。[ゲスト イントロスペクション パートナーの管理者ロールを持つユーザーの作成](#) を参照してください。
- 7 パートナー サービスを NSX-T Data Center に登録します。パートナーのドキュメントを参照してください。
- 8 サービスを展開します。[サービスの展開](#) を参照してください。
- 9 ゲスト イントロスペクション ポリシーを使用します。[ゲスト イントロスペクション ポリシーの使用](#) を参照してください。
- 10 エンドポイント保護ルールを追加して発行します。[エンドポイント保護ルールの追加および発行](#) を参照してください。
- 11 エンドポイント保護ルールをモニタリングします。[エンドポイント保護状態のモニタリング](#) を参照してください。

エンドポイント保護を設定するための前提条件

ゲスト仮想マシンのエンドポイント保護を設定する前に、前提条件を満たしていることを確認します。

前提条件

- すべてのホストに NSX Manager がインストールされていること。
- トランスポート ノード プロファイルを適用して、トランスポート ノードとして NSX-T Data Center クラスターを準備し、設定します。ホストをトランスポート ノードとして設定した後に、ゲスト イントロスペクション コンポーネントがインストールされていること。『NSX-T Data Center インストール ガイド』を参照してください。
- パートナー コンソールがインストールされ、サービスを NSX-T Data Center で登録するように設定されていること。
- ゲスト仮想マシンで仮想マシン ハードウェア構成ファイル バージョン 9 以降が実行されていることを確認します。
- VMware Tools を設定し、シン エージェントをインストールします。
 - [Linux 仮想マシンへのゲスト イントロスペクション シン エージェントのインストール](#) を参照してください。

- [Windows 仮想マシンへのゲスト イントロスペクション シン エージェントのインストール](#) を参照してください。
- [ネットワーク イントロスペクション用の Linux シン エージェントのインストール](#) を参照してください。

Linux 仮想マシンへのゲスト イントロスペクション シン エージェントのインストール

ゲスト イントロスペクションはアンチウイルスのみを目的として、Linux でファイル イントロスペクションをサポートします。ゲスト イントロスペクションのセキュリティ ソリューションを使用して Linux 仮想マシンを保護するには、ゲスト イントロスペクション シン エージェントをインストールする必要があります。

Linux シン エージェントは、オペレーティング システム固有パッケージ (OSP) の一部として使用できます。パッケージは、VMware パッケージ ポータルにホストされます。Enterprise Administrator または Security Administrator (NSX Administrator ではない) は、NSX の外にあるゲスト仮想マシンに、このエージェントをインストールすることもできます。

VMware Tools をインストールする必要はありません。

使用する Linux オペレーティング システムに基づいて、次の手順を root 権限で実行します。

前提条件

- ゲスト仮想マシンにサポートされているバージョンの Linux がインストールされていることを確認してください。
 - Red Hat Enterprise Linux (RHEL) 7.4 (64 ビット) GA
 - SUSE Linux Enterprise Server (SLES) 12 (64 ビット) GA
 - Ubuntu 16.04.5 LTS (64 ビット) GA
 - CentOS 7.4 GA
- Linux 仮想マシンに GLib 2.0 がインストールされていることを確認します。

手順

1 Ubuntu システムの場合

- 次のコマンドを使用して、VMware パッケージ パブリック キーを取得しインポートします。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- vmware.list という名前の新しいファイルを /etc/apt/sources.list.d の下に作成します。
- そのファイルを次の内容で編集します。

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- このパッケージをインストールします。

```
apt-get update
apt-get install vmware-nsx-gi-file
```

2 RHEL7 システムの場合

- a 次のコマンドを使用して、VMware パッケージ パブリック キーを取得しインポートします。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b `vmware.repo` という名前の新しいファイルを `/etc/yum.repos.d` の下に作成します。
- c そのファイルを次の内容で編集します。

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

3 このパッケージをインストールします。

```
yum install vmware-nsx-gi-file
```

4 SLES システムの場合

- a 次のコマンドを使用して、VMware パッケージ パブリック キーを取得しインポートします。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 次のリポジトリを追加します。

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c このパッケージをインストールします。

```
zypper install vmware-nsx-gi-file
```

5 CentOS システムの場合

- a 次のコマンドを使用して、VMware パッケージ パブリック キーを取得しインポートします。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b `vmware.repo` という名前の新しいファイルを `/etc/yum.repos.d` の下に作成します。

- c そのファイルを次の内容で編集します。

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

次のステップ

管理者権限を持つユーザーでログインし、`service vsespd status` コマンドを使って、シン エージェントが実行されているかどうかを確認します。実行されている場合、状態は「running」になります。

ネットワーク イントロスペクション用の Linux シン エージェントのインストール

ネットワーク トラフィックのイントロスペクションを行う Linux シン エージェントをインストールします。

重要： ゲスト仮想マシンをアンチウイルスから保護するため、ネットワーク イントロスペクション用に Linux シン エージェントをインストールする必要はありません。

ネットワーク トラフィックのイントロスペクションに使用する Linux シン エージェント ドライバは、オープンソース ドライバに依存します。

前提条件

次のパッケージをインストールします。

- glib2
- libnetfilter-contrack3/ libnetfilter-contrack
- libnetfilter-queue1/ libnetfilter-queue
- iptables

手順

1 ゲスト イントロスペクションによって提供されるオープンソース ドライバをインストールします。

- a オペレーティング システムのベース URL として次の URL を追加します。

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

- b VMware パッケージ キーをインポートします。

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c リポジトリを更新し、オープンソース ドライバをインストールします。

```
apt-get install Guest-Introspection-for-VMware-NSX
```

2 ファイルやネットワーク トラフィックのイントロスペクションに使用される Linux シン エージェントをインストールします。

- ファイルとネットワークのイントロスペクション パッケージをインストールするには、手順 c で `vmware-nsx-gi` パッケージを選択します。
- ネットワーク イントロスペクション パッケージをインストールするには、手順 c で `vmware-nsx-gi-net` パッケージを選択します。
- a オペレーティング システムのベース URL として次の URL を追加します。

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

- b VMware パッケージ キーをインポートします。

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c いずれかのドライバをインストールします。

```
vmware-nsx-gi
vmware-nsx-gi-net
```

Windows 仮想マシンへのゲスト イントロスペクション シン エージェントのインストール

ゲスト イントロスペクションのセキュリティ ソリューションを使用して仮想マシンを保護するには、仮想マシンにゲスト イントロスペクション シン エージェント（ゲスト イントロスペクション ドライバともいいます）をインストールする必要があります。ゲスト イントロスペクション ドライバは、VMware Tools for Windows に含まれていますが、デフォルトではインストールされません。Windows 仮想マシンにゲスト イントロスペクションをインストールするには、カスタム インストールを実行し、ドライバを選択する必要があります。

ゲスト イントロスペクション ドライバがインストールされた Windows 仮想マシンは、セキュリティ ソリューションがインストールされた ESXi ホストで起動されると自動的に保護されます。保護対象の仮想マシンは、シャットダウンから再起動の間や、vMotion がセキュリティ ソリューションのインストールされた別の ESXi に移動した後でも、常に保護された状態が維持されます

- vSphere 6.0 を使用している場合は、VMware Tools をインストールします。手順については、[Windows 仮想マシンへの VMware Tools の手動インストールまたはアップグレード](#)を参照してください。
- vSphere 6.5 を使用している場合は、<https://www.vmware.com/support/pubs/vmware-tools-pubs.html> で VMware Tools のインストール手順を確認してください。

前提条件

ゲスト仮想マシンにはサポートされているバージョンの Windows がインストールされていることを確認してください。NSX のゲスト イントロスペクションでは、次の Windows オペレーティング システムがサポートされています。

- Windows XP SP3 以降 (32 ビット)
- Windows Vista (32 ビット)
- Windows 7 (32 ビットまたは 64 ビット)
- Windows 8 (32 ビットまたは 64 ビット)
- Windows 8.1 (32 ビットまたは 64 ビット) (vSphere 6.0 以降)
- Windows 10
- Windows 2003 SP2 以降 (32 ビットまたは 64 ビット)
- Windows 2003 R2 (32 ビットまたは 64 ビット)
- Windows 2008 (32 ビットまたは 64 ビット)
- Windows 2008 R2 (64 ビット)
- Windows 2012 (64 ビット)
- Windows 2012 R2 (64 ビット) (vSphere 6.0 以降)
- Windows Server 2016
- Windows Server 2019

手順

- 1 vSphere のバージョンの手順に従って、VMware Tools のインストールを開始します。[カスタム インストール] を選択します。
- 2 VMCI ドライバ セクションを展開します。

使用可能なオプションは、VMware Tools のバージョンによって異なります。

3 仮想マシンにインストールするドライバを選択します。

ドライバ	説明
vShield Endpoint ドライバ	ファイル イントロスペクション (vsepflt) とネットワーク イントロスペクション (vnetflt) のドライバをインストールします。
ゲスト イントロスペクション ドライバ	ファイル イントロスペクション (vsepflt) とネットワーク イントロスペクション (vnetflt) のドライバをインストールします。
NSX ファイル イントロスペクション ドライバと NSX ネットワーク イントロスペクション ドライバ	NSX ファイル イントロスペクション ドライバを選択して Vsepflt をインストールします。 必要に応じて、NSX ネットワーク イントロスペクション ドライバを選択して vnetflt (Windows 10 以降の場合は vnetWFP) をインストールします。 注： NSX ネットワーク イントロスペクション ドライバは、Identity Firewall またはエンドポイントの監視機能を使用している場合にのみ選択します。

4 追加するドライバの横にあるドロップ ダウン メニューで、[この機能はローカル ハード ドライブにインストールされます] を選択します。

5 残りの手順に従います。

次のステップ

管理者権限を持つユーザーでログインし、fltmc コマンドを使って、シン エージェントが実行されているかどうかを確認します。出力の [フィルタ名] 列に、該当するシン エージェントとともに、エントリ vsepflt が表示されます。

サポート対象のソフトウェア

ゲスト イントロスペクションは、特定のバージョンのソフトウェアと相互運用できます。

VMware Tools

VMware Tools バージョン 10.3.10 がサポートされています。

VMware Tools と NSX-T の相互運用性を確認します。[VMware 製品の相互運用性マトリックス](#)を参照してください。

サポートされる OS

- Windows 7
- Windows 8、8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server
- CentOS 7.4 GA
- RHEL 7.4 GA

- Ubuntu 16.04.5 LTS (64 ビット)
- SLES 12 GA

サポート対象のホスト

サポート対象の ESXi ホストについては、[VMware 製品互換性マトリクス](#)を参照してください。

ゲスト イントロスペクション パートナーの管理者ロールを持つユーザーの作成

NSX-T Data Center で使用可能なゲスト イントロスペクション パートナーの管理者ロールをユーザーに割り当てます。

注：セキュリティ上の問題を回避するため、ゲスト イントロスペクション パートナーの管理者ロールに関連付けられているユーザーがパートナー サービスの登録を行うことをおすすめします。

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 [システム] → [ユーザー] → [ロールの割り当て] の順に選択します。
- 3 [追加] をクリックします。
- 4 ユーザーを選択して、そのユーザーに、**GI パートナー管理者** ロールを割り当てます。

次のステップ

サービスを NSX-T Data Center に登録します。[サービスの NSX-T Data Center への登録](#) を参照してください。

サービスの NSX-T Data Center への登録

サードパーティのセキュリティ サービスを NSX-T Data Center に登録します。

前提条件

- 前提条件を満たしていることを確認します。[エンドポイント保護を設定するための前提条件](#) を参照してください。
- vIDM ユーザーに GI パートナーの管理者ロールが割り当てられていることを確認します。このロールは、サービスを NSX-T Data Center に登録するために使用されます。

手順

- 1 GI パートナー管理者の権限でパートナー コンソールにログインします。
- 2 サービス、ベンダー テンプレートを登録して、パートナー ソリューションを NSX-T Data Center で設定します。パートナーのドキュメントを参照してください。

次のステップ

パートナー サービスのカタログを表示します。[パートナー サービスのカタログの表示](#) を参照してください。

パートナー サービスのカタログの表示

カタログ画面には、NSX-T Data Center に登録されているすべてのパートナー、およびこれらのサービスが表示されます。

前提条件

- パートナーが、NSX-T Data Center にサービスを登録していること。
- サービスがクラスタに展開されていること。

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 [システム] - [サービス展開] - [カタログ] を選択します。
- 3 サービスの [表示] をクリックします。[展開] 画面に、展開の状態、ネットワークの詳細、クラスタの詳細など、サービスに関する詳細が表示されます。

次のステップ

パートナー サービス仮想マシンをアップグレードします。

サービスの展開

サービスを登録した後、サービスがネットワーク トラフィックの処理を開始できるように、サービスのインスタンスを展開する必要があります。

クラスタ内のすべての NSX-T Data Center ホストに、パートナー セキュリティ エンジンを実行するパートナー サービス仮想マシンを展開します。vSphere ESX Agency Manager (EAM) サービスは、各ホストにパートナー サービス仮想マシンを展開する際に使用されます。サービス仮想マシンを展開したら、ここで使用するポリシー ルールを作成して、ゲスト仮想マシンを保護することができます。

前提条件

- すべてのホストが、vCenter Server によって管理されていること。
- パートナー サービスは NSX-T Data Center に登録されていて、展開する準備ができていること。
- NSX-T Data Center 管理者が、パートナー サービスおよびベンダー テンプレートにアクセスできること
- サービス仮想マシンとパートナーの Service Manager (コンソール) の両方が、管理ネットワーク レベルで相互に通信できること。
- 以下のように、ホストを NSX-T Data Center トランスポート ノードとして準備すること。
 - トランスポート ゾーンを作成します。
 - トンネル エンドポイントの IP アドレス用の IP アドレス プールを作成します。
 - アップリンク プロファイルを作成します。
 - トランスポート ノード プロファイルを追加し、NSX-T Data Center トランスポート ノードの自動展開用クラスタを準備します。
 - スタンドアローン ホストまたは管理対象ホストを構成します。

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 [システム] タブに移動して、[サービスの展開] をクリックします。
- 3 [パートナー サービス] ドロップダウンから、展開するサービスを選択します。
- 4 [展開] をクリックして、[サービスの展開] をクリックします。
- 5 サービスの展開名を入力します。
- 6 [コンピュート マネージャ] フィールドで、サービスを展開する vCenter Server のコンピューティング リソースを選択します。
- 7 [クラスタ] フィールドで、サービスを展開する必要があるクラスタを選択します。
- 8 [データストア] ドロップダウン メニューで、次の操作を実行できます。
 - a サービス仮想マシンのリポジトリとしてデータストアを選択します。
 - b [ホストに指定] を選択します。この設定が有効な場合は、このウィザードでデータストアおよびポート グループを選択する必要はありません。vCenter Server で EAM のエージェントを直接設定して、サービス展開に使用する特定のデータストアおよびポート グループをポイントするように指定することができます。

EAM の構成方法について確認するには、vSphere のドキュメントを参照してください。
- 9 [ネットワーク] 列で [設定] をクリックします。
- 10 管理ネットワーク インターフェイスを [ホストに指定] または [DVPG] に設定します。
- 11 ネットワーク タイプを DHCP または固定 IP プールに設定します。ネットワーク タイプを固定 IP プールに設定した場合は、使用可能な IP プールのリストから選択します。
- 12 [展開の仕様] フィールドで、ホストベースの展開を選択して、すべてのホストにサービスを展開します。パートナーによって登録されたサービスに応じて、複数のサービスを単一のサービス仮想マシンの一部として展開できます。
- 13 [展開テンプレート] フィールドで、登録されている展開テンプレートを選択します。
- 14 [保存] をクリックします。

結果

新しいホストがクラスタに追加されると、EAM は新しいホストにサービス仮想マシンを自動的に展開します。展開プロセスは、ベンダーの実装によって時間がかかることがあります。NSX Manager ユーザー インターフェイスに状態を表示できます。状態が **展開に成功** に変わった場合は、サービスがホストに正常に展開されています。

クラスタからホストを削除するには、まずクラスタをメンテナンス モードにします。次に、ゲスト仮想マシンを別のホストに移行するオプションを選択し、移行を完了します。

次のステップ

ホストに展開されたサービス インスタンスに関する展開の詳細および健全性の状態を確認します。[サービス インスタンスの詳細の表示](#) を参照してください。

サービス インスタンスの詳細の表示

クラスタのメンバー ホストに展開されたサービス インスタンスに関する展開の詳細および健全性の状態を確認します。

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 [システム] - [サービス展開] - [サービス インスタンス] を選択します。
- 3 [パートナー サービス] ドロップダウン メニューからパートナー サービスを選択して、サービス インスタンスに関連する詳細を表示します。

表 10-9.

フィールド	説明
サービス インスタンス名	特定のホストのサービス インスタンスを識別する一意の ID。
サービス展開名	サービスの展開時に入力した名前。
展開先	ホスト IP アドレスまたは FQDN
展開モード	クラスタまたはスタンドアローン
展開状態	成功した展開を判別する稼働中の状態
健全性状態	<p>サービス インスタンスが展開されると、健全性の状態は Ready になります。健全性の状態を 状態 Ready から Up にするには、必要な設定変更を行います。サービス インスタンスの起動 を参照してください。</p> <p>NSX-T Data Center によって次のパラメータが正常に認識されると、健全性の状態が Ready から Up に変わります。</p> <ul style="list-style-type: none"> ■ ソリューションの状態：稼働中 ■ NSX-T Data Center Guest Introspection Agent と NSX-T Data Center Ops Agent 間の接続：稼働中 ■ 健全性の状態を受信した日時：<日、日付、時間>

次のステップ

サービス インスタンスを起動します。[サービス インスタンスの起動](#) を参照してください。

サービス インスタンスの起動

サービス インスタンスを展開した後、健全性の状態を稼働中にするには、NSX-T Data Center で特定のパラメータを更新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>>) に管理者権限でログインします。
- 2 [システム] - [サービス展開] - [サービス インスタンス] を選択します。

- 3 [パートナー サービス] ドロップダウン メニューからパートナー サービスを選択して、サービス インスタンスに関連する詳細を表示します。
- 4 [健全性ステータス] 列で、サービス インスタンスの状態が Ready と表示されます。これは、サービス インスタンスがエンドポイント保護ポリシー ルールを使用して設定され、仮想マシンを保護する準備ができていることを示します。
- 5 健全性の状態を Up にするには、NSX-T Data Center で次のパラメータを更新する必要があります。
 - ゲスト仮想マシンをホストで使用可能にする。
 - ゲスト仮想マシンをパワーオンする。
 - エンドポイント保護ルールをゲスト仮想マシンに適用する。
 - サポートされているバージョンの VMware Tools とファイル イントロスペクション ドライバを使用して、ゲスト仮想マシンを設定する。

次のステップ

サービス プロファイルを追加します。[サービス プロファイルの追加](#) を参照してください。

サービス プロファイルの追加

ゲスト イントロスペクション ポリシーを実装できるのは、NSX-T Data Center でサービス プロファイルが使用可能な場合のみです。サービス プロファイルは、パートナーにより提供されるテンプレートから作成されます。サービス プロファイルを使用すると、管理者は、ベンダーから提供されたベンダー テンプレートを選択することにより、仮想マシンの保護レベル（ゴールド、シルバー、プラチナ ポリシー）を選択することができます。

たとえば、ベンダーはゴールド、プラチナ、およびシルバーのポリシー レベルを提供できます。作成されたプロファイルは、それぞれ異なるタイプのワークロードを処理できます。ゴールド サービス プロファイルは、PCI タイプのワークロードに対して完全なマルウェア対策を行います。シルバー サービス プロファイルは、通常のワークロードに対して基本的なマルウェア対策の保護のみを行います。

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 [セキュリティ] - [エンドポイントの保護] - [エンドポイント保護ルール] - [サービス プロファイル] を選択します。
- 3 [パートナー サービス] フィールドで、サービス プロファイルを作成するサービスを選択します。
- 4 [サービス プロファイルの追加] をクリックします。
- 5 サービス プロファイル名を入力し、ベンダー テンプレートを選択します。必要に応じて、説明およびタグを追加します。
- 6 [保存] をクリックします。

サービス プロファイルを作成するために使用するベンダー テンプレート ID がパートナーのコンソールに渡されます。パートナーはベンダー テンプレート ID を保存して、これらのベンダー テンプレートによって保護されるゲスト仮想マシンの使用量を追跡します。

結果

サービス プロファイルを作成した後に、NSX 管理者は仮想マシンのグループにサービス プロファイルに関連付けるためのルールを作成し、その後でポリシー ルールを発行します。

次のステップ

マルウェアから保護する必要があるゲスト仮想マシン グループに、エンドポイント保護ポリシーを適用します。[ゲスト イントロスペクション ポリシーの使用](#) を参照してください。

ゲスト イントロスペクション ポリシーの使用

仮想マシン グループにポリシーを適用するには、サービス プロファイルを仮想マシン グループに関連付けるルールを作成します。ルールが仮想マシン グループに適用されるとすぐに、保護が開始します。

エンドポイント保護ポリシーとは、ゲスト仮想マシンにサービス プロファイルを実装することによってマルウェアからゲスト仮想マシンを保護する、パートナー提供の保護サービスのことです。仮想マシン グループにルールが適用されている場合は、このグループ内のすべてのゲスト仮想マシンがこのサービス プロファイルによって保護されます。ゲスト仮想マシンでファイル アクセス イベントが発生すると、各ゲスト仮想マシンで実行中の GI シン エージェントは、ファイルのコンテキスト（ファイルの属性、ファイルのハンドル、その他のコンテキスト詳細など）を収集して、このイベントをサービス仮想マシンに通知します。サービス仮想マシンがファイルの内容をスキャンする場合は、EPsec API ライブラリを使用して詳細を要求します。サービス仮想マシンで問題なしと判断された場合、GI シン エージェントはユーザーにファイルへのアクセスを許可します。サービス仮想マシンからファイルの感染が報告された場合、GI シン エージェントは、ユーザーに対してこのファイルへのアクセスを禁止します。

仮想マシン グループにセキュリティ サービスを実行するには、次の操作を実行する必要があります。

手順

- 1 ポリシーとルールを定義します。
- 2 仮想マシン グループを構成するためのメンバーシップの基準を定義します。
- 3 仮想マシン グループのルールを定義します。
- 4 ルールを発行します。

エンドポイント保護ルールの追加および発行

仮想マシン グループにポリシー ルールを発行すると、保護する必要がある仮想マシン グループが特定のサービス プロファイルに関連付けられます。

手順

- 1 ポリシー セクションでポリシーを選択します。
- 2 [追加] -> [ルールの追加] の順にクリックします。
- 3 新しいルールでルール名を入力します。
- 4 [グループの選択] フィールドで編集アイコンをクリックします。

- 5 [グループの設定] 画面で、既存のグループのリストから選択するか、新しいグループを追加します。
 - a 新しいグループを追加するには、[グループの追加] をクリックし、詳細を入力して [保存] をクリックします。
[グループの追加](#) を参照してください。
- 6 [グループ] 列で仮想マシン グループを選択します。
- 7 [サービス プロファイル] 列で、グループ内のゲスト仮想マシンに目的の保護レベルを提供するサービス プロファイルを選択します。
 - a 新しいサービス プロファイルを追加するには、[サービス プロファイルの追加] をクリックし、詳細を入力して [保存] をクリックします。
[サービス プロファイルの追加](#) を参照してください。
- 8 [発行] をクリックします。

結果

エンドポイント保護ポリシーは仮想マシン グループを保護します。

次のステップ

別の仮想マシン グループに必要な保護のタイプに応じて、ルールの順序を変更することができます。[ゲスト イントロスペクションでエンドポイント保護ポリシーを実行する方法](#) を参照してください。

エンドポイント保護状態のモニタリング

保護されている仮想マシンと保護されていない仮想マシンの設定状態をモニタリングします。ホスト エージェントとサービス仮想マシンの問題、VMware Tools と一緒にインストールされたファイル イントロスペクション ドライバで設定されている仮想マシンをモニタリングします。

次のものを確認できます。

- サービス展開状態
- エンドポイント保護の設定状態
- エンドポイント保護に設定したキャパシティ状態

サービス展開の状態の表示

モニタリング ダッシュボードにサービス展開の詳細を表示します。

EPP ポリシーのシステム全体の状態を表示します。

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 [ホーム] > [モニタリング - ダッシュボード] に移動します。
- 3 ドロップダウン メニューから [モニタリング - システム] をクリックします。

- 4 システムのクラスタ間の展開状態を表示するには、エンドポイント保護ウィジェットに移動し、ドーナツ チャートをクリックして展開の成功または失敗を確認します。

[サービス展開] ページに展開の状態が表示されます。

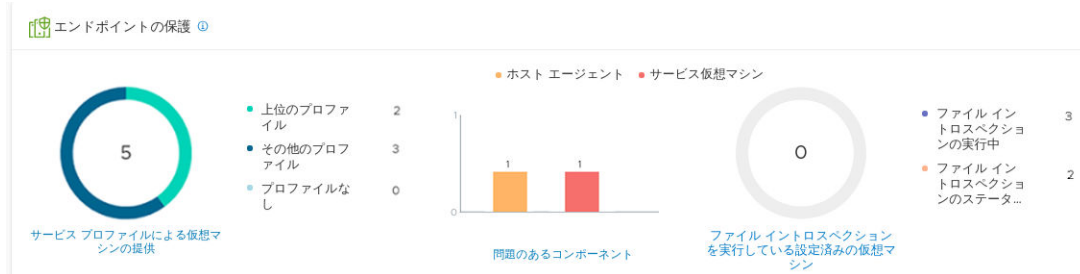
エンドポイント保護の設定状態の表示

エンドポイント保護サービスの設定状態を表示します。

EPP ポリシーのシステム全体の状態を表示します。

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 [ホーム] > [セキュリティ] > [セキュリティの概要] の順に移動します。
- 3 クラスタ上の EPP の状態を表示するには、[セキュリティ] ウィジェットをクリックします。
- 4 [セキュリティの概要] ページで、[設定] をクリックします。



- 5 [エンドポイント保護] セクションで、次を表示します。

- a [サービス プロファイルによる仮想マシンの提供] ウィジェットには、次の情報が表示されます。

- 1 上位のプロファイルで保護されている仮想マシンの数。上位のプロファイルは、クラスタで最大数の仮想マシンを保護しているプロファイルです。
- 2 残りのサービス プロファイルで保護されている仮想マシンは、[その他のプロファイル] に分類されます。
- 3 保護されていない仮想マシンは [プロファイルなし] に分類されます。

[エンドポイント保護ルール] ページには、エンドポイント保護ポリシーで保護されている仮想マシンが表示されます。

- b [問題のあるコンポーネント] ウィジェットには次の情報が表示されます。

- 1 ホスト：コンテキスト マルチプレクサに関連する問題。
- 2 SVM：サービス仮想マシンに関連する問題。たとえば、SVM の状態が「停止」で、ゲスト仮想マシンとの SVM 接続が停止しているとします。

[展開] ページの [状態] 列に、健全性の問題が表示されます。

- c [ファイル イントロスペクションを実行している構成済みの仮想マシン] ウィジェットには次の情報が表示されます。

- 1 ファイル イントロスペクション ドライバで保護されている仮想マシン。
- 2 ファイル イントロスペクション ドライバの状態が仮想マシン。

ESXi Agency Manager (EAM) は、ホスト、SVM、構成エラーに関連するいくつかの問題の解決を試みます。[パートナー サービスの問題の解決](#) を参照してください。

エンドポイント保護に設定したキャパシティ状態の表示

エンドポイント保護サービスのキャパシティ状態を表示します。

EPP ポリシーのキャパシティ状態を表示します。

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 [ホーム] > [モニタリング - ダッシュボード] に移動します。
- 3 ドロップダウン メニューから [モニタリング - ネットワークとセキュリティ] をクリックします。
- 4 クラスタ上の EPP の状態を表示するには、[セキュリティ] ウィジェットをクリックします。
- 5 [セキュリティの概要] ページで、[キャパシティ] をクリックし、これらのパラメータのキャパシティ状態を表示します。

制限	最大キャパシティ	現在のインベントリ (総数済み)	警告アラート	重大アラート
分散ファイアウォール ルール	100,000	2	0%	70% 100%
システム規模のファイアウォール セクション	10,000	5	0.05%	70% 100%

- a [システム全体のエンドポイント保護が有効になっているホスト]：保護されたホストの数がしきい値に達すると、NSX Manager は対応するしきい値制限に達したときに警告アラートまたはクリティカル アラートを通知します。
- b [システム全体のエンドポイント保護が有効になっている仮想マシン]：保護された仮想マシンの数がしきい値に達すると、NSX Manager は対応するしきい値制限に達したときに警告アラートまたはクリティカル アラートを通知します。

注： これらのパラメータのしきい値の制限を設定すると、これらのパラメータが設定したしきい値に達したときにアラートを受け取り、状態を確認することができます。

エンドポイント保護の管理

ポリシーの競合やサービス仮想マシンの健全性の問題を解決し、エンドポイント保護ポリシーの機能を確認します。

パートナー サービスの問題の解決

パートナー サービス仮想マシンが機能していない場合、ゲスト仮想マシンはマルウェアから保護されません。

各ホストで、次のサービスまたはプロセスが稼動中であり、実行されていることを確認します。

- ESXi Agency Manager (EAM) サービスが稼動中であり、実行している必要があります。次の URL にアクセスできる必要があります。

```
https://<vCenter_Server_IP_Address>/eam/mob
```

ESXi Agency Manager がオンラインであることを確認します。

```
root> service-control --status vmware-eam
```

- サービス仮想マシンがゲスト仮想マシンを保護できるように、サービス仮想マシンのポートグループを削除しないでください。

```
https://<vCenter_Server_IP_Address>/ui
```

- vCenter Server で仮想マシンに移動して、[ネットワーク] タブをクリックして、[vmervice-vshield-pg] が表示されているかどうかを確認します。
- Context Multiplexer (MUX) サービスが稼動中であり、実行している必要があります。 nsx-context-mux VIB がホストが稼動中であり、実行していることを確認します。
- NSX-T Data Center がパートナー サービス コンソールとの通信に使用する管理インターフェイスが稼動している必要があります。
- MUX とサービス仮想マシン間の通信を可能にする制御インターフェイスが稼動している必要があります。MUX とサービス仮想マシンを接続するポート グループを作成する必要があります。パートナー サービスを使用するには、このインターフェイスとポート グループの両方が必要です。

ESXi Agency Manager に関する問題

表では、NSX Manager ユーザー インターフェイスの [解決] ボタンを使用して解決できる ESXi Agency Manager の問題が示されています。また、NSX Manager とエラーの詳細が示されています。

表 10-10. ESXi Agency Manager に関する問題

問題	カテゴリ	説明	解決方法
エージェント OVF にアクセスできない	仮想マシンが展開されない	エージェント仮想マシンがホストに展開されることが期待されたにも関わらず、ESXi Agent Manager がエージェントの OVF パッケージにアクセスできないため、エージェント仮想マシンを展開できません。この問題は、OVF パッケージを提供する Web サーバが停止している場合に発生することがあります。この Web サーバは通常、エージェントを作成したソリューションの内部に配置されます。	ESXi Agency Manager (EAM) サービスによって、OVF のダウンロード操作が再試行されます。パートナー管理コンソールの状態を確認します。[[解決] をクリックします。

表 10-10. ESXi Agency Manager に関する問題（続き）

ホストのバージョンに互換性が ない	仮想マシンが展開されない	エージェント仮想マシンがホストに展開されている必要があります。ただし、互換性の問題のため、エージェントがホストに展開されていません。	エージェントとホストとの互換性を確保するため、ホストまたはソリューションをアップグレードしてください。サービス仮想マシンの互換性を確認します。[] [解決] をクリックします。
リソース不足	仮想マシンが展開されない	エージェント仮想マシンがホストに展開されている必要があります。ただし、ホストの CPU またはメモリ リソースが少ないため、ESXi Agency Manager (EAM) サービスはエージェント仮想マシンを展開しませんでした。	ESXi Agency Manager (EAM) サービスは、仮想マシンの再展開を試みます。CPU とメモリ リソースが使用可能であることを確認します。ホストを確認して、一部のリソースを解放します。[] [解決] をクリックします。
容量不足	仮想マシンが展開されない	エージェント仮想マシンがホストに展開されている必要があります。ただし、ホストのエージェント データストアに十分な空き容量がないため、エージェント仮想マシンは展開されませんでした。	ESXi Agency Manager (EAM) サービスは、仮想マシンの再展開を試みます。データストアの領域を解放します。[] [解決] をクリックします。
エージェント仮想マシン ネットワークがない	仮想マシンが展開されない	エージェント仮想マシンがホストに展開されることが期待されたにも関わらず、ホストにエージェント ネットワークが設定されていなかったため、エージェントを展開できません。	customAgentVmNetwork に一覧表示されているネットワークの 1 つをホストに追加します。この問題は、データストアが使用可能になった後に自動的に解決されます。
OVF 形式が無効	仮想マシンが展開されない	エージェント仮想マシンがホストでプロビジョニングされることが期待されたにも関わらず、OVF パッケージのプロビジョニングに失敗したため、プロビジョニングできません。OVF パッケージを提供するソリューションがアップグレードされるか、パッチが適用されて、エージェント仮想マシンに有効な OVF パッケージが提供されるようになるまで、プロビジョニングが成功する確率は低くなります。	ESXi Agency Manager (EAM) サービスは、サービス仮想マシンの再展開を試みます。パートナー ソリューションのドキュメントを確認するか、パートナー ソリューションをアップグレードして有効な OVF パッケージ入手します。[] [解決] をクリックします。
エージェント IP アドレス プールが見つからない	仮想マシンがパワーオフ状態	エージェント仮想マシンがパワーオンすることが期待されたにも関わらず、エージェントの仮想マシン ネットワーク上に定義された IP アドレスがないため、エージェント仮想マシンがパワーオフされました。	仮想マシン ネットワークの IP アドレスを定義します。[] [解決] をクリックします。

表 10-10. ESXi Agency Manager に関する問題（続き）

エージェント仮想マシン データストアがない	仮想マシンがパワーオフ状態	エージェント仮想マシンはホストに展開されることが期待されたにも関わらず、ホストにエージェント データストアが設定されていなかったため、エージェントを展開できません。	customAgentVmDatastore に一覧表示されているデータストアの 1 つをホストに追加します。この問題は、データストアが使用可能になった後に自動的に解決されます。
カスタム エージェント仮想マシン ネットワークがない	エージェント仮想マシン ネットワークがない	エージェント仮想マシンがホストに展開されることが期待されたにも関わらず、ホストにエージェント ネットワークが設定されていなかったため、エージェントを展開できません。	カスタム エージェント仮想マシン ネットワークに一覧表示されているネットワークのいずれかにホストを追加します。この問題は、カスタム仮想マシン ネットワークが使用可能になった後に自動的に解決されます。
カスタム エージェント仮想マシン データストアがない	エージェント仮想マシン データストアがない	エージェント仮想マシンはホストに展開されることが期待されたにも関わらず、ホストにエージェント データストアが設定されていなかったため、エージェントを展開できません。	カスタム エージェント仮想マシン データストアに一覧表示されているデータストアのいずれかにホストを追加します。この問題は自動的に解決されます。
エージェンシーの実体が見あたらない	エージェンシーの問題	エージェンシーを作成したソリューションが vCenter Server から登録解除されています。	ソリューションを vCenter Server に登録します。
DvFilter スイッチが見あたらない	ホストの問題	dvFilter スイッチはホスト上にありますが、ホスト上のどのエージェントも dvFilter に依存していません。これは、エージェンシーの設定を変更したときにホストが切断された場合に発生します。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスが、エージェンシーの設定が更新される前にホストに接続しようとしています。
エージェント仮想マシンが不明	ホストの問題	エージェント仮想マシンが vCenter Server インベントリ内に見つかりましたが、このインベントリはこの vSphere ESX Agent Manager サーバ インスタンス内のどのエージェンシーにも属していません。	[解決] をクリックします。ESXi エージェンシー Manager (EAM) サービスが、仮想マシンが属するインベントリに仮想マシンを配置しようとしています。
OVF のプロパティが無効	仮想マシンの問題	エージェント仮想マシンをパワーオンする必要があるにもかかわらず、OVF プロパティが見つからないか、値が無効です。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスは、正しい OVF プロパティの再設定を試みます。
仮想マシンが破損している	仮想マシンの問題	エージェント仮想マシンが破損しています。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスは、仮想マシンの修復を試みます。
仮想マシンの実体が見あたらない	仮想マシンの問題	ホスト上にエージェント仮想マシンがありますが、このホストはエージェンシーの範囲から除外されています。これは、エージェンシーの設定を変更したときにホストが切断された場合に発生します。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスがホストをエージェンシー構成に再接続しようとしています。

表 10-10. ESXi Agency Manager に関する問題（続き）

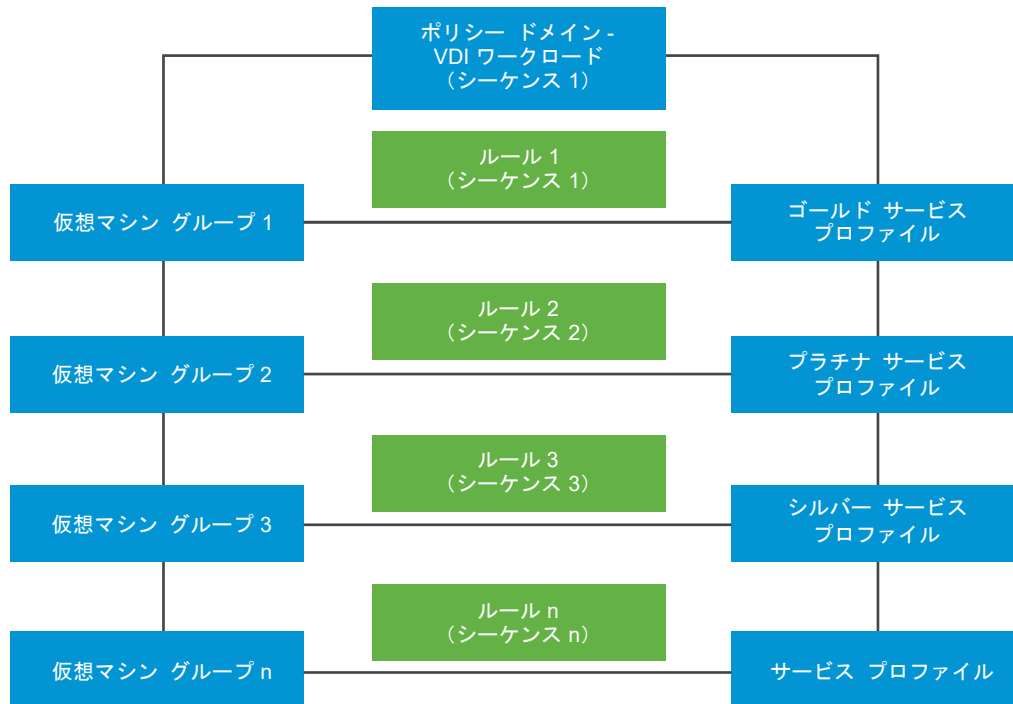
仮想マシンがデプロイされる	仮想マシンの問題	エージェント仮想マシンがホストから削除されることが期待されたにも関わらず、削除されません。vSphere ESX Agent Manager がエージェント仮想マシンを削除できなかった具体的な理由です（ホストがメンテナンスモードである、パワーオフされた、スタンバイ モードであるなど）。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスがホストからエージェント仮想マシンを削除しようとしています。
仮想マシンがパワーオフ状態	仮想マシンの問題	エージェント仮想マシンがパワーオン状態になることが期待されたにも関わらず、パワーオフ状態です。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスは、仮想マシンのパワーオンを試みます。
仮想マシンがパワーオン状態	仮想マシンの問題	エージェント仮想マシンがパワーオフ状態になることが期待されたにも関わらず、パワーオン状態です。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスは、仮想マシンのパワーオフを試みます。
仮想マシンがサスペンド中	仮想マシンの問題	エージェント仮想マシンがパワーオン状態になることが期待されたにも関わらず、サスペンドされています。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスは、仮想マシンのパワーオンを試みます。
仮想マシンのフォルダが正しくない	仮想マシンの問題	エージェント仮想マシンが指定したエージェント仮想マシン フォルダにあることが期待されたにも関わらず、別のフォルダ内に見つかりました。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスが、指定されたフォルダにエージェント仮想マシンの配置を試みています。
仮想マシンのリソース プールが正しくない	仮想マシンの問題	エージェント仮想マシンが指定したエージェント仮想マシンのリソース プール内にあることが期待されたにも関わらず、別のリソース プール内に見つかりました。	[解決] をクリックします。ESXi Agency Manager (EAM) サービスが、指定されたリソース プールにエージェント仮想マシンを配置しようとしています。
仮想マシンが展開されない	エージェントの問題	エージェント仮想マシンがホストに展開されることが期待されたにも関わらず、展開されません。ESXi Agent Manager がエージェントを展開できなかった具体的な理由（エージェントの OVF パッケージにアクセスできない、またはホストの設定ミスなど）です。この問題は、エージェント仮想マシンがホストから明示的に削除されている場合も発生することがあります。	[解決] をクリックして、エージェント仮想マシンを展開します。

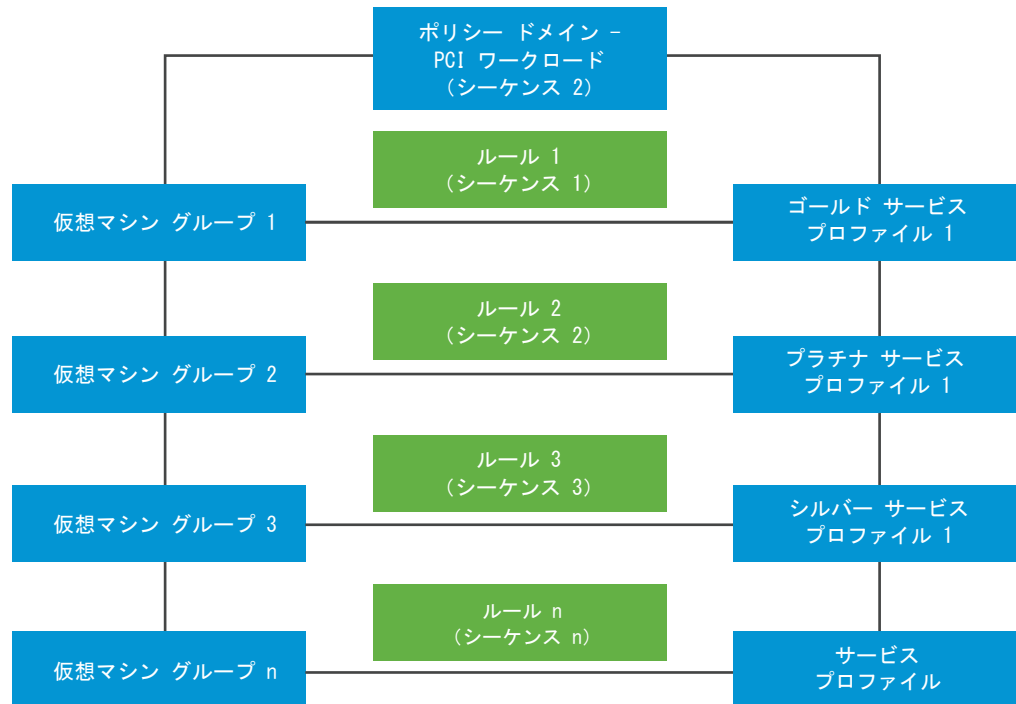
次に、仮想マシン グループにエンドポイントの保護を設定します。[エンドポイントの保護](#) を参照してください。

ゲスト イントロスペクションでエンドポイント保護ポリシーを実行する方法

エンドポイント保護ポリシーは、特定の順序で適用されます。ポリシーを設計する場合は、ルールに関連付けられたシーケンス番号、およびルールをホストしているドメインを考慮します。

シナリオ：組織で実行されている多数のワークロードの中から、分かりやすく例示するため、2種類のワークロードについて考えます。仮想デスクトップ インフラストラクチャ (VDI) を実行する仮想マシンのワークロードと、PCI-DSS（クレジットカード業界のセキュリティ基準）を実行する仮想マシンのワークロードです。組織内の従業員のセクションでは、リモート デスクトップにアクセスする必要があり、これによって仮想デスクトップ インフラストラクチャ (VDI) のワークロードが発生します。これらの VDI ワークロードには、組織によって設定されたコンプライアンス ルールに基づき、ゴールド レベルの保護ポリシーが必要になることがあります。一方、PCI-DSS ワークロードには、保護レベルが最も高い、プラチナ レベルの保護が必要です。





2つのワークロード タイプがあるため、VDI ワークロード用とサーバ ワークロード用にそれぞれ1つずつ、合計 2つのポリシーを作成します。各ポリシーまたはセクション内でワークロード タイプが反映されるドメインを定義し、このセクション内で該当するワークロードのルールを定義します。ゲスト仮想マシンでゲスト イントロスペクション サービスを開始するためのルールを公開します。ゲスト イントロスペクションでは、実行するルールのシーケンス全体を特定するために、ポリシー シーケンス番号とルール シーケンス番号の 2 つのシーケンス番号を内部で使用します。各ルールは、保護する仮想マシンの判別、および仮想マシンを保護するために適用する必要がある保護ポリシーの判別という 2 つの目的に対応しています。

シーケンスの順序を変更するには、NSX-T Policy Manager の UI でルールをドラッグしてシーケンスの順序を変更します。API を使用して、ルールのシーケンス番号を明示的に割り当てることもできます。

または、NSX-T Data Center API 呼び出しを行って、仮想マシン グループにサービス プロファイルに関連付けることによってルールを手動で定義し、ルールのシーケンス番号を宣言します。API およびパラメータの詳細については、『NSX-T Data Center API ガイド』を参照してください。サービス構成 API を呼び出して、仮想マシン グループなどのエンティティにプロファイルを適用します。

表 10-11. NSX-T Data Center API は、仮想マシン グループにサービス プロファイルを適用するルールを定義する際に使用されます。

API	詳細
サービス構成に関するすべての詳細を取得する。	<pre>GET /api/v1/service-configs</pre> <p>サービス構成 API は仮想マシン グループに適用されたサービス プロファイルの詳細、保護されている仮想マシン グループ、およびルールの優先順位を決定するシーケンス番号または優先順位番号を返します。</p>
サービス構成を作成する。	<pre>POST /api/v1/service-configs</pre> <p>サービス構成 API はサービス プロファイル、保護する仮想マシン グループ、およびルールに適用する必要があるシーケンス番号または優先順位番号を入力パラメータとして使用します。</p>
サービス構成を削除する。	<pre>DELETE /api/v1/service-configs/ <config-set-id></pre> <p>サービス構成 API は、仮想マシン グループに適用された設定を削除します。</p>
特定の設定の詳細を取得する。	<pre>GET /api/v1/service-configs/ <config-set-id></pre> <p>特定の設定の詳細を取得します。</p>
サービス構成を更新する。	<pre>PUT /api/v1/service-configs/ <config-set-id></pre> <p>サービス構成を更新する。</p>
有効なプロファイルを取得する。	<pre>GET /api/v1/service-configs/ effective-profiles?resource_id=<resource-id> &resource_type=<resource-type></pre> <p>サービス構成 API は特定の仮想マシン グループに適用されたプロファイルのみを返します。</p>

次に示す推奨事項に基づき、ルールを効率的に管理します。

- ルールを最初に実行する必要があるポリシーに、より大きなシーケンス番号を設定します。UI でポリシーをドラッグし、優先順位を変更することができます。
- 同様に、各ポリシー内のルールに、より大きなシーケンス番号を設定します。
- 必要なルール数に応じて、2、3、4、または 10 の倍数の間隔でルールを配置できます。したがって、2 つの連続するルールの位置が 10 離れている場合は、すべてのルールのシーケンス順を変更しなくても、ルールの再シーケンス化をより柔軟に行うことができます。たとえば、多数のルールを定義する予定がない場合は、ルールの間隔を 10 にして配置することができます。このようにすると、ルール 1 はシーケンス番号 1、ルール 2 はシーケンス番号 10、ルール 3 はシーケンス番号 20 などのようになります。この推奨設定を行うと、ルールを効率的に管理する上で柔軟性が高まり、すべてのルールを再シーケンス化する必要がなくなります。

内部的には、ゲスト イントロスペクションにより、これらのポリシー ルールは次の方法でシーケンス化されます。

```
Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (1001)

- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (1010)

- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (1020)

- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (1030)


Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (2001)

- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (2010)

- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (2020)

- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (2030)
```

上記のシーケンス番号に基づき、ポリシー 1 のルールを実行してから、ポリシー 2 のルールを実行します。

ただし、意図したルールが仮想マシン グループまたは仮想マシンに適用されない場合があります。必要なポリシー保護レベルを適用できるよう、これらの競合を解決する必要があります。

エンドポイント ポリシーが競合する場合の解決策

複数のルールでそれぞれ構成された 2 つのポリシー ドメインがあるシナリオを取り上げます。Admin は、グループのメンバーシップを最終的に取得できる仮想マシンを常に把握しているわけではありません。仮想マシンは OS 名、コンピュータ名、ユーザー、タグ付けなどの動的なメンバーシップ基準に基づいてグループに関連付けられるためです。

競合は次の場合に発生します。

- 仮想マシンが 2 つのグループに属していて、それぞれのグループが異なるプロファイルで保護されている場合。
- パートナー サービス仮想マシンが、複数のサービス プロファイルに関連付けられている場合。
- ゲスト仮想マシンで予期せぬルールが実行されたか、仮想マシン グループでルールが実行されていない場合。
- ポリシー ルールまたはドメインにシーケンス番号が割り当てられていない場合。

表 10-12. ポリシーの競合の解決

シナリオ	想定されるエンドポイント保護のフロー	解決方法
<p>1 台の仮想マシンが複数のグループのメンバーシップを取得する。そして、各グループが、それぞれ異なるタイプのサービス プロファイルによって保護されている場合。</p> <p>想定される保護が仮想マシンに適用されていない場合。</p>	<p>メンバーシップ基準に沿って作成された仮想マシングループがあるということは、仮想マシンがグループに動的に追加されたことを意味します。このような場合は、同じ仮想マシンが複数のグループに属することができます。仮想マシンはメンバーシップ基準に沿ってグループに動的に設定されるため、仮想マシンが所属するグループを事前に判別することはできません。</p> <p>仮想マシン 1 がグループ 1 およびグループ 2 に含まれているとします。</p> <ul style="list-style-type: none"> ■ ルール 1: グループ 1 (OS 名別) は、シーケンス番号 1 でゴールド (サービス プロファイル) に適用されます。 ■ ルール 2: グループ 2 (タグ別) は、シーケンス番号 10 でプラチナが適用されます。 <p>エンドポイント保護ポリシーにより、ゴールド サービス プロファイルは仮想マシン 1 で実行されますが、プラチナ サービス プロファイルは仮想マシン 1 で実行されません。</p>	<p>ルール 1 よりも前に実行されるように、ルール 2 のシーケンス番号を変更します。</p> <ul style="list-style-type: none"> ■ NSX-T Policy Manager の UI で、ルール 2 をルール リスト内のルール 1 より前の位置までドラッグします。 ■ NSX-T Policy Manager API を使用して、ルール 2 にさらに大きなシーケンス番号を手動で追加します。
<p>ルールにより、2 つの仮想マシン グループを保護するために同じサービス プロファイルが関連付けられている場合。エンドポイントの保護を行っても、2 番目の仮想マシン グループではルールが実行されない場合。</p>	<p>エンドポイントの保護により、この仮想マシンでは最初のサービス プロファイルのみが実行されます。これは、ポリシーまたはドメインをまたがる他のルールに、同じサービス プロファイルを適用することはできないためです。</p> <p>仮想マシン 1 がグループ 1 およびグループ 2 に含まれているとします。</p> <p>ルール 1: グループ 1 (OS 名別) は、ゴールド (サービス プロファイル) に適用されます。</p> <p>ルール 2: グループ 2 (タグ別) は、ゴールド (サービス プロファイル) に適用されます。</p>	<ul style="list-style-type: none"> ■ ルール 1 にグループ 2 を追加します。(ルール 1: グループ 1、グループ 2 にはプロファイル 1 が適用されます)

仮想マシンの検疫

パートナーが設定した保護レベルとタグに基づいて、ルールを仮想マシン グループに追加すると、仮想マシンが感染していると見なされ隔離の必要がある場合があります。

パートナーは `virus_found=true` タグが含まれる API を使用し、感染している仮想マシンにタグを付けます。影響を受ける仮想マシンには、`virus_found=true` タグが追加されます。

管理者は、`virus_found=true` 値のタグに基づいて定義済み検疫グループを作成できます。タグ付けされると、このグループに感染した仮想マシンがまとめられます。Admin として、検疫グループ専用のファイアウォール ルールを設定できます。検疫グループに複数のファイアウォール ルールを設定することができます。たとえば、検疫グループに対するすべての送受信トラフィックをブロックすることもできます。

サービス インスタンスの健全性状態の確認

サービス インスタンスの健全性状態は、多くの要因に依存します。これには、パートナーのソリューションの状態、Guest Introspection Agent (コンテキスト マルチプレクサ) とコンテキスト エンジン (Ops Agent) の接続の状

態、Guest Introspection Agent 情報の可用性、NSX Manager でのサービス仮想マシン プロトコルの情報などがあります。

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 [システム] - [サービス展開] - [サービス インスタンス] を選択します。
- 3 [健全性状態] 列で  をクリックしてサービス インスタンスの健全性を確認します。

表 10-13. サード パーティ製サービス インスタンスの健全性状態

パラメータ	説明
健全性状態の受信時間	NSX Manager がサービス インスタンスの健全性状態の詳細を受信した最新のタイムスタンプ。
ソリューションの状態	サービス仮想マシンで実行中のパートナー ソリューションの状態。「UP」状態はパートナー ソリューションが正常に実行されていることを示します。
NSX-T Data Center Guest Introspection Agent と NSX-T Data Center Ops Agent 間の接続	NSX-T Data Center Guest Introspection Agent (コンテキスト マルチプレクサ) が Ops Agent (コンテキスト エンジンを含む) に接続されている場合に状態が「UP」になります。コンテキスト マルチプレクサは、サービス仮想マシンの健全性情報をコンテキスト エンジンに転送します。サービス仮想マシンは、サービス仮想マシンと仮想マシンの構成を相互に共有することで、サービス仮想マシンによって保護されるゲスト仮想マシンを把握します。
サービス仮想マシン プロトコルのバージョン	問題のトラブルシューティングを行う際に内部で使用するトランスポート プロトコルのバージョン。
NSX-T Data Center Guest Introspection Agent の情報	NSX-T Data Center Guest Introspection Agent とサービス仮想マシン間のプロトコル バージョンの互換性を表します。

- 4 健全性状態が Up (状態は緑色で表示) で、パートナー コンソールにすべてのゲスト仮想マシンが保護されていると表示された場合、サービス インスタンスの健全性状態は Up になります。
- 5 健全性状態が Up (状態は緑色で表示) で、パートナー コンソールにゲスト仮想マシンが保護されていないと表示された場合は、次の手順を実行します。
 - a VMware サポートに問い合わせ、この問題を解決します。サービス インスタンスの健全性状態は、NSX Manager ユーザー インターフェイスに正しく反映されない場合、「Down」と表示されることもあります。

- 6 健全性状態が Down（状態は赤色で表示）の場合、サービス インスタンスの健全性を決定する 1 つ以上の要因が停止しています。

表 10-14. 健全性状態のトラブルシューティング

健全性状態の属性	解決方法
ソリューションの状態が Down または Not available。	<ol style="list-style-type: none"> 1 サービス展開の状態が Up（緑色）であることを確認します。問題が発生した場合は、パートナー サービスの問題の解決を参照してください。 2 影響を受けるホストの 1 台以上の仮想マシンがエンドポイント保護ポリシーで保護されていることを確認します。 3 パートナー コンソールから、ソリューション サービスがホスト上のサービス仮想マシンで実行されているかどうかを確認します。詳細については、パートナーのドキュメントを参照してください。 4 上記の手順でも問題が解決しない場合は、VMware サポートにお問い合わせください。
NSX-T Data Center Guest Introspection Agent と NSX-T Data Center Ops Agent 間の接続が Down。	<ol style="list-style-type: none"> 1 サービス展開の状態が Up（緑色）であることを確認します。問題が発生した場合は、パートナー サービスの問題の解決を参照してください。 2 影響を受けるホストの 1 台以上の仮想マシンがエンドポイント保護ポリシーで保護されていることを確認します。 3 パートナー コンソールから、ソリューション サービスがホスト上のサービス仮想マシンで実行されているかどうかを確認します。詳細については、パートナーのドキュメントを参照してください。 4 上記の手順でも問題が解決しない場合は、VMware サポートにお問い合わせください。
サービス仮想マシン プロトコルのバージョンが Unavailable。	<ol style="list-style-type: none"> 1 サービス展開の状態が Up（緑色）であることを確認します。問題が発生した場合は、パートナー サービスの問題の解決を参照してください。 2 影響を受けるホストの 1 台以上の仮想マシンがエンドポイント保護ポリシーで保護されていることを確認します。 3 パートナー コンソールから、ソリューション サービスがホスト上のサービス仮想マシンで実行されているかどうかを確認します。詳細については、パートナーのドキュメントを参照してください。 4 上記の手順でも問題が解決しない場合は、VMware サポートにお問い合わせください。
NSX-T Data Center Guest Introspection Agent の情報が Unavailable。	VMware サポートにお問い合わせください。

パートナー サービスの削除

パートナー サービスを削除するには、API 呼び出しを行います。API 呼び出しを行って、ホストに展開されたパートナー サービスまたはサービス仮想マシンを削除するには、あらかじめ NSX Manager ユーザー インターフェイスから次の操作を実行しておく必要があります。

パートナー サービスを削除するには、次の操作を実行します。

手順

- 1 ホスト上で実行されている仮想マシン グループに適用される EPP ルールを削除します。

- 仮想マシン グループに適用されるサービス プロファイルの保護を削除します。
- パートナーの Service Manager とサービス仮想マシンを割り当てるソリューションを削除するには、次の API 呼び出しを行います。

```
/DEL https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/{{service_id}}/
solution-configs/<solution-config-id>
```

- サービス展開を削除するには、次の API 呼び出しを行います。

```
/DEL https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/<service-id>/service-
deployments/<service-deployment-id>
```

API のパラメータの詳細については、『NSX-T Data Center API ガイド』を参照してください。

セキュリティ プロファイル

このセクションには、ファイアウォール操作を調整するプロファイル（セッションタイマー、フラッド防止、DNS セキュリティ）が含まれています。

セッション タイマーの作成

セッション タイマーは、セッションが非アクティブ状態になった後にファイアウォールでそのセッションが保持される期間を定義します。

プロトコルのセッションがタイムアウトになると、そのセッションは閉じられます。ファイアウォールで、TCP、UDP、ICMP セッションに複数のタイムアウトを指定し、ユーザー定義のグループ、Tier-0 または Tier-1 ゲートウェイに適用できます。デフォルトのセッションの値は、ネットワークのニーズに応じて変更できます。設定値が小さすぎるとタイムアウトが頻繁に発生するようになり、大きすぎると障害検知が遅れる可能性があります。

手順

- [セキュリティ] - [設定] - [セキュリティ プロファイル] - [セッション タイマー] に移動します。
- [プロファイルの追加] をクリックします。
[プロファイル] 画面が表示され、デフォルト値が入力されます。
- タイマー プロファイルで、[名前] と [説明]（オプション）を入力します。
- [設定] をクリックして、このタイマー プロファイルを適用する Tier-0 または Tier-1 のゲートウェイか、グループを選択します。
- プロトコルを選択します。デフォルト値を受け入れるか、別の値を入力します。

TCP 変数	説明
First Packet	最初のパケットが送信された後の、接続のタイムアウト値です。デフォルトは 120 秒です。
Opening	2 番目のパケットが転送された後の、接続のタイムアウト値です。デフォルトは 30 秒です。
Established	接続が完全に確立された後の、接続のタイムアウト値です。
Closing	最初の FIN が送信された後の、接続のタイムアウト値です。デフォルトは 120 秒です。

TCP 変数	説明
Fin Wait	両方の FIN が交換され、接続が閉じられた後の、接続のタイムアウト値です。デフォルトは 45 秒です。
Closed	1 つのエンドポイントが RST を送信した後の、接続のタイムアウト値です。デフォルトは 20 秒です。
UDP 変数	説明
First Packet	最初のパケットが送信された後の、接続のタイムアウト値です。これは、新しい UDP フローの最初のタイムアウトになります。デフォルトは 60 秒です。
Single	送信元ホストが複数のパケットを送信し、宛先ホストが送り返さなかった場合の、接続のタイムアウト値です。デフォルトは 30 秒です。
Multiple	両方のホストがパケットを送信した場合の、接続のタイムアウト値です。デフォルトは 60 秒です。
ICMP 変数	説明
First Packet	最初のパケットが送信された後の、接続のタイムアウト値です。これは、新しい ICMP フローの最初のタイムアウトになります。デフォルトは 20 秒です。
Error reply	ICMP パケットへの応答で ICMP エラーが返された後の、接続のタイムアウト値です。デフォルトは 10 秒です。

6 [保存] をクリックします。

次のステップ

保存後、[グループとプロファイルの優先順位の管理](#)をクリックしてグループを管理し、プロファイルの割り当ての優先順位を設定します。

セッション タイマーのデフォルト値

セッション タイマー プロファイルは、Tier-0 または Tier-1 ルーター インターフェイスまたはセグメントを含むグループにタイムアウト値を適用します。タイムアウト値により、セッションの終了後にプロトコル セッションがアクティブな状態を維持する時間が決まります。

セッション タイマーの値

- API およびユーザー インターフェイスで表示されるデフォルトのタイマー プロファイルは、分散ファイアウォール (DFW) にのみ適用されます。
- ゲートウェイ ファイアウォール (GFW) のデフォルトのセッション タイマーは、API およびユーザー インターフェイスの使用中表示されるデフォルトのプロファイル タイマーとは異なります。GFW のデフォルトのセッション タイマーは、North-South トラフィック用に最適化されており、デフォルトでは短い期間になっています。
- ファイアウォールのセッション タイマーは、API とユーザー インターフェイスを使用して、DFW と GFW の両方で変更できます。
- 必要に応じて、DFW と GFW の両方にデフォルト以外の同じタイマー プロファイルを適用できます。

タイマーの値をカスタマイズしない場合、ゲートウェイはデフォルト値を使用します。ゲートウェイ ファイアウォールのタイマーのデフォルト値は次のとおりです。

タイマー プロパティ	Edge のデフォルト値 (秒)	最小 (秒)	最大 (秒)
ICMP エラー応答	6	10	4320000
ICMP の最初のバケット	6	10	4320000
TCP 終了済み	2	10	4320000
TCP 終了中	900	10	4320000
TCP 確立済み	7200	120	4320000
TCP Fin 待機中	4	10	4320000
TCP の最初のバケット	120	10	4320000
TCP 開始中	30	10	4320000
UDP の最初のバケット	30	10	4320000
UDP 複数	30	10	4320000
UDP 単一	30	10	4320000

分散ファイアウォールのセッション タイマーのデフォルト値は次のとおりです。

タイマー プロパティ	DFW のデフォルト値 (秒)	最小 (秒)	最大 (秒)
ICMP エラー応答	10	10	4320000
ICMP の最初のバケット	20	10	4320000
TCP 終了済み	20	10	4320000
TCP 終了中	120	10	4320000
TCP 確立済み	43200	120	4320000
TCP Fin 待機中	45	10	4320000
TCP の最初のバケット	120	10	4320000
TCP 開始中	30	10	4320000
UDP の最初のバケット	60	10	4320000
UDP 複数	60	10	4320000
UDP 単一	30	10	4320000

フラッド防止

フラッド防止は、サービス拒否 (DDoS) 攻撃に対する保護に役立ちます。

DDoS 攻撃は、サーバに大量の要求を処理させて、使用可能なすべてのサーバ リソースを消費することにより、サーバでの正規のトラフィックの処理を妨害することを目的としています。フラッド防止プロファイルを作成すると、ICMP、UDP、ハーフオープン の TCP フローに対してアクティブなセッション制限を適用できます。分散ファイアウォールは、SYN_SENT および SYN_RECEIVED 状態にあるフロー エントリをキャッシュに保存し、ACK をイニシエータから受信した後に TCP 状態に昇格させ、3 方向ハンドシェイクを完了します。

手順

- 1 [セキュリティ] - [セキュリティ プロファイル] - [フラッド防止] の順に移動します。
- 2 [プロファイルの追加] をクリックして、[Edge ゲートウェイ プロファイルの追加] または [ファイアウォール プロファイルの追加] を選択します。
- 3 フラッド防止プロファイルのパラメータを入力します。

表 10-15. ファイアウォールと Edge Gateway プロファイルのパラメータ

パラメータ	最小値と最大値	デフォルト	
TCP ハーフ オープン接続の制限 : TCP SYN フラッド攻撃は、ファイアウォールで許可されるアクティブで、完全に確立されていない TCP フローの数を制限することで回避できます。	1 ~ 1,000,000	ファイアウォール : なし Edge Gateway : 1,000,000	アクティブな TCP ハーフオープン接続の数を制限するには、このテキスト ボックスを設定します。このテキスト ボックスを空にすると、この制限は ESX ノードで無効になり、Edge Gateway の値がデフォルトになります。
UDP アクティブ フロー制限 : UDP フラッド攻撃は、ファイアウォールで許可されるアクティブな UDP フローの数を制限することで回避できます。UDP フロー制限の設定に達すると、新しいフローを確立する後続の UDP パケットがドロップされます。	1 ~ 1,000,000	ファイアウォール : なし Edge Gateway : 1,000,000	アクティブな UDP 接続の数を制限するには、このテキスト ボックスを設定します。このテキスト ボックスを空にすると、この制限は ESX ノードで無効になり、Edge Gateway の値がデフォルトになります。
ICMP アクティブ フロー制限 : ICMP フラッド攻撃は、ファイアウォールで許可されるアクティブな ICMP フローの数を制限することで回避できます。ICMP フロー制限の設定に達すると、新しいフローを確立する後続の ICMP パケットがドロップされます。	1 ~ 1,000,000	ファイアウォール : なし Edge Gateway : 10,000	アクティブな ICMP オープン接続の数を制限するには、このテキスト ボックスを設定します。このテキスト ボックスを空にすると、この制限は ESX ノードで無効になり、Edge Gateway の値がデフォルトになります。
その他のアクティブ接続の制限	1 ~ 1,000,000	ファイアウォール : なし Edge Gateway : 10,000	ICMP、TCP、UDP ハーフオープン接続以外のアクティブな接続数を制限するには、このテキスト ボックスを設定します。このテキスト ボックスを空にすると、この制限は ESX ノードで無効になり、Edge Gateway の値がデフォルトになります。

表 10-15. ファイアウォールと Edge Gateway プロファイルのパラメータ（続き）

パラメータ	最小値と最大値	デフォルト	
SYN キャッシュ：SYN キャッシュは、TCP ハーフオープン接続の制限が設定されている場合に使用されます。完全に確立されていない TCP セッションの syncache を維持することで、アクティブなハーフオープン接続の数が限定されます。このキャッシュは、SYN_SENT および SYN_RECEIVED 状態にあるフロー エントリを格納します。各 syncache エントリは、イニシエータから ACK を受信した後、完全な TCP 状態のエントリに昇格し、3 方向のハンドシェイクが完了します。		ファイアウォール プロファイルでのみ使用できます。	オンとオフを切り替えます。SYN キャッシュの有効化は、TCP ハーフオープン接続制限が設定されている場合にのみ有効です。
RST スプーフィング：SYN キャッシュから ハーフオープン状態を削除するときに、サーバに対して偽の RST を生成します。サーバで SYN フラッドに関連付けられた状態（ハーフオープン）をクリーンアップできます。		ファイアウォール プロファイルでのみ使用できます。	オンとオフを切り替えます。このオプションを使用するには、SYN キャッシュを選択する必要があります

4 プロファイルを Edge Gateway とファイアウォール グループに適用するには、[設定] をクリックします。

5 [保存] をクリックします。

次のステップ

保存後、[グループとプロファイルの優先順位の管理](#)をクリックしてグループを管理し、プロファイルの割り当ての優先順位を設定します。

DNS セキュリティの設定

DNS セキュリティ プロファイルを作成すると、DNS 関連の攻撃を防ぐことができます。

DNS セキュリティ プロファイルを設定したら、次の操作を行います。

- トランスポート ノードの仮想マシンまたは仮想マシン グループの DNS 応答をスヌーピングし、FQDN と IP アドレスを関連付けます。
- グローバルとデフォルトの DNS サーバ情報を追加し、DFW を使用しているすべての仮想マシンに適用します。
- 選択した仮想マシンに対して、選択した DNS サーバ情報を指定します。
- DNS プロファイルをグループに適用します。

注： 現在のリリースでは、ESXi のみがサポートされます。

手順

- 1 [セキュリティ] - [設定] - [セキュリティ プロファイル] - [DNS セキュリティ] に移動します。
- 2 [プロファイルの追加] をクリックします。
- 3 次の値を入力します。

オプション	説明
プロファイル名	プロファイル名を入力します。
TTL	<p>このフィールドは、DNS キャッシュ エントリの有効期間を秒単位でキャプチャします。次のオプションがあります。</p> <p>TTL 0：キャッシュされたエントリは期限切れになりません。</p> <p>TTL 1 ～ 3599：無効</p> <p>TTL 3600 ～ 864000：有効</p> <p>TTL が空の場合：DNS 応答パケットから TTL が自動的に設定されます。</p> <p>注： DNS セキュリティ プロファイルのデフォルトの DNS キャッシュ タイムアウトは 24 時間です。</p>
適用先	<p>任意の基準に基づいてグループを選択し、DNS セキュリティ プロファイルを適用できます。</p> <p>注： 1 台の仮想マシンに適用できる DNS サーバ プロファイルは 1 つだけです。</p>
タグ	任意。検索を簡単にするため、DNS プロファイルにタグと範囲を割り当てます。詳細については、 オブジェクトへのタグの追加 を参照してください。

- 4 [保存] をクリックします。

次のステップ

保存後、[グループとプロファイルの優先順位の管理](#)をクリックしてグループを管理し、プロファイルの割り当ての優先順位を設定します。

グループとプロファイルの優先順位の管理

複数のグループを 1 つのセキュリティ プロファイルに割り当てることができます。NSX-T Data Center は、優先順位が最も高いグループにセキュリティ プロファイルを適用します。

1 つのセキュリティ プロファイルを複数のグループに割り当てると、NSX-T Data Center はそのリストから最も新しいグループに最も高い優先順位を割り当てます。グループの優先順位は変更できます。

グループに優先順位を割り当てするには：

前提条件

- セッション タイマー グループには、セグメント、セグメント ポート、仮想マシンのみをメンバーとして含める必要があります。その他のカテゴリ タイプはサポートされていません。
- DNS セキュリティ グループには、仮想マシンのみをメンバーとして含める必要があります。その他のカテゴリ タイプはサポートされていません。

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 [セキュリティ] > [セキュリティ プロファイル] の順に移動します。
- 3 [グループとプロファイルの優先順位の管理] をクリックします。
- 4 グループに最も高い優先順位を割り当てるには、そのグループをリストの先頭に移動します。
- 5 [閉じる] をクリックします。

結果

最も高い優先順位のグループにセキュリティ プロファイルが適用されます。

NSX-T Data Center インベントリのサービス、グループ、コンテキスト プロファイル、仮想マシンを設定できます。

[インベントリ] タブをクリックすると、インベントリ オブジェクトの概要が表示され、インベントリ内のグループ、サービス、仮想マシン、コンテキスト プロファイルの数が表示されます。さらに、グループに関する次の情報も表示されます。

- ポリシーで使用されているグループの数
- ポリシーで使用されていないグループの数
- メンバーを持つグループの数
- メンバーを持たないグループの数
- ID グループの数
- ポリシーで使用されている ID グループの数
- ポリシーで使用されていない ID グループの数

この章には、次のトピックが含まれています。

- [サービスの追加](#)
- [グループの追加](#)
- [コンテキスト プロファイルの追加](#)

サービスの追加

サービスを設定して、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、サービスを使用して、ファイアウォール ルール内で特定のタイプのトラフィックを許可またはブロックすることもできます。サービスを作成した後でタイプを変更することはできません。一部のサービスは事前定義されていて、変更または削除できません。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [インベントリ] - [サービス] の順に選択します。

- 3 [新しいサービスの追加] をクリックします。
- 4 名前を入力します。
- 5 [サービス エントリの設定] をクリックします。[新しいサービス エントリの追加] をクリックします。
- 6 新しいサービスに対して、サービスのタイプを選択し、追加のプロパティを指定します。
使用可能なタイプは [IP]、[IGMP]、[ICMPv4]、[ICMPv6]、[ALG]、[TCP]、[UDP]、および [Ether] です。
- 7 [保存] をクリックします。
- 8 (オプション) 1 つ以上のタグを追加します。
- 9 (オプション) 説明を入力します。
- 10 [保存] をクリックします。

グループの追加

グループには静的および動的に追加されたさまざまなオブジェクトが含まれています。これらは、ファイアウォール ルールの送信元または宛先として使用できます。

また、仮想マシン、IP セット、MAC セット、セグメント ポート、セグメント、Active Directory ユーザー グループ、およびその他のグループの組み合わせを含むように設定できます。グループの動的な追加は、タグ、マシン名、OS 名、またはコンピュータ名に基づいて行うことができます。動的オブジェクトまたは論理オブジェクトに基づくグループは、分散ファイアウォール ルールの [適用先] フィールドで使用できません。

NSX 内のタグは大文字と小文字が区別されますが、タグに基づくグループでは区別されません。たとえば、動的グループ メンバーシップの基準が VM Tag Equals 'quarantine' 場合、「quarantine」または「QUARANTINE」のいずれかのタグを含むすべての仮想マシンがこのグループに含まれます。

グループはファイアウォール ルールから除外できます。また、最大で 100 個のグループがリストに表示されます。IP セット、MAC セット、Active Directory グループは、ファイアウォール除外リストにあるグループのメンバーとして追加できません。詳細については、[ファイアウォール除外リストの管理](#)を参照してください。

NSX Cloud の注： NSX Cloud を使用している場合は、[NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化](#)を参照して、パブリック クラウド タグで NSX Manager 内のワークロード仮想マシンをグループ化する方法を確認してください。

1 つの ID ベースのグループは、分散ファイアウォール ルール内の送信元としてのみ使用できます。ソースで IP ベースと ID ベースのグループが必要な場合は、それぞれのグループにファイアウォール ルールを作成します。

IP アドレス、MAC アドレス、または Active Directory グループのみで構成されるグループは、[適用先] テキスト ボックスで使用できません。

注： ホストが vCenter Server に追加されたり、vCenter Server から削除されると、ホストの仮想マシンの外部 ID が変更されます。仮想マシンがグループの固定メンバーで、その外部 ID が変更されると、NSX Manager のユーザー インターフェイスで、この仮想マシンはグループのメンバーとして表示されなくなります。ただし、グループのリストを取得する API を実行すると、このグループに元の外部 ID を持つ仮想マシンが含まれています。グループの固定メンバーとして追加した仮想マシンの外部 ID が変更された場合は、新しい外部 ID を使用して仮想マシンを再度追加する必要があります。動的なメンバーシップ基準を使用して、この問題を回避することもできます。

手順

1 ナビゲーション パネルから、[インベントリ] - [グループ] の順に選択します。

2 [グループの追加] をクリックします。

3 グループ名を入力します。

4 (オプション) [メンバーの設定] をクリックします。

メンバーシップの基準ごとに、最大で 5 つのルールを論理 AND 演算子と組み合わせて指定することができます。利用可能なメンバー基準は以下に適用できます。

- [セグメント ポート] - タグとオプションのスコープを指定できます。
- [セグメント] - タグとオプションのスコープを指定できます。
- [仮想マシン] - 名前、タグ、コンピュータの OS 名、または一定の条件を満たすコンピュータ名（特定の文字列と等しい、特定の文字列で開始または終了する、特定の文字列と等しくないなど）を指定できます。
- [IP セット] - タグとオプションのスコープを指定できます。

5 (オプション) [メンバー] をクリックしてメンバーを選択します。

使用可能なメンバー タイプは次のとおりです。

- [グループ]
- [セグメント]
- [セグメント ポート]
- [仮想ネットワーク インターフェイス]
- [仮想マシン]

6 (オプション) [IP /MAC アドレス] をクリックして、IP アドレスおよび MAC アドレスをグループ メンバーとして追加します。

IPv4、IPv6、マルチキャスト アドレスがサポートされています。

7 (オプション) [Active Directory グループ] をクリックして、Active Directory グループを追加します。

Active Directory のメンバーを持つグループは、Identity Firewall の分散ファイアウォール ルールの送信元フィールドに使用できます。グループには、Active Directory とコンピュート メンバーの両方を含めることができます。

8 (オプション) 説明とタグを入力します。

9 [適用] をクリックします。

グループが表示され、メンバーとグループの使用場所を表示するオプションが示されます。

コンテキスト プロファイルの追加

コンテキスト プロファイルを使用すると、レイヤー 7 アプリケーション ID やドメイン名などの属性キー値のペアを作成できます。定義したコンテキスト プロファイルは、1 つ以上の分散ファイアウォール ルールとゲートウェイ ファイアウォール ルールで使用できます。

コンテキスト プロファイルで使用する属性には、アプリケーション ID とドメイン名 (FQDN) の 2 つがあります。アプリケーション ID を選択する場合、TLS_Version や CIPHER_SUITE などのサブ属性を 1 つ以上含めることができます。1 つのコンテキスト プロファイル内でアプリケーション ID とドメイン名の両方を使用できます。同じプロファイル内で複数のアプリケーション ID を使用することもできます。サブ属性を持つアプリケーション ID は 1 つ使用できます。1 つのプロファイル内で複数のアプリケーション ID 属性が使用されている場合、サブ属性はクリアされます。

現在は、事前定義済みのドメインのリストがサポートされています。属性タイプ「ドメイン (FQDN) 名」の新しいコンテキスト プロファイルを追加する場合、FQDN のリストを表示できます。API 呼び出し `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` を実行して FQDN のリストを表示することもできます。

注：

- ゲートウェイ ファイアウォール ルールでは、コンテキスト プロファイルに FQDN 属性または他のサブ属性は使用できません。
- コンテキスト プロファイルは、Tier-0 ゲートウェイ ファイアウォール ポリシーでサポートされていません。ゲートウェイ ファイアウォール ルールでは、FQDN 属性または他のサブ属性は使用できません。

手順

- 1 [インベントリ] - [コンテキスト プロファイル] の順に選択します。
- 2 [新しいコンテキスト プロファイルの追加] をクリックします。
- 3 [プロファイル名] を入力します。
- 4 [属性] 列で [設定] をクリックします。
- 5 属性を選択するか、[属性の追加] をクリックして、[アプリケーション ID] または [ドメイン名 (FQDN)] を選択します。
- 6 1 つ以上の属性を選択します。
- 7 (オプション) SSL や CIFS などのサブ属性を含む属性を選択した場合は、[サブ属性/値] 列で [設定] をクリックします。
 - a [サブ属性の追加] をクリックして、ドロップダウン メニューからサブ属性のカテゴリを選択します。
 - b 1 つ以上のサブ属性を選択します。

c [追加] をクリックします。[サブ属性の追加] をクリックして、別のサブ属性を追加できます。

d [適用] をクリックします。

8 [追加] をクリックします。

9 (オプション) 別のタイプの属性を追加するには、[属性の追加] を再度クリックします。

10 [適用] をクリックします。

11 (オプション) 説明を入力します。

12 (オプション) タグを入力します。

13 [保存] をクリックします。

次のステップ

このコンテキスト プロファイルをレイヤー 7 の分散ファイアウォール ルール (レイヤー 7 またはドメイン名) またはゲートウェイ ファイアウォール ルール (レイヤー 7) に適用します。

NSX-T 環境やネットワーク トラフィックの監視には、いくつかの方法があります。

この章には、次のトピックが含まれています。

- ファイアウォールの IPFIX プロファイルの追加
- スイッチの IPFIX プロファイルの追加
- IPFIX コレクタの追加
- ポート ミラーリング プロファイルの追加
- 簡易ネットワーク管理プロトコル (SNMP)
- vRealize Log Insight によるシステムの監視
- vRealize Operations Manager によるシステムの監視
- vRealize Network Insight Cloud によるシステムの監視
- 高度な監視ツール

ファイアウォールの IPFIX プロファイルの追加

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>>) に管理者権限でログインします。
- 2 [プランとトラブルシューティング] - [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] タブをクリックします。
- 4 [ファイアウォールの IPFIX プロファイルの追加] をクリックします。

5 次の詳細をすべて入力します。

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。 注： グローバル プロファイルを作成する場合は、プロファイルに Global という名前を付ける必要があります。UI からグローバル プロファイルを編集または削除することはできませんが、NSX-T Data Center API を使用すると、このような操作を行うことができます。
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。
観測ドメイン ID	このパラメータは、ネットワーク フローの送信元の観測ドメインを特定します。デフォルトは 0 で、特定の観測ドメインを指定しません。
コレクタの構成	ドロップダウン メニューからコレクタを選択します。
適用先	[設定] をクリックして、フィルタを適用するグループを選択するか、新しいグループを作成します。
優先順位	このパラメータは、複数のプロファイルを適用する際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。

6 [保存] をクリックし、[はい] をクリックしてプロファイルの設定を続行します。

7 [保存] をクリックします。

スイッチの IPFIX プロファイルの追加

セグメントとも呼ばれる、スイッチの IPFIX プロファイルを設定できます。

フローベースのネットワーク モニタリングにより、ネットワーク管理者はネットワークを通過するトラフィックを把握できます。

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 [プランとトラブルシューティング] - [IPFIX] の順に選択します。
- 3 [スイッチの IPFIX プロファイル] タブをクリックします。
- 4 [スイッチの IPFIX プロファイルの追加] をクリックします。
- 5 次の詳細を入力します。

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。 注： グローバル プロファイルを作成する場合は、プロファイルに Global という名前を付ける必要があります。UI からグローバル プロファイルを編集または削除することはできませんが、NSX-T Data Center API を使用すると、このような操作を行うことができます。
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パケットを受信中の場合でも、フローはタイムアウトになります。デフォルト値は 300 です。

設定	説明
アイドル タイムアウト (秒)	フローと関連付けられているパケットを受信しない場合に、フローがタイムアウトするまでの時間 (秒) を指定します。これは ESXi の場合にのみ有効です。KVM の場合は、アクティブ タイムアウトの値に基づいて、すべてのフローがタイムアウトします。デフォルト値は 300 です。
パケット サンプリング率 (%)	サンプリングされるパケットの割合です (概数値)。この設定を高くすると、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。
コレクタの構成	ドロップダウン メニューからコレクタを選択します。
適用先	カテゴリ (セグメント、セグメント ポートまたはグループ) を選択します。選択したオブジェクトに IPFIX プロファイルが適用されます。
優先順位	このパラメータは、複数のプロファイルを適用する際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。
最大フロー数	ブリッジにキャッシュされるフローの最大数を指定します。KVM の場合にのみ有効です。ESXi では設定できません。デフォルト値は 16384 です。
観測ドメイン ID	観測ドメイン ID は、ネットワーク フローの送信元である観測ドメインを識別します。特定の観測ドメインがないことを示すには、0 を入力します。
オーバーレイ フローのエクスポート	このパラメータでは、アップリンクとトンネル ポートのオーバーレイ フローをサンプリングしてエクスポートするかどうかを定義します。サンプルには、vNIC フローとオーバーレイ フローの両方が含まれます。デフォルトは [有効] です。無効にすると、vNIC フローのみがサンプリングされ、エクスポートされます。
タグ	タグを入力して検索しやすくします。

6 [保存] をクリックし、[はい] をクリックしてプロファイルの設定を続行します。

7 [適用先] をクリックして、プロファイルをオブジェクトに適用します。

1 つ以上のオブジェクトを選択します。

8 [保存] をクリックします。

IPFIX コレクタの追加

ファイアウォールおよびスイッチに 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>>) に管理者権限でログインします。
- 2 [プランとトラブルシューティング] - [IPFIX] の順に選択します。
- 3 [コレクタ] タブをクリックします。
- 4 [新しいコレクタの追加] - [IPFIX スイッチ] または [新しいコレクタの追加] - [IPFIX ファイアウォール] の順に選択します。
- 5 名前を入力します。

- 6 最大 4 つのコレクタの IP アドレスおよびポートを入力します。IPv4 と IPv6 の両方のアドレスがサポートされています。
- 7 [保存] をクリックします。

ポート ミラーリング プロファイルの追加

ポート ミラーリング セッション用にポート ミラーリング プロファイルを設定できます。

論理 SPAN は、オーバーレイ セグメントでのみサポートされます。VLAN セグメントには対応していません。

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 [プランとトラブルシューティング] - [ポート ミラーリング] の順に選択します。
- 3 [プロファイルの追加] - [リモート L3 SPAN] または [プロファイルの追加] - [論理 SPAN] の順に選択します。
- 4 名前を入力します。必要に応じて説明も入力します。
- 5 次に示すプロファイルの詳細を入力します。

セッション タイプ	パラメータ
リモート L3 SPAN	<ul style="list-style-type: none"> ■ [方向]: [双方向]、[入力方向]、または [出力方向] を選択します。 ■ [スナップの長さ]: パケットからキャプチャするバイト数を指定します。 ■ [カプセル化タイプ]: [GRE]、[ERSPAN 2]、または [ERSPAN 3] を選択します。 ■ [GRE キー]: カプセル化タイプが [GRE] の場合は、GRE キーを指定します。 ■ [ERSPAN ID]: カプセル化タイプが [ERSPAN 2] または [ERSPAN 3] の場合は、ERSPAN ID を指定します。
論理 SPAN	<ul style="list-style-type: none"> ■ [方向]: [双方向]、[入力方向]、または [出力方向] を選択します。 ■ [スナップの長さ]: パケットからキャプチャするバイト数を指定します。

- 6 [送信元] 列の [設定] をクリックして、宛先を設定します。

論理 SPAN の場合、使用可能な送信元は [セグメント ポート]、[仮想マシンのグループ]、[仮想ネットワーク インターフェイスのグループ] です。

リモート L3 SPAN の場合、使用可能な送信元は [セグメント]、[セグメント ポート]、[仮想マシンのグループ]、[仮想ネットワーク インターフェイスのグループ] です。

- 7 [宛先] 列の [設定] をクリックして、宛先を設定します。
- 8 [保存] をクリックします。

簡易ネットワーク管理プロトコル (SNMP)

簡易ネットワーク管理プロトコル (SNMP) を使用して、NSX-T Data Center コンポーネントをモニタリングできます。デフォルトでは、インストール後に SNMP サービスは開始しません。

手順

- 1 NSX Manager CLI または NSX Edge CLI にログインします。
- 2 次のコマンドを実行します。

- SNMPv1/SNMPv2 の場合：

```
set snmp community <community-string>
start service snmp
```

community-string の文字数の上限は 64 です。

- SNMPv3 の場合

```
set snmp v3-users <user_name> auth-password <auth_password> priv-password
<priv_password>

start service snmp
```

user_name の文字数の上限は 32 です。パスワードが PAM の制約を満たしていることを確認します。デフォルトのエンジン ID を変更する場合は、次のコマンドを使用します。

```
set snmp v3-engine-id <v3-engine-id>

start service snmp
```

v3-engine-id は、10 ～ 64 文字の 16 進数から構成される文字列です。

NSX-T Data Center は、認証とプライバシーのプロトコルとして SHA1 と AES128 をサポートします。API 呼び出しを使用して SNMPv3 を設定することもできます。詳細については、『NSX-T Data Center API ガイド』を参照してください。

例：

vRealize Log Insight によるシステムの監視

Log Insight NSX-T コンテンツ パックを使用して、NSX-T Data Center 環境を監視できます。

このコンテンツ パックには次のアラートがあります。

アラート名	説明
SysCpuUsage	CPU 使用率が 10 分以上 95% を超えています。
SysMemUsage	メモリ使用量が 10 分以上 95% を超えています。
SysDiskUsage	1 つ以上のパーティションのディスク使用率が 10 分以上 89% を超えています。
PasswordExpiry	アプライアンスのユーザー アカウントのパスワードがまもなく期限切れになるのか、すでに期限切れになっています。
CertificateExpiry	1 つ以上の CA 署名証明書が期限切れになっています。
ClusterNodeStatus	ローカル Edge クラスター ノードが停止しています。

アラート名	説明
BackupFailure	NSX でスケジューリングされたバックアップ処理が失敗しました。
VipLeadership	NSX 管理クラスタの VIP が停止しています。
ApiRateLimit	クライアント API が、設定されたしきい値に達しました。
CorfuQuorumLost	クラスタ内で 2 台のノードが停止し、corfu クォーラムが失われました。
DfwHeapMem	DFW ヒープ メモリが、設定されたしきい値を超えました。
ProcessStatus	重要なプロセスの状態が変更されました。
ClusterFailoverStatus	SR 高可用性状態が変更されたか、アクティブ/スタンバイサービスがフェイルオーバーされました。
DhcpPoolUsageOverloadedEvent	DHCP プールが、設定された使用率のしきい値に達しました。
FabricCryptoStatus	Known_Answer_Tests (KAT) が失敗したため、Edge 暗号化 MUX ドライバが停止しています。
VpnTunnelState	VPN トンネルが停止しています。
BfdTunnelStatus	BFD トンネルの状態が変更されました。
RoutingBgpNeighborStatus	BGP ネイバーが停止状態になっています。
VpnL2SessionStatus	L2 VPN セッションが停止しています。
VpnIkeSessionStatus	IKE セッションが停止しています。
RoutingStatus	ルーティング (BGP/BFD) が停止しています。
DnsForwarderStatus	DNS フォワーダの実行が停止状態になっています。
TnConnDown_15min	トランスポート ノードからコントローラ/マネージャへの接続が 15 分以上停止しています。
TnConnDown_5min	トランスポート ノードからコントローラ/マネージャへの接続が 5 分以上停止しています。
ServiceDown	1 つ以上のサービスが停止しています。
IpNotAvailableInPool	プール内に使用可能な IP アドレスがないか、設定されたしきい値に達しています。
LoadBalancerError	NSX ロード バランサ サービスがエラー状態になっています。
LoadBalancerDown	NSX ロード バランサ サービスが停止状態になっています。
LoadBalancerVsDown	VS の状態：すべてのプール メンバーが停止しています。
LoadBalancerPoolDown	プールの状態：すべてのプール メンバーが停止しています。
ProcessCrash	データベースまたは他の LB プロセス（ディスパッチャなど）で、プロセスまたはデーモンがクラッシュしています。

vRealize Operations Manager によるシステムの監視

vRealize Operations Manager を使用して、NSX-T Data Center 環境を監視できます。

表 12-1. NSX-T 管理パックのアラート

アラート	説明	推奨
NSX-T 管理サービスが失敗しました	NSX-T Data Center ホストの管理サービスが実行されていないときにトリガされます。	NSX-T Manager にログインして、失敗した管理サービスを再起動してください。
論理スイッチの管理状態が稼動中ではありません	論理スイッチの管理状態が無効になるとトリガされます。	NSX-T にログインして、必要に応じて管理状態を有効にしてください。
Edge ノードのコントローラ/マネージャ接続が接続中ではありません	NSX-T Data Center で Edge ノードの接続状態が停止になるとトリガされます。	Edge ノードと Controller クラスタおよび Manager クラスタとの接続状態を確認し、切断された接続を修正してください。
Edge ホスト ノードが失敗/エラー状態です	次のいずれかの理由で NSX-T Data Center のホスト ノードがエラー状態または失敗状態になるとトリガされます。 <ul style="list-style-type: none"> ■ Edge 構成エラー ■ インストールの失敗 ■ アンインストールの失敗 ■ アップグレードの失敗 ■ 仮想マシンの展開の失敗 ■ 仮想マシンのパワーオフの失敗 ■ 仮想マシンのパワーオンの失敗 ■ 仮想マシンの展開解除の失敗 	Edge ホスト ノードが失敗またはエラー状態です。ホスト ノードの状態を確認して、問題を修正してください。
BFD サービスが無効になっています	論理ルーターで BFD サービスが有効になっていないとトリガされます。	ネイバーが設定されていますが、Tier-O ルーターの BFD サービスが有効になっていません。必要であれば、BFD サービスを有効にしてください。
NAT ルールが構成されていません	論理ルーターの NAT ルールが構成されていなかったとトリガされます。	NSX-T Manager にログインし、論理ルーターに NAT ルールを追加してください。
スタティック ルートが構成されていません	論理ルーターのスタティック ルートが構成されていなかったとトリガされます。	NSX-T Manager にログインし、必要であれば論理ルーターにスタティック ルートを追加してください。
ルート アドバタイズメント サービスが無効になっています	論理ルーターでルート アドバタイズ サービスが有効になっていないとトリガされます。	ルート アドバタイズが設定されていますが、Tier-1 ルーターのルート アドバタイズ サービスが有効になっていません。NSX-T Manager にログインして、サービスを有効にしてください。
ルート再配布サービスが無効になっています	論理ルーターでルート再配布サービスが有効になっていないとトリガされます。	ルート再配布ルールが設定されていますが、Tier-O ルーターのルート再配布サービスが有効になっていません。NSX-T Manager にログインして、サービスを有効にしてください。

表 12-1. NSX-T 管理パックのアラート（続き）

アラート	説明	推奨
論理ルーターの ECMP サービスが無効になっています	論理ルーターで ECMP サービスが有効になっていないとトリガされます。	ネイバーが設定されていますが、Tier-0 ルーターの BGP ECMP サービスが有効になっていません。NSX-T Manager にログインして、サービスを有効にしてください。
コントローラ ノード接続が切断されています	NSX-T Data Center でコントローラ ノードの接続が停止状態になるとトリガされます。	NSX-T Manager にログインして、管理ノードおよび Controller クラスタとコントローラ ノードの接続を確認し、切断状態を解決してください。
展開されているコントローラ ノードは 3 つ未満です	NSX-T Data Center サーバに展開されているコントローラ ノードが 3 台未満の場合にトリガされます。	クラスタに 3 台以上のコントローラ ノードを展開してください。
Controller クラスタの状態が安定していません	NSX-T Data Center のすべてのコントローラ ノードが停止するとトリガされます。	Controller クラスタの状態を確認してください。
管理状態が安定していません	管理クラスタのいずれかのノードが停止状態になるとトリガされます。	管理クラスタの状態を確認してください。
ファイル システムの使用量が 85% を超えています	コントローラ仮想マシンのゲスト ファイル システムの使用量が 85% を超えるとトリガされます。	ファイル システムの使用量が 85% を超えています。ファイル システムを確認してクリーンアップを行い、空き容量を増やしてください。
ファイル システムの使用量が 75% を超えています	コントローラ仮想マシンのゲスト ファイル システムの使用量が 75% を超えるとトリガされます。	ファイル システムの使用量が 75% を超えています。ファイル システムを確認してクリーンアップを行い、空き容量を増やしてください。
ファイル システムの使用量が 70% を超えています	コントローラ仮想マシンのゲスト ファイル システムの使用量が 70% を超えるとトリガされます。	ファイル システムの使用量が 70% を超えています。ファイル システムを確認してクリーンアップを行い、空き容量を増やしてください。
Edge クラスタの状態がダウンになっています	Edge クラスタが停止状態になるとトリガされます。	Edge クラスタの状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
論理スイッチの状態が失敗しました	論理スイッチの状態が失敗になるとトリガされます。	論理スイッチの状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
ロード バランサ サービスの動作状態が停止	ロード バランサ サービスの動作が停止状態になるとトリガされます。	ロード バランサ サービスの動作状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。

表 12-1. NSX-T 管理パックのアラート（続き）

アラート	説明	推奨
ロード バランサ サービスの動作状態がエラー	ロード バランサ サービスの動作状態がエラーになるとトリガされます。	ロード バランサ サービスの動作状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
ロード バランサ仮想サーバの動作状態が停止	ロード バランサ仮想サーバの動作が停止状態になるとトリガされます。	ロード バランサ仮想サーバの動作状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
ロード バランサ仮想サーバの動作状態が分離	ロード バランサ仮想サーバの動作が分離状態になるとトリガされます。	ロード バランサ仮想サーバの動作状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
Edge ノードの構成状態が失敗しました	Edge ノードの構成状態が失敗になるとトリガされます。	Edge ノードの構成状態を確認してください。必要に応じて、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
管理サービスの監視ランタイム状態が失敗しました	管理サービスの監視ランタイムが停止状態になるとトリガされます。	NSX-T Manager 仮想アプライアンスにログインして、失敗した管理サービスを再起動してください。
管理クラスタの管理状態が安定していません	管理クラスタの管理状態が不安定になるとトリガされます。	管理クラスタの状態を確認してください。
展開されているマネージャ ノードは 3 台未満です	NSX-T サーバに展開されているマネージャ ノードが 3 台未満の場合にトリガされます。	クラスタに 3 台以上のマネージャ ノードを展開してください。
マネージャ ノード接続が切断されています	マネージャ ノードのマネージャの接続が停止状態になるとトリガされます。	NSX-T Manager にログインして、マネージャ ノードのマネージャ接続を確認し、NSX-T および VMware のドキュメントで推奨されている標準的なトラブルシューティング手順に従ってください。
マネージャ ノードのファイル システムの使用量が 85% を超えています	マネージャ ノードのゲスト ファイル システムの使用量が 85% を超えるとトリガされます。	ファイル システムの使用量が 85% を超えています。ファイル システムを確認してクリーンアップを行い、空き容量を増やしてください。

表 12-1. NSX-T 管理パックのアラート（続き）

アラート	説明	推奨
マネージャ ノードのファイル システムの使用量が 75% を超えています	マネージャ ノードのゲスト ファイル システムの使用量が 75% を超えるとトリガされます。	ファイル システムの使用量が 75% を超えています。ファイル システムを確認してクリーンアップを行い、空き容量を増やしてください。
マネージャ ノードのファイル システムの使用量が 70% を超えています	マネージャ ノードのゲスト ファイル システムの使用量が 70% を超えるとトリガされます。	ファイル システムの使用量が 70% を超えています。ファイル システムを確認してクリーンアップを行い、空き容量を増やしてください。

vRealize Network Insight Cloud によるシステムの監視

vRealize Network Insight Cloud を使用して、NSX-T Data Center 環境を監視できます。

表 12-2. vRealize Network Insight で計算された NSX-T イベント

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	NSX-T Tier-1 論理ルーターの切断イベント	NSX-T Tier-1 論理ルーターが Tier-0 ルーターから切断されています。このルーターの下位のネットワークに外部からアクセスすることはできません。また、その逆方向にアクセスすることもできません。
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	ルーティングのアドバタイズが無効です	NSX-T Tier-1 論理ルーターでルーティングのアドバタイズが無効になっています。このルーターの下位のネットワークには外部からアクセスできません。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	重大	NSX-T Edge ノードにマネージャが接続されていません	NSX-T Edge ノードにマネージャが接続されていません。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge ノードのコントローラの接続が低下しました	NSX-T Edge ノードが 1 台以上のコントローラと通信できません。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	重大	NSX-T Edge ノードにコントローラが接続されていません	NSX-T Edge ノードは、どのコントローラとも通信できません。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtumismatchEvent	警告	NSX-T Tier-0 とアップリンク スイッチ / ルーター間で MTU が一致しません	Tier-0 論理ルーターのインターフェイスに設定された MTU が、同じ L2 ネットワーク内のアップリンク スイッチ / ルーターのインターフェイスと一致しません。これは、ネットワークのパフォーマンスに影響を与える可能性があります。
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	情報	1 台以上の仮想マシンが NSX-T DFW ファイアウォールから除外されました。	NSX-T DFW ファイアウォールで保護されていない仮想マシンが 1 台以上あります。vRealize Network Insight は、これらの仮想マシンの IPFIX フローを受信しません。
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	警告	アップリンク VLAN の設定が正しくありません	Tier-0 ルーターのアップリンク ポートの VLAN が外部ゲートウェイの VLAN と異なるため、通信は中断されます。
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	トランスポート ノードに接続されているトランスポート ゾーンがありません。	トランスポート ノードに接続されたトランスポート ゾーンがありません。これが原因で、仮想マシンは接続に失敗した可能性があります。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	トランスポート ノードで使用できる VTEP がありません。	すべての VTEP がトランスポート ノードから削除されています。これが原因で、仮想マシンは接続に失敗した可能性があります。
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	重大	NSX-T コントローラ ノードにコントロール クラスタが接続されていません	NSX-T コントローラ ノードでコントロール クラスタへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	重大	NSX-T コントローラ ノードに管理プレーンが接続されていません	NSX-T コントローラ ノードで管理プレーンへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	重大	NSX-T 管理ノードに管理クラスタが接続されていません	NSX-T 管理ノードで管理クラスタへの接続が失われました。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	警告	NSX-T ホスト ノードにマネージャが接続されていません	ホスト トランスポート ノードと NSX Manager の接続状態の同期が失われました
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlrConnectivityStatusUnknownEvent	重大	NSX-T Edge ノードのコントローラ接続が不明です。	NSX-T Edge ノードのコントローラ接続が不明です。
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlrConnectivityStatusDownEvent	警告	NSX-T ホスト ノードにコントローラが接続されていません	NSX-T ホスト ノードは、どのコントローラとも通信できません。
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlrConnectivityStatusDegradedEvent	警告	NSX-T ホスト ノードのコントローラの接続が低下しました	NSX-T ホスト ノードが 1 台以上のコントローラと通信できません。
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlrConnectivityStatusUnknownEvent	警告	NSX-T ホスト ノードのコントローラ接続が不明です。	NSX-T ホスト ノードのコントローラ接続が不明です。
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC の状態が「切断」です。	NSX-T ホスト トランスポート ノードの物理 NIC の状態が「切断」です。
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC の状態が「劣化」です	NSX-T ホスト トランスポート ノードの物理 NIC の状態が「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC の状態が「不明」です。	NSX-T ホスト トランスポート ノードの物理 NIC の状態が「不明」です。
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	重大	NSX-T Edge トランスポート ノードの物理 NIC の状態が「切断」です。	NSX-T Edge トランスポート ノードの物理 NIC の状態が「切断」です。
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	重大	NSX-T Edge トランスポート ノードの物理 NIC の状態が「劣化」です。	NSX-T Edge トランスポート ノードの物理 NIC の状態が「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	重大	NSX-T Edge トランスポート ノードの物理 NIC の状態が「不明」です。	NSX-T Edge トランスポート ノードの物理 NIC の状態が「不明」です。
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	警告	NSX-T ホスト トランスポート ノードのトンネルの状態が「停止」です。	NSX-T ホスト トランスポート ノードのトンネルの状態が「停止」です。
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードのトンネルの状態が「劣化」です。	NSX-T ホスト トランスポート ノードのトンネルの状態が「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードのトンネルの状態が「不明」です。	NSX-T ホスト トランスポート ノードのトンネルの状態が「不明」です。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	重大	NSX-T Edge トランスポート ノードのトンネルの状態が「停止」です。	NSX-T Edge トランスポート ノードのトンネルの状態が「停止」です。
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradeEvent	重大	NSX-T Edge トランスポート ノードのトンネルの状態が「劣化」です。	NSX-T Edge トランスポート ノードのトンネルの状態が「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	重大	NSX-T Edge トランスポート ノードのトンネルの状態が「不明」です。	NSX-T Edge トランスポート ノードのトンネルの状態が「不明」です。
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	警告	NSX-T ホスト トランスポート ノードの状態が「切断」です。	NSX-T ホスト トランスポート ノードの状態が「切断」です。
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードの状態が「劣化」です。	NSX-T ホスト トランスポート ノードの状態が「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードの状態が「不明」です。	NSX-T ホスト トランスポート ノードの状態が「不明」です。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	重大	NSX-T Edge トランスポート ノードの状態が「切断」です。	NSX-T Edge トランスポート ノードの状態が「切断」です。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	重大	NSX-T Edge トランスポート ノードの状態が「劣化」です。	NSX-T Edge トランスポート ノードの状態が「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	重大	NSX-T Edge トランスポート ノードの状態が「不明」です。	NSX-T Edge トランスポート ノードの状態が「不明」です。
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	警告	NSX-T 論理スイッチの管理状態が「切断」です	NSX-T 論理スイッチの管理状態が「切断」です
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	重大	NSX-T 論理ポートの動作状態が「切断」です	NSX-T 論理ポートの動作状態が「切断」です。これにより、同じ論理スイッチに接続された 2 つの仮想インターフェイス (VIF) 間で、仮想マシンから別の仮想マシンに ping を実行できなくなるなどの通信障害が発生する可能性があります。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	警告	NSX-T 論理ポートの動作状態が「不明」です	NSX-T 論理ポートの動作状態が「不明」です。これにより、同じ論理スイッチに接続された 2 つの仮想インターフェイス (VIF) 間で、仮想マシンから別の仮想マシンに ping を実行できなくなるなどの通信障害が発生する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	警告	NSX-T コンピュート マネージャの接続状態が接続中ではありません	NSX-T コンピュート マネージャの接続状態が接続中ではありません
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackUpDisabledEvent	警告	NSX-T Manager のバックアップがスケジュール設定されていません。	NSX-T Manager のバックアップがスケジュール設定されていません
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	重大	NSX-T DFW ファイアウォールが無効になっています。	分散ファイアウォールが NSX-T Manager で無効になっています
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	NSX-T 論理ポートで受信パケットがドロップされています。	NSX-T 論理ポートで受信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	警告	NSX-T 論理ポートで送信パケットがドロップされています。	NSX-T 論理ポートで送信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	警告	NSX-T 論理スイッチで受信パケットがドロップされています	NSX-T 論理スイッチで受信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	警告	NSX-T 論理スイッチで送信パケットがドロップされています	NSX-T 論理スイッチで送信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	NSX-T 管理ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T 管理ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは NSX-T 管理クラスタに関連するネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	重大	NSX-T Edge ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T Edge ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは、Edge クラスタのネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	警告	NSX-T ホスト ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T ホスト ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは ESXi ホストのネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	警告	NSX-T 管理ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T 管理ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは NSX-T 管理クラスタに関連するネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	重大	NSX-T Edge ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T Edge ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは、Edge クラスタのネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	警告	NSX-T ホスト ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T ホスト ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは ESXi ホストのネットワークトラフィックに影響する可能性があります。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	警告	CM インベントリ サービスが実行を停止しました	CM インベントリ サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	警告	コントローラ サービスが実行を停止しました。	コントローラ サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	警告	データストア サービスが実行を停止しました。	データストア サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	警告	HTTP サービスが実行を停止しました。	HTTP サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	警告	アップグレード インストール サービスが実行を停止しました。	アップグレード インストール サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	警告	Liagent サービスが実行を停止しました。	Liagent サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	警告	マネージャ サービスが実行を停止しました。	マネージャ サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatusEvent	警告	管理プレーン サービスが実行を停止しました。	管理サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinatorStatusEvent	警告	移行コーディネータ サービスが実行を停止しました。	移行コーディネータ サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEvent	警告	ノード管理サービスが実行を停止しました。	ノード管理サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	警告	ノード統計サービスが実行を停止しました。	ノード統計サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	警告	メッセージ バス サービスが実行を停止しました。	メッセージ バス クライアント サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	警告	プラットフォーム クライアント サービスが実行を停止しました。	プラットフォーム クライアント サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	警告	エージェント アップグレード サービスが実行を停止しました。	アップグレード サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	警告	NTP サービスが実行を停止しました。	NTP サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	警告	ポリシー サービスが実行を停止しました。	ポリシー サービスの状態が停止になりました。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	警告	検索サービスが実行を停止しました。	検索サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP サービスが実行を停止しました。	SNMP サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	警告	SSH サービスが実行を停止しました。	SSH サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	警告	Syslog サービスが実行を停止しました。	Syslog サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	テレメトリ サービスが実行を停止しました。	テレメトリ サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	警告	UI サービスが実行を停止しました。	UI サービスの状態が停止になりました。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	重大	CM インベントリ サービスが停止しました	NSX-T 管理ノードのサービスの1つである CM インベントリ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	重大	コントローラ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるコントローラ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	重大	データストア サービスが停止しました	NSX-T 管理ノードのサービスの1つであるデータストア サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	重大	HTTP サービスが停止しました	NSX-T 管理ノードのサービスの1つである HTTP サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	警告	インストール アップグレード サービスが停止しました	NSX-T 管理ノードのサービスの1つであるインストール アップグレード サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	警告	Liagent サービスが停止しました	NSX-T 管理ノードのサービスの1つである LI エージェント サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	重大	マネージャ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるマネージャ サービスが実行を停止しました。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	警告	管理プレーン サービスが 停止しました	NSX-T 管理ノードのサー ビスの1つである管理プ レーン バス サービスが実 行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	警告	移行コーディネータ サー ビスが停止しました	NSX-T 管理ノードのサー ビスの1つである移行コ ーディネータ サービスが 実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEve nt	重大	ノード管理サービスが停 止しました	NSX-T 管理ノードのサー ビスの1つであるノード 管理サービスが実行を停 止しました。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEven t	重大	ノード統計サービスが停 止しました	NSX-T 管理ノードのサー ビスの1つであるノード 統計サービスが実行を停 止しました。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStat usEvent	警告	メッセージ バス サービス が停止しました	NSX-T 管理ノードのサー ビスの1つであるメッセ ージ バス サービスが実行 を停止しました。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientSta tusEvent	重大	プラットフォーム クライ アント サービスが停止し ました	NSX-T 管理ノードのサー ビスの1つであるブラッ トフォーム クライアント サービスが実行を停止し ました。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentSt atusEvent	警告	アップグレード エージェ ント サービスが停止しま した	NSX-T 管理ノードのサー ビスの1つ（アップグレー ド エージェント サービ ス）が停止しました。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	重大	NTP サービスが停止しま した	NSX-T 管理ノードのサー ビスの1つである NTP サービスが実行を停止し ました。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	重大	ポリシー サービスが停止 しました	NSX-T 管理ノードのサー ビスの1つであるポリシ ー サービスが実行を停止 しました。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	重大	検索サービスが停止しま した	NSX-T 管理ノードのサー ビスの1つである検索サ ービスが実行を停止しま した。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP サービスが停止し ました	NSX-T 管理ノードのサー ビスの1つである SNMP サービスが実行を停止し ました。

表 12-2. vRealize Network Insight で計算された NSX-T イベント（続き）

OID	イベント名	デフォルトの重要度	UI 名	説明
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	重大	SSH サービスが停止しました	NSX-T 管理ノードのサービスの 1 つである SSH サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	重大	Syslog サービスが停止しました	NSX-T 管理ノードのサービスの 1 つである Syslog サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	テレメトリ サービスが停止しました	NSX-T 管理ノードのサービスの 1 つであるテレメトリ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	重大	UI サービスが停止しました	NSX-T 管理ノードのサービスの 1 つである UI サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	重大	クラスタ マネージャ サービスが停止しました	NSX-T 管理ノードのサービスの 1 つであるクラスタ マネージャ サービスが実行を停止しました。

NSX-T システム イベント

vRealize Network Insight でサポートされている NSX-T 2.2 ～ 2.5 のイベントは次のとおりです。これらの NSX-T システム イベントのオブジェクト ID (OID) は 1.3.6.1.4.1.6876.100.1.0.80203 です。

表 12-3. NSX-T システム イベント

イベント名	説明
vmwNSXPlatformSysCpuUsage	マネージャと Edge アプライアンスの両方の CPU 使用率 (NSX-T 2.2)。
vmwNSXPlatformSysDiskUsage	マネージャと Edge アプライアンスの両方のディスク容量使用率 (/var/log パーティション) (NSX-T 2.2)。
vmwNSXPlatformSysMemUsage	マネージャと Edge アプライアンスの両方のメモリ使用率 (NSX-T 2.2)。
vmwNSXPlatformSysConfigDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/config パーティション) (NSX-T 2.4)。
vmwNSXPlatformSysVarDumpDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/var/dump パーティション) (NSX-T 2.5)。
vmwNSXPlatformSysRepositoryDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/repository パーティション) (NSX-T 2.5)。
vmwNSXPlatformSysRootDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (ルート パーティション) (NSX-T 2.5)。

表 12-3. NSX-T システム イベント （続き）

イベント名	説明
vmwNSXPlatformSysTmpDiskUsage	マネージャと Edge アプライアンスのディスク使用率（tmp パーティション）（NSX-T 2.5）。
vmwNSXPlatformSysImageDiskUsage	マネージャと Edge アプライアンスのディスク使用率（/image パーティション）（NSX-T 2.5）。
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP プールの overloaded/normal（NSX-T 2.5）。
vmwNSXDhcpPoolLeaseAllocationFailedEvent	DHCP プールのリース割り当て失敗/成功（NSX-T 2.5）。
vmwNSXPlatformPasswordExpiryStatus	マネージャのパスワード期限切れ（NSX-T 2.4）。
vmwNSXPlatformCertificateExpiryStatus	マネージャの証明書期限切れ（NSX-T 2.4）。
vmwNSXRoutingBgpNeighborStatus	BGP ネイバーの状態（NSX-T 2.2）。
vmwNSXVpnTunnelState	VPN トンネルが動作/停止（NSX-T 2.2）。
vmwNSXVpnL2TunnelStatus	L2 VPN セッションが動作/停止（NSX-T 2.2）。
vmwNSXVpnIkeSessionStatus	IKE セッションが動作/停止（NSX-T 2.2）。
vmwNSXDnsForwarderStatus	DNS フォワーダの状態（NSX-T 2.4）。
vmwNSXClusterNodeStatus	クラスタ ノードの状態（NSX-T 2.4）。
vmwNSXFabricCryptoStatus	Edge 暗号化 MUX ドライバが Known_Answer_Tests (KAT) に失敗/合格（NSX-T 2.4）。
マネージャのディスク使用率が良好ではありません	
BGP ネイバーが停止しています	BGP ネイバーが停止している場合はアラートが必要です。
BGP ネイバーが動作しています	ネイバーが起動するときに、アラームをクリアします。
ストレージ使用率が X を超過	ストレージのアラームが X を超過 - すべてのアプライアンス仮想マシン（MP、CCP）またはトランスポート ノード（Edge、ホスト）でイベントが発生します。
メモリ使用率が X を超過	メモリのアラームが X を超過 - すべてのアプライアンス仮想マシン（MP、CCP）またはトランスポート ノード（Edge、ホスト）でイベントが発生します。
CPU 使用率が X を超過	CPU のアラームが X を超過 - すべてのアプライアンス仮想マシン（MP、CCP）またはトランスポート ノード（Edge、ホスト）でイベントが発生します。

高度な監視ツール

NSX-T は、ポート接続の表示、トレースフロー、ポート ミラーリング、アクティビティ モニタリングなど、高度な監視方法をサポートしています。

ポート接続情報の表示

ポート接続ツールを使用して、2 台の仮想マシン間の接続状態を迅速に視覚化し、トラブルシューティングを実行できます。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に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 [ネットワークとセキュリティの詳細設定] - [ツール] - [ポート接続] 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。

トレースフロー

トレースフローを使用すると、ネットワークにパケットを挿入し、ネットワーク全体のフローを監視できます。このフローにより、ネットワークを監視し、ボトルネックや中断などの問題を特定できます。

トレースフローにより、パケットが宛先に到達するまでに経由する 1 つ以上のパスを特定できます。つまり、逆にパケットが途中でドロップされた場所を特定することができます。エンティティごとに入出力のパケット処理が報告されるため、パケットの受信時に問題が発生したのか、パケットの転送時に問題が発生したのかがわかります。

トレースフローは、ゲスト仮想マシンのスタック間でやりとりされる ping の要求/応答と同じではないことに留意してください。トレースフローでは、オーバーレイ ネットワークを移動するマーク付きのパケットを監視します。オーバーレイ ネットワークを移動するパケットを宛先のゲスト仮想マシンまたは Edge アップリンクに配信されるまで監視します。挿入されたマーク付きのパケットは、実際には宛先ゲスト仮想マシンに配信されません。

トレースフローは、トランスポート ノードで使用できます。ICMP、TCP、UDP、DHCP、DNS、ARP/NDP など、IPv4 と IPv6 の両方のプロトコルをサポートします。

カスタム ヘッダ フィールドやパケット サイズを指定してパケットを構築できます。トレースフローの送信元または宛先には、論理スイッチポート、論理ルーターのアップリンク ポート、CSP、DHCP ポートなどになります。ターゲット エンドポイントは、NSX オーバーレイまたはアンダーレイの任意のデバイスにすることができます。ただし、NSX Edge ノードのアップリンクの先にある宛先を選択することはできません。宛先は、同じサブネット上に存在しているか、または NSX 分散論理ルーターを経由して到達できる必要があります。

NSX ブリッジが設定されている場合、未知の宛先 MAC アドレスを持つパケットは常にブリッジに送信されます。通常、ブリッジはこれらのパケットを VLAN に転送し、トレースフロー パケットを送信済みとして報告します。パケットが配信済みと報告されたからといって、必ずしもトレース パケットが指定された宛先に配信されたことを意味するわけではありません。

トレースフローの観察では、ブロードキャストされたトレースフロー パケットが対象に含まれることがあります。ESXi ホストは、宛先ホストの MAC アドレスが不明な場合にトレースフロー パケットをブロードキャストします。ブロードキャスト トラフィックの場合、ソースは仮想マシン vNIC になります。ブロードキャスト トラフィックのレイヤー 2 ターゲット MAC アドレスは FF:FF:FF:FF:FF:FF です。ファイアウォール検査の有効なパケットを作成するために、ブロードキャスト トレースフロー操作では、サブネット プリフィックスの長さが必要になります。サブネット マスクにより、NSX はパケットの IP ネットワーク アドレスを計算できます。

トレースフローによるパケットのパスのトレース

パケットのパスを調べるには、トレースフローを使用します。トレースフローは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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ツール] - [トレースフロー] の順に選択します。
- 3 IPv4 または IPv6 のアドレスを選択します。
- 4 トラフィック タイプを選択します。

IPv4 アドレスの場合、トラフィック タイプの選択肢はユニキャスト、マルチキャスト、ブロードキャストです。

IPv6 アドレスの場合、トラフィック タイプの選択肢はユニキャストまたはマルチキャストです。

注：VMware Cloud (VMC) 環境では、マルチキャストとブロードキャストはサポートされません。

5 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	宛先
ユニキャスト	<p>仮想マシンまたは論理ポートを選択します。仮想マシンの場合：</p> <ul style="list-style-type: none"> ■ ドロップダウン リストから仮想マシンを選択します。 ■ 仮想インターフェイスを選択します。 ■ 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 リストから 1 つを選択します。 ■ 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>論理ポートの場合：</p> <ul style="list-style-type: none"> ■ 接続の種類を [VIF]、[DHCP]、[Edge アップリンク]、または [Edge 統合サービス] の中から選択します。 ■ ポートを選択します。 	<p>仮想マシン、論理ポート、または IP アドレス/MAC アドレスを選択します。仮想マシンの場合：</p> <ul style="list-style-type: none"> ■ ドロップダウン リストから仮想マシンを選択します。 ■ 仮想インターフェイスを選択します。 ■ 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 リストから 1 つを選択します。 ■ 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>論理ポートの場合：</p> <ul style="list-style-type: none"> ■ 接続の種類を [VIF]、[DHCP]、[Edge アップリンク]、または [Edge 統合サービス] の中から選択します。 ■ ポートを選択します。 <p>IP アドレス/MAC アドレスの場合：</p> <ul style="list-style-type: none"> ■ 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。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。レイヤー 3 の場合は、IP アドレスを入力します。
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。

6 （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。

7 （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	デフォルトは 128 です。
TTL	デフォルトは 64 です。
タイムアウト (ミリ秒)	デフォルトは 10000 です。
Ethertype	デフォルトは 2048 です。
ペイロード タイプ	[Base64]、[16 進数]、[プレーン テキスト]、[バイナリ]、または [10 進数] を選択します。
ペイロード データ	選択したタイプに基づいてフォーマットされたペイロードです。

8 (オプション) プロトコルを選択し、関連情報を入力します。

プロトコル	パラメータ
TCP	送信元ポート、宛先ポート、および TCP フラグを指定します。
UDP	送信元ポートおよび宛先ポートを指定します。
ICMPv6	ICMP ID およびシーケンスを指定します。
ICMP	ICMP ID およびシーケンスを指定します。
DHCPv6	DHCP メッセージタイプを [要請]、[アドバタイズ]、[要求]、または [返信] の中选择します。
DHCP	DHCP OP コードを [起動要求] または [起動応答] の中选择します。
DNS	アドレスを指定して、メッセージタイプを [クエリ] または [応答] の中选择します。

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 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。

論理 SPAN は、オーバーレイ論理スイッチでのみサポートされます。VLAN 論理スイッチには対応していません。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

この機能には次の制限があります。

- ソースのミラー 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。
- 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。
- ローカル SPAN セッションの場合、ミラー セッションの送信元ポートと宛先ポートが同じホスト vSwitch 上にある必要があります。したがって、ソースまたはターゲット 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PMENT キット (DPDK) を使用してパケット処理のパフォーマンスを改善します。

注： モニター仮想マシンの MTU 設定が、パケットの処理に十分な大きさであることを確認します。KVM の場合は、ハイパーバイザーの仮想 NIC デバイスの MTU 設定も確認します。カプセル化によってパケットのサイズが増えるため、パケットをカプセル化する場合は特に重要な作業です。十分な大きさでない場合、パケットがドロップされる可能性があります。これは VMXNET3 NIC を使用する ESXi 仮想マシンの場合は問題ではありませんが、ESXi および KVM 仮想マシンでその他のタイプの NIC を使用する場合は問題となる可能性があります。

注： KVM ホストの仮想マシンを含む L3 ポート ミラーリング セッションでは、MTU サイズを十分に増やして、カプセル化によって必要となる追加容量を処理できるようにする必要があります。ミラートラフィックは、OVS インターフェイスおよび OVS アップリンクを通過します。OVS インターフェイスの MTU は、カプセル化とミラーリング前の元のパケットのサイズより、100 バイト以上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>>) に管理者権限でログインします。
- 2 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。
- 3 [ネットワークとセキュリティの詳細設定] - [ツール] - [ポート ミラーリング セッション] の順に選択します。
- 4 [追加] をクリックし、セッション タイプを選択します。

使用可能なタイプは、[ローカル SPAN]、[リモート SPAN]、[リモート L3 SPAN]、および[論理 SPAN] です。

5 セッションの名前を入力します。必要に応じて説明も入力します。

6 追加のパラメータを指定します。

セッション タイプ	パラメータ
ローカル SPAN	<ul style="list-style-type: none"> ■ [トランスポート ノード] : トランスポート ノードを選択します。 ■ [方向] : [双方向]、[入力方向]、または [出力方向] を選択します。 ■ [パケット切り捨て長] : パケット廃棄の値を選択します。
リモート SPAN	<ul style="list-style-type: none"> ■ [セッション タイプ] : [RSPAN 送信元セッション] または [RSPAN 宛先セッション] を選択します。 ■ [トランスポート ノード] : トランスポート ノードを選択します。 ■ [方向] : [双方向]、[入力方向]、または [出力方向] を選択します。 ■ [パケット切り捨て長] : パケット廃棄の値を選択します。 ■ [VLAN ID のカプセル化] : カプセル化 VLAN ID を指定します。 ■ [元の VLAN の保持] : 元の VLAN ID を保持するかどうかを選択します。
リモート L3 SPAN	<ul style="list-style-type: none"> ■ [カプセル化] : [GRE]、[ERSPAN 2]、または [ERSPAN 3] を選択します。 ■ [GRE キー] : カプセル化が [GRE] の場合は、GRE キーを指定します。[ERSPAN ID] : カプセル化が [ERSPAN 2] または [ERSPAN 3] の場合は、ERSPAN ID を指定します。 ■ [方向] : [双方向]、[入力方向]、または [出力方向] を選択します。 ■ [パケット切り捨て長] : パケット廃棄の値を選択します。
論理 SPAN	<ul style="list-style-type: none"> ■ [論理スイッチ] : 論理スイッチを選択します。 ■ [方向] : [双方向]、[入力方向]、または [出力方向] を選択します。 ■ [パケット切り捨て長] : パケット廃棄の値を選択します。

7 [次へ] をクリックします。

8 ソース情報を指定します。

セッション タイプ	パラメータ
ローカル SPAN	<ul style="list-style-type: none"> ■ N-VDS を選択します。 ■ 物理インターフェイスを選択します。 ■ カプセル化されたパケットを有効または無効にします。 ■ 仮想マシンを選択します。 ■ 仮想インターフェイスを選択します。
リモート SPAN	<ul style="list-style-type: none"> ■ 仮想マシンを選択します。 ■ 仮想インターフェイスを選択します。
リモート L3 SPAN	<ul style="list-style-type: none"> ■ 仮想マシンを選択します。 ■ 仮想インターフェイスを選択します。 ■ 論理スイッチを選択します。
論理 SPAN	<ul style="list-style-type: none"> ■ 論理ポートを選択します。

9 [次へ] をクリックします。

10 ターゲットの情報を指定します。

セッションタイプ	パラメータ
ローカル SPAN	<ul style="list-style-type: none"> ■ 仮想マシンを選択します。 ■ 仮想インターフェイスを選択します。
リモート SPAN	<ul style="list-style-type: none"> ■ N-VDS を選択します。 ■ 物理インターフェイスを選択します。
リモート L3 SPAN	<ul style="list-style-type: none"> ■ IPv4 アドレスを指定します。
論理 SPAN	<ul style="list-style-type: none"> ■ 論理ポートを選択します。

11 [保存] 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は、ソースもターゲットも変更できません。

ポート ミラーリング セッションのフィルタの設定

ポート ミラーリング セッションのフィルタを設定し、ミラー化されたデータ量を制限できます。

この機能には次の機能と制限があります。

- ESXi および KVM ホストのトランスポート ノードのみがサポートされます。
- 送信元と宛先の IP アドレス、IP プレフィックス、および IP 範囲がサポートされます。
- 送信元または宛先の IP セットはサポートされません。
- ESXi または KVM のミラー統計はサポートされません。

API を使用してフィルタを設定する必要があります。NSX Manager ユーザー インターフェイスの使用はサポートされません。ポート ミラーリング API および PortMirroringFilter スキーマの詳細については、『NSX-T Data Center API リファレンス』を参照してください。

手順

- 1 NSX Manager ユーザー インターフェイスまたは API を使用してポート ミラーリング セッションを構成します。
- 2 GET /api/v1/mirror-sessions API を呼び出し、ポート ミラーリング セッションの情報を取得します。
- 3 GET /api/v1/mirror-sessions/<mirror-session-id> API を呼び出し、1 つまたは複数のフィルタを追加します。次はその例です。

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
  "display_name": "port-mirror-session-1",
  "description": "Pnic port mirror session 1",
  "mirror_sources": [
    {
      "resource_type": "LogicalPortMirrorSource",
```

```

    "port_ids": [
      "6a361832-43e4-430d-a48a-b84a6cba73c3"
    ]
  },
  "mirror_destination": {
    "resource_type": "LogicalPortMirrorDestination",
    "port_ids": [
      "3e42e8b2d-3047-4550-b230-dd1ee0e10b34"
    ]
  },
  "port_mirroring_filters": [
    {
      "filter_action": "MIRROR",
      "src_ips": {
        "ip-addresses": [
          "192.168.175.250",
          "2001:bd6::c:2957:160:126"
        ]
      },
      "dst_ips": {
        "ip-addresses": [
          "192.168.160.126",
          "2001:bd6::c:2957:175:250"
        ]
      }
    }
  ],
  "session_type": "LogicalPortMirrorSession",
  "preserve_original_vlan": false,
  "direction": "BIDIRECTIONAL",
  "_revision": 0
}

```

- 4 (オプション) `get mirroring-session <session-number>` CLI コマンドを呼び出すと、フィルタなど、ポート ミラーリング セッションのプロパティを表示できます。

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。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

この機能は、RFC 7011 と RFC 7012 で指定されている標準に準拠しています。

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 Data Center 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 Data Center 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トリーが含まれます。
- 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トリーが含まれます。

スイッチの IPFIX コレクタの設定

スイッチに 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ツール] - [IPFIX] の順に選択します。
- 3 [スイッチの IPFIX コレクタ] タブをクリックします。
- 4 [追加] をクリックして、コレクタを追加します。
- 5 名前を入力します。必要に応じて説明も入力します。
- 6 [追加] をクリックし、IP アドレスとコレクタの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。
- 7 [追加] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ツール] - [IPFIX] の順に選択します。

3 [スイッチの IPFIX 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。 注： グローバル プロファイルを作成する場合は、プロファイルに Global という名前を付ける必要があります。UI からグローバル プロファイルを編集または削除することはできませんが、NSX-T Data Center API を使用すると、このような操作を行うことができます。
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パケットを受信中の場合でも、フローはタイムアウトになります。デフォルト値は 300 です。
アイドル タイムアウト (秒)	フローと関連付けられているパケットを受信しない場合に、フローがタイムアウトするまでの時間 (秒) を指定します。これは ESXi の場合にのみ有効です。KVM の場合は、アクティブ タイムアウトの値に基づいて、すべてのフローがタイムアウトします。デフォルト値は 300 です。
最大フロー数	ブリッジにキャッシュされるフローの最大数を指定します。KVM の場合にのみ有効です。ESXi では設定できません。デフォルト値は 16384 です。
オーバーレイ フローのエクスポート	サンプルの結果にオーバーレイ フロー情報を含めるかどうかを指定する設定。
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。
観測ドメイン ID	観測ドメイン ID は、ネットワーク フローの送信元である観測ドメインを識別します。特定の観測ドメインがないことを示すには、0 を入力します。
コレクタのプロファイル	前の手順で設定したスイッチ IPFIX コレクタを選択します。
優先順位	このパラメータは、複数のプロファイルを適用する際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。

5 [追加] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ツール] - [IPFIX] の順に選択します。
- 3 [ファイアウォールの IPFIX コレクタ] タブをクリックします。
- 4 [追加] をクリックして、コレクタを追加します。
- 5 名前を入力します。必要に応じて説明も入力します。
- 6 [追加] をクリックし、IP アドレスとコレクタの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。

7 [追加] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ツール] - [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] タブをクリックします。
- 4 [追加] 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。 注： グローバル プロファイルを作成する場合は、プロファイルに Global という名前を付ける必要があります。UI からグローバル プロファイルを編集または削除することはできませんが、NSX-T Data Center API を使用すると、このような操作を行うことができます。
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。
優先順位	このパラメータは、複数のプロファイルを適用する際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。
観測ドメイン ID	このパラメータは、ネットワーク フローの送信元の観測ドメインを特定します。デフォルトは 0 で、特定の観測ドメインを指定しません。

- 5 [追加] をクリックします。

ESXi の IPFIX テンプレート

ESXi ホスト トランスポート ノードは、8 つの論理スイッチ IPFIX フロー テンプレートと 2 つの分散ファイアウォール IPFIX フロー テンプレートをサポートしています

次の表に、論理スイッチ IPFIX パケット内の VMware 固有の要素を示します。

エレメント ID	パラメータ名	データ タイプ	ユニット
880	tenantProtocol	unsigned8	1 バイト
881	tenantSourceIPv4	ipv4Address	4 バイト
882	tenantDestIPv4	ipv4Address	4 バイト
883	tenantSourceIPv6	ipv6Address	16 バイト
884	tenantDestIPv6	ipv6Address	16 バイト
886	tenantSourcePort	unsigned16	2 バイト
887	tenantDestPort	unsigned16	2 バイト
888	egressInterfaceAttr	unsigned16	2 バイト

エレメント ID	パラメータ名	データ タイプ	ユニット
889	vxlanExportRole	unsigned8	1 バイト
890	ingressInterfaceAttr	unsigned16	2 バイト
898	virtualObsID	string	可変長

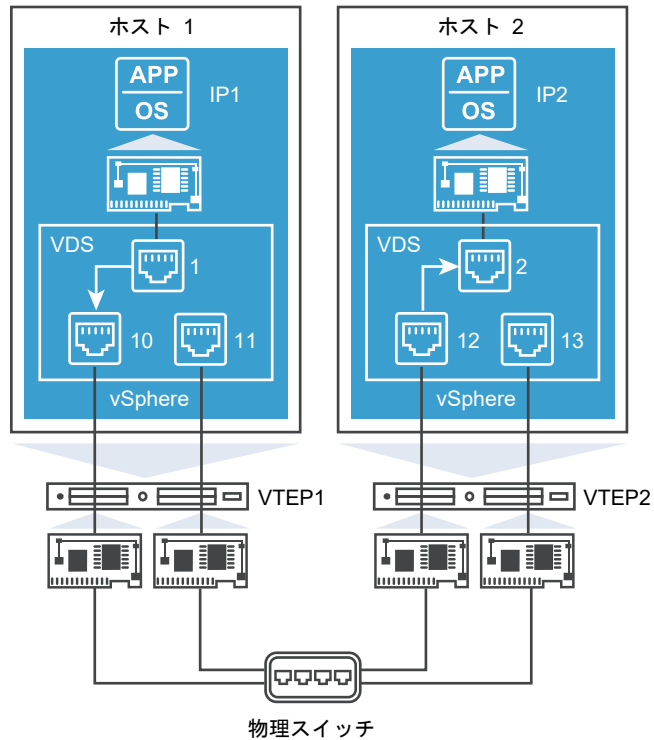
次の表に、分散ファイアウォール IPFIX パケット内の VMware 固有の要素を示します。

エレメント ID	パラメータ名	データ タイプ	ユニット
950	ruleId	unsigned32	4 バイト
951	vmUuid	string	16 バイト
952	vnidIndex	unsigned32	4 バイト
953	sessionFlags	unsigned8	1 バイト
954	flowDirection	unsigned8	1 バイト
955	algControlFlowId	unsigned64	8 バイト
956	algType	unsigned8	1 バイト
957	algFlowType	unsigned8	1 バイト
958	averageLatency	unsigned32	4 バイト
959	retransmissionCount	unsigned32	4 バイト
960	vifUuid	octetArray	16 バイト
961	vifId	string	可変長

ESXi 論理スイッチの IPFIX テンプレート

ESXi ホスト トランスポート ノードは、8 つの論理スイッチ IPFIX フロー テンプレートをサポートしています。

次の図は、IPFIX 機能によってモニタリングされる ESXi ホストに接続された仮想マシン間のトラフィック フローを示しています。



IPv4 のカプセル化テンプレートには次の要素があります。

- 標準的な要素
- SrcAddr : VTEP1
- DstAddr : VTEP2
- tenantSourceIPv4 : IP1
- tenantDestIPv4 : IP2
- tenantSourcePort : 10000
- tenantDestPort : 80
- tenantProtocol : TCP
- ingressInterfaceAttr : 0x03 (トンネル ポート)
- egressInterfaceAttr : 0x01
- encapExportRole : 01
- virtualObsID : 89fd5032-2dc9-4fc3-993a-9bb4b616de54 (論理ポート ID)

IPv4 テンプレート

テンプレート ID : 256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
```

```

IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv4 カプセル化テンプレート

テンプレート ID : 257

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)

```

```
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()
```

IPv4 ICMP テンプレート

テンプレート ID : 258

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()
```

IPv4 ICMP カプセル化テンプレート

テンプレート ID : 259

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
```

```
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv6 テンプレート

テンプレート ID : 260

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS,1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv6 カプセル化テンプレート

テンプレート ID : 261

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
```

```

IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP テンプレート

テンプレート ID : 262

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP カプセル化テンプレート

テンプレート ID : 263

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)

```



```

IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

ESXi 分散ファイアウォール IPFIX テンプレート

ESXi ホスト トランスポート ノードは、2 つの分散ファイアウォール IPFIX フロー テンプレートをサポートしています。

IPv4 テンプレート

テンプレート ID : 288

```

IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv4, 1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv4, 1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds, 4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(firewallEvent, 1)
IPFIX_TEMPLATE_FIELD(direction, 1)
IPFIX_TEMPLATE_FIELD(ruleId, 4)
IPFIX_TEMPLATE_FIELD(vifUuid, 16)
IPFIX_TEMPLATE_FIELD(sessionFlags, 1)
IPFIX_TEMPLATE_FIELD(flowDirection, 1)
IPFIX_TEMPLATE_FIELD(flowId, 8)
IPFIX_TEMPLATE_FIELD(algControlFlowId, 8)
IPFIX_TEMPLATE_FIELD(algType, 1)
IPFIX_TEMPLATE_FIELD(algFlowType, 1)

```

```
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)
```

IPv6 テンプレート

テンプレート ID : 289

```
IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)
```

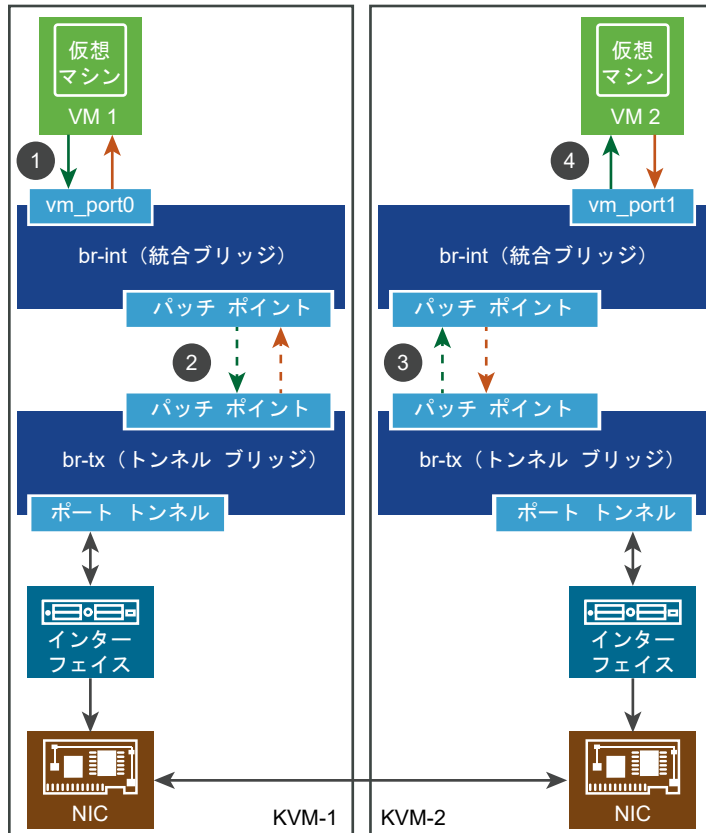
KVM の IPFIX テンプレート

KVM ホスト トランスポート ノードは、88 個の IPFIX フロー テンプレートと 1 つのオプション テンプレートをサポートしています。

次の表に、KVM IPFIX パケット内の VMware 固有の要素を示します。

エレメント ID	パラメータ名	データ タイプ	ユニット
891	tunnelType	unsigned8	1 バイト
892	tunnelKey	バイト数	可変長
893	tunnelSourceIPv4Address	unsigned32	4 バイト
894	tunnelDestinationIPv4Address	unsigned32	4 バイト
895	tunnelProtocolIdentifier	unsigned8	1 バイト
896	tunnelSourceTransportPort	unsigned16	2 バイト
897	tunnelDestinationTransportPort	unsigned16	2 バイト
898	virtualObsID	string	可変長

次の図は、IPFIX 機能によってモニタリングされる KVM ホストに接続された仮想マシン間のトラフィック フローを示しています。



KVM IPv4 IPFIX の入力方向テンプレートには、次の要素があります。

- 標準的な要素
- virtualObsID : 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34 (論理ポート ID)

KVM イーサネットの IPFIX テンプレート

KVM のイーサネットの IPFIX テンプレートは 4 つあります (入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向)。

イーサネットの入力方向

テンプレート ID : 256。フィールド数 : 27。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)

- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

イーサネットの出力方向

テンプレート ID : 257。フィールド数 : 31。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)

- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 8)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

トンネルを使用するイーサネットの入力方向

テンプレート ID : 258。フィールド数 : 34。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)

- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

トンネルを使用するイーサネットの出力方向

テンプレート ID : 259。フィールド数 : 38。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 8)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)

- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

KVM の IPv4 の IPFIX テンプレート

KVM の IPv4 の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 の入力方向

テンプレート ID : 276。フィールド数 : 45。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))

- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv4 の出力方向

テンプレート ID : 277。フィールド数 : 49。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)

- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)

- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 の入力方向

テンプレート ID : 278。フィールド数 : 52。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)

- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)

- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 の出力方向

テンプレート ID : 279。フィールド数 : 56。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))

- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv4 を介した TCP の IPFIX テンプレート

KVM 向けの IPv4 を介した TCP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 を介した TCP の入力方向

テンプレート ID : 280。フィールド数 : 53。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)

- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

IPv4 を介した TCP の出力方向

テンプレート ID : 281。フィールド数 : 57。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)

- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)

- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv4 を介した TCP の入力方向

テンプレート ID : 282。フィールド数 : 60。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)

- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)

- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv4 を介した TCP の出力方向

テンプレート ID : 283。フィールド数 : 64。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)

- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)

- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

KVM 向けの IPv4 を介した UDP の IPFIX テンプレート

KVM 向けの IPv4 を介した UDP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 を介した UDP の入力方向

テンプレート ID : 284。フィールド数 : 47。

フィールドは次のとおりです。

- observationPointId (length : 4)

- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)

- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv4 を介した UDP の出力方向

テンプレート ID : 285。フィールド数 : 51。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)

- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)

- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 を介した UDP の入力方向

テンプレート ID : 286。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))

- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 を介した UDP の出力方向

テンプレート ID : 287。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))

- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv4 を介した SCTP の IPFIX テンプレート

KVM 向けの IPv4 を介した SCTP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 を介した SCTP の入力方向

テンプレート ID : 288。フィールド数 : 47。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)

- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv4 を介した SCTP の出力方向

テンプレート ID : 289。フィールド数 : 51。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)

- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)

- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 を介した SCTP の入力方向

テンプレート ID : 290。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))

- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 を介した SCTP の出力方向

テンプレート ID : 291。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))

- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM の ICMPv4 の IPFIX テンプレート

KVM の ICMPv4 の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

ICMPv4 の入力方向

テンプレート ID : 292。フィールド数 : 47。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)

- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

ICMPv4 の出力方向

テンプレート ID : 293。フィールド数 : 51。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)

- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)

- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv4 の入力方向

テンプレート ID : 294。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))

- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)

- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv4 の出力方向

テンプレート ID : 295。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))

- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM の IPv6 の IPFIX テンプレート

KVM の IPv6 の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 の入力方向

テンプレート ID : 296。フィールド数 : 46。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)

- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv6 の出力方向

テンプレート ID : 297。フィールド数 : 50。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)

- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)

- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 の入力方向

テンプレート ID : 298。フィールド数 : 53。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))

- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)

- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 の出力方向

テンプレート ID : 299。フィールド数 : 57。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))

- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv6 を介した TCP の IPFIX テンプレート

KVM 向けの IPv6 を介した TCP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 を介した TCP の入力方向

テンプレート ID : 300。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)

- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

IPv6 を介した TCP の出力方向

テンプレート ID : 301。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)

- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)

- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv6 を介した TCP の入力方向

テンプレート ID : 302。フィールド数 : 61。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)

- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)

- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv6 を介した TCP の出力方向

テンプレート ID : 303。フィールド数 : 65。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)

- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)

- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

KVM 向けの IPv6 を介した UDP の IPFIX テンプレート

KVM 向けの IPv6 を介した UDP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 を介した UDP の入力方向

テンプレート ID : 304。フィールド数 : 48。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)

- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv6 を介した UDP の出力方向

テンプレート ID : 305。フィールド数 : 52。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)

- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)

- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 を介した UDP の入力方向

テンプレート ID : 306。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)

- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)

- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 を介した UDP の出力方向

テンプレート ID : 307。フィールド数 : 59。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))

- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv6 を介した SCTP の IPFIX テンプレート

KVM 向けの IPv6 を介した SCTP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 を介した SCTP の入力方向

テンプレート ID : 308。フィールド数 : 48。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)

- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv6 を介した SCTP の出力方向

テンプレート ID : 309。フィールド数 : 52。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)

- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)

- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 を介した SCTP の入力方向

テンプレート ID : 310。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)

- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)

- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 を介した SCTP の出力方向

テンプレート ID : 311。フィールド数 : 59。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)

- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)

- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM の ICMPv6 の IPFIX テンプレート

KVM の ICMPv6 の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

ICMPv6 の入力方向

テンプレート ID : 312。フィールド数 : 48。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)

- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMcastOctetTotalCount (length : 8)

ICMPv6 の出力方向

テンプレート ID : 313。フィールド数 : 52。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)

- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)

- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv6 の入力方向

テンプレート ID : 314。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)

- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)

- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv6 の出力方向

テンプレート ID : 315。フィールド数 : 59。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)

- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM のイーサネット VLAN の IPFIX テンプレート

KVM のイーサネット VLAN の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

イーサネット VLAN の入力方向

テンプレート ID : 316。フィールド数 : 30。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)

- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

イーサネット VLAN の出力方向

テンプレート ID : 317。フィールド数 : 34。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 8)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)

- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

トンネルを使用するイーサネット VLAN の入力方向

テンプレート ID : 318。フィールド数 : 37。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)

- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

トンネルを使用するイーサネット VLAN の出力方向

テンプレート ID : 319。フィールド数 : 41。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)

- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 8)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)

- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

KVM の IPv4 VLAN の IPFIX テンプレート

KVM の IPv4 VLAN の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 VLAN の入力方向

テンプレート ID : 336。フィールド数 : 48。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)

- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv4 VLAN の出力方向

テンプレート ID : 337。フィールド数 : 52。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)

- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 VLAN の入力方向

テンプレート ID : 338。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)

- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)

- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMcastOctetTotalCount (length : 8)

トンネルを使用する IPv4 VLAN の出力方向

テンプレート ID : 339。フィールド数 : 59。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)

- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)

- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv4 VLAN を介した TCP の IPFIX テンプレート

KVM 向けの IPv4 VLAN を介した TCP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 VLAN を介した TCP の入力方向

テンプレート ID : 340。フィールド数 : 56。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)

- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)

- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

IPv4 VLAN を介した TCP の出力方向

テンプレート ID : 341。フィールド数 : 60。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)

- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)

- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMcastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv4 VLAN を介した TCP の入力方向

テンプレート ID : 342。フィールド数 : 63。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)

- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)

- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv4 VLAN を介した TCP の出力方向

テンプレート ID : 343。フィールド数 : 67。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)

- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)

- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

KVM 向けの IPv4 VLAN を介した UDP の IPFIX テンプレート

KVM 向けの IPv4 VLAN を介した UDP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 VLAN を介した UDP の入力方向

テンプレート ID : 344。フィールド数 : 50。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)

- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv4 VLAN を介した UDP の出力方向

テンプレート ID : 345。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)

- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)

- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 VLAN を介した UDP の入力方向

テンプレート ID : 346。フィールド数 : 57。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))

- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 VLAN を介した UDP の出力方向

テンプレート ID : 347。フィールド数 : 61。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))

- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv4 VLAN を介した SCTP の IPFIX テンプレート

KVM 向けの IPv4 VLAN を介した SCTP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv4 VLAN を介した SCTP の入力方向

テンプレート ID : 348。フィールド数 : 50。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)

- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv4 VLAN を介した SCTP の出力方向

テンプレート ID : 349。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)

- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)

- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 VLAN を介した SCTP の入力方向

テンプレート ID : 350。フィールド数 : 57。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)

- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)

- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv4 VLAN を介した SCTP の出力方向

テンプレート ID : 351。フィールド数 : 61。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)

- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)

- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM の ICMPv4 VLAN の IPFIX テンプレート

KVM の ICMPv4 VLAN の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

ICMPv4 VLAN の入力方向

テンプレート ID : 352。フィールド数 : 50。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)

- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)

- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

ICMPv4 VLAN の出力方向

テンプレート ID : 353。フィールド数 : 54。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)

- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv4 VLAN の入力方向

テンプレート ID : 354。フィールド数 : 57。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))

- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv4 VLAN の出力方向

テンプレート ID : 355。フィールド数 : 61。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)

- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IP_SRC_ADDR (length : 4)
- IP_DST_ADDR (length : 4)
- ICMP_IPv4_TYPE (length : 1)
- ICMP_IPv4_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))

- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM の IPv6 VLAN の IPFIX テンプレート

KVM の IPv6 VLAN の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 VLAN の入力方向

テンプレート ID : 356。フィールド数 : 49。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)

- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv6 VLAN の出力方向

テンプレート ID : 357。フィールド数 : 53。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)

- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 VLAN の入力方向

テンプレート ID : 358。フィールド数 : 56。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)

- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)

- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 VLAN の出力方向

テンプレート ID : 359。フィールド数 : 60。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)

- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)

- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv6 VLAN を介した TCP の IPFIX テンプレート

KVM 向けの IPv6 VLAN を介した TCP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 VLAN を介した TCP の入力方向

テンプレート ID : 360。フィールド数 : 57。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)

- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)

- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

IPv6 VLAN を介した TCP の出力方向

テンプレート ID : 361。フィールド数 : 61。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)

- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)

- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv6 VLAN を介した TCP の入力方向

テンプレート ID : 362。フィールド数 : 64。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))

- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

トンネルを使用する IPv6 VLAN を介した TCP の出力方向

テンプレート ID : 363。フィールド数 : 68。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)

- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)

- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMcastOctetTotalCount (length : 8)
- tcpAckTotalCount (length : 8)
- tcpFinTotalCount (length : 8)
- tcpPshTotalCount (length : 8)
- tcpRstTotalCount (length : 8)
- tcpSynTotalCount (length : 8)
- tcpUrgTotalCount (length : 8)

KVM 向けの IPv6 VLAN を介した UDP の IPFIX テンプレート

KVM 向けの IPv6 VLAN を介した UDP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 VLAN を介した UDP の入力方向

テンプレート ID : 364。フィールド数 : 51。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)

- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)

- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv6 VLAN を介した UDP の出力方向

テンプレート ID : 365。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)

- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 VLAN を介した UDP の入力方向

テンプレート ID : 366。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))

- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 VLAN を介した UDP の出力方向

テンプレート ID : 367。フィールド数 : 62。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))

- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM 向けの IPv6 VLAN を介した SCTP の IPFIX テンプレート

KVM 向けの IPv6 VLAN を介した SCTP の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

IPv6 VLAN を介した SCTP の入力方向

テンプレート ID : 368。フィールド数 : 51。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)

- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

IPv6 VLAN を介した SCTP の出力方向

テンプレート ID : 369。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)

- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)

- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 VLAN を介した SCTP の入力方向

テンプレート ID : 370。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)

- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)

- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する IPv6 VLAN を介した SCTP の出力方向

テンプレート ID : 371。フィールド数 : 62。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)

- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- L4_SRC_PORT (length : 2)
- L4_DST_PORT (length : 2)
- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)

- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM の ICMPv6 VLAN の IPFIX テンプレート

KVM の ICMPv6 の IPFIX テンプレートは 4 つあります（入力方向、出力方向、トンネルを使用する入力方向、およびトンネルを使用する出力方向）。

ICMPv6 の入力方向

テンプレート ID : 372。フィールド数 : 51。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)

- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)

- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

ICMPv6 の出力方向

テンプレート ID : 373。フィールド数 : 55。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)

- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)

- IP_LENGTH_MINIMUM (length : 8)
- IP_LENGTH_MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv6 の入力方向

テンプレート ID : 374。フィールド数 : 58。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)
- 893 (length : 4、PEN : VMware Inc. (6876))

- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMcastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)
- MUL_DOCTETS (length : 8)

- postMCastOctetTotalCount (length : 8)

トンネルを使用する ICMPv6 の出力方向

テンプレート ID : 375。フィールド数 : 62。

フィールドは次のとおりです。

- observationPointId (length : 4)
- DIRECTION (length : 1)
- SRC_MAC (length : 6)
- DESTINATION_MAC (length : 6)
- ethernetType (length : 2)
- ethernetHeaderLength (length : 1)
- INPUT_SNMP (length : 4)
- Unknown(368) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- OUTPUT_SNMP (length : 4)
- Unknown(369) (length : 4)
- IF_NAME (length : 可変)
- IF_DESC (length : 可変)
- SRC_VLAN (length : 2)
- dot1qVlanId (length : 2)
- dot1qPriority (length : 1)
- IP_PROTOCOL_VERSION (length : 1)
- IP_TTL (length : 1)
- PROTOCOL (length : 1)
- IP_DSCP (length : 1)
- IP_PRECEDENCE (length : 1)
- IP_TOS (length : 1)
- IPV6_SRC_ADDR (length : 4)
- IPV6_DST_ADDR (length : 4)
- FLOW_LABEL (length : 4)
- ICMP_IPv6_TYPE (length : 1)
- ICMP_IPv6_CODE (length : 1)

- 893 (length : 4、PEN : VMware Inc. (6876))
- 894 (length : 4、PEN : VMware Inc. (6876))
- 895 (length : 1、PEN : VMware Inc. (6876))
- 896 (length : 2、PEN : VMware Inc. (6876))
- 897 (length : 2、PEN : VMware Inc. (6876))
- 891 (length : 1、PEN : VMware Inc. (6876))
- 892 (length : 可変、PEN : VMware Inc. (6876))
- 898 (length : 可変、PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (length : 4)
- flowEndDeltaMicroseconds (length : 4)
- DROPPED_PACKETS (length : 8)
- DROPPED_PACKETS_TOTAL (length : 8)
- PKTS (length : 8)
- PACKETS_TOTAL (length : 8)
- Unknown(354) (length : 8)
- Unknown(355) (length : 8)
- Unknown(356) (length : 8)
- Unknown(357) (length : 8)
- Unknown(358) (length : 8)
- MUL_DPKTS (length : 8)
- postMCastPacketTotalCount (length : 8)
- Unknown(352) (length : 8)
- Unknown(353) (length : 8)
- flowEndReason (length : 1)
- DROPPED_BYTES (length : 8)
- DROPPED_BYTES_TOTAL (length : 8)
- BYTES (length : 8)
- BYTES_TOTAL (length : 8)
- BYTES_SQUARED (length : 8)
- BYTES_SQUARED_PERMANENT (length : 8)
- IP LENGTH MINIMUM (length : 8)
- IP LENGTH MAXIMUM (length : 8)

- MUL_DOCTETS (length : 8)
- postMCastOctetTotalCount (length : 8)

KVM のオプション IPFIX テンプレート

IETF RFC 7011 の 3.4.2 節に基づく KVM のオプション テンプレートは 1 つあります。

オプション テンプレート

テンプレート ID : 462。スコープ数 : 1。データ数 : 1。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [ポート] の選択
- 3 ポートの名前をクリックします。
- 4 [監視] タブをクリックします。

ポートの状態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] をクリックします。
- 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] 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。

論理スイッチと関連オブジェクトは、[ネットワークとセキュリティの詳細設定] タブで設定できます。論理スイッチは、基盤となるハードウェアから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。

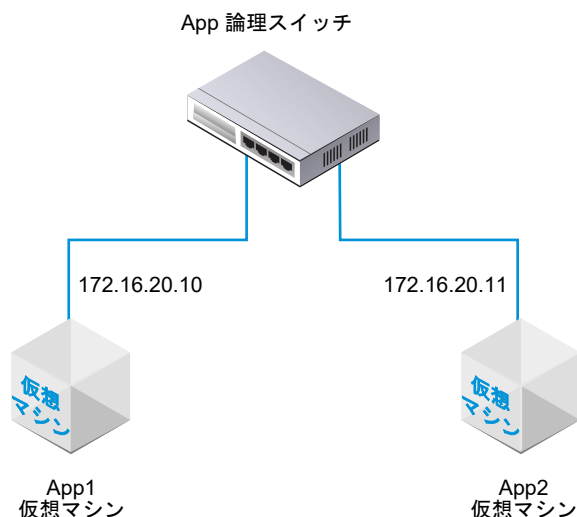
注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 [NSX Manager の概要](#) を参照してください。

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 13-1. 論理スイッチ トポロジ



たとえば、上のトポロジは 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。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

この章には、次のトピックが含まれています。

- [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](#)
- [論理スイッチへの仮想マシンの接続](#)
- [論理スイッチ ポートの作成](#)
- [レイヤー 2 接続のテスト](#)
- [NSX Edge アップリンク用の VLAN 論理スイッチの作成](#)
- [論理スイッチおよび論理ポートのスイッチング プロファイル](#)
- [拡張ネットワーク スタック](#)
- [レイヤー 2 ブリッジ](#)

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 の構成に応じて、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 Data Center 論理スイッチが複数のハイパーバイザーにまたがる場合があることに注意してください。特定のハイパーバイザー上の仮想マシンによって送信された BUM トラフィックを、同じ論理スイッチに接続された他の仮想マシンをホストするリモート ハイパーバイザーにレプリケートする必要があります。このフラッドを有効にするために、NSX-T Data Center 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 Data Center 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 Data Center 管理プレーン エージェント (MPA) および NSX-T Data Center 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 Data Center 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 Data Center 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 Data Center 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。[13 章 論理スイッチおよび 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。

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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチ] - [追加] を選択します。
- 3 論理スイッチの名前と、必要に応じて説明を入力します。
- 4 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。
- 5 アップリンク チーミング ポリシーの名前を入力します。
- 6 [管理状態] を [稼動中] または [停止] に設定します。
- 7 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	レプリケーターは、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 でレプリケーターとなる 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。

- 8 （オプション）VLAN タギングに使用する VLAN ID または VLAN ID の範囲を指定します。
このスイッチに接続された仮想マシンに対してゲスト VLAN タギングをサポートするには、VLAN ID の範囲を指定する必要があります。これは、トランク VLAN ID 範囲とも呼ばれます。論理ポートではトランク VLAN ID 範囲に基づいてパケットがフィルタリングされ、ゲスト仮想マシンはトランク VLAN ID 範囲に基づいてパケットを独自の VLAN ID でタグ付けできます。
- 9 （オプション）[スイッチング プロファイル] 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。
- 10 [保存] 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。

論理スイッチへの仮想マシンの接続

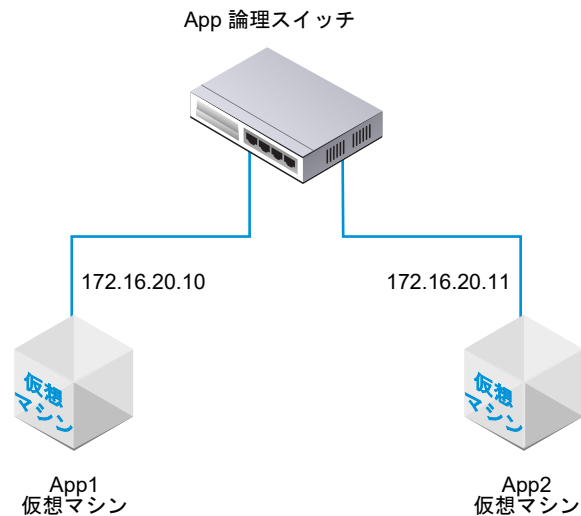
仮想マシンを論理スイッチに接続する設定は、ホストによって異なります。

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 Data Center 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 Data Center 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 Data Center 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 Data Center 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 Data Center 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 Data Center 管理プレーン (MPA) と NSX-T Data Center 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 Data Center 論理スイッチに接続します。

次はその例です。

1-vm_ubuntu_1404_srv_64-local-645-bfd95df0-ea28-4408-ae9a-2561750b0674 - 設定の編集

仮想ハードウェア | 仮想マシン オプション | Storage DRS ルール | vApp オプション

CPU	1	
メモリ	1024	MB
ハード ディスク 1	16	GB
SCSI コントローラ 0	LSI Logic パラレル	
*ネットワークアダプタ 1	LS.ONE (nsx.LogicalSwitch)	<input checked="" type="checkbox"/> 接続中
ネットワークアダプタ 2	lswitch301 (nsx.LogicalSwitch)	<input checked="" type="checkbox"/> 接続中
ビデオ カード	カスタム設定の指定	
VMCI デバイス		

- 2 [OK] をクリックします。

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。[ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [ポート] の NSX Manager の論理スイッチ ポートと VIF 接続 ID を表示できます。

GET <https://<mgr-ip>/api/v1/logical-ports/> API 呼び出しを使用して、対応する VIF 接続 ID のポートの詳細と管理状態を表示します。運用状態を表示するには、適切な論理ポート ID で <https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status> API 呼び出しを使用します。

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 Data Center 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。

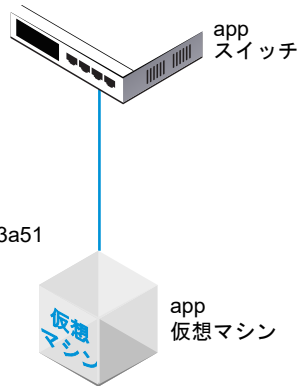
スタンドアロン ESXi にホストされている仮想マシンの NSX-T Data Center 論理スイッチへの接続

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 Data Center 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 Data Center 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 Data Center 管理プレーン (MPA) と NSX-T Data Center 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 追加

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

結果から仮想マシンの externalId を検出します。

次はその例です。

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

{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    {
      "instanceUuid": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
      "moIdOnHost": 5,
      "externalId": "[50066bae-0f8a-386b-e62e-b0b9c6013a51]",
      "hostLocalId": 5,
      "locationId": "564dc020-1565-e3f4-f591-ee3953eef3ff",
      "biosUuid": "4206f47d-fef7-08c5-5bf7-ea26a4c6b18d"
    }
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
}
```

```
"host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
"local_id_on_host": "5"
}
```

3 仮想マシンをパワーオフし、ホストから登録解除します。

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

```
[user@host:~] [vim-cmd /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

概要 監視 管理 ▾ 関連 ▾

▽ サマリ | 編集

名前	app-switch
ID	b68e7ac3-877a-420e-af47-53e974c17915
場所	
説明	lswitch202 (created through automation)
管理状態	● 稼動中
レプリケーション モード	ヘッド レプリケーション
VLAN	該当なし
VNI	71681
論理ポート	1
トラフィック タイプ	オーバーレイ
トランスポート ゾーン	transportzone1
アップリンク チーミング ポリシ...	[Use Default]
N-VDS モード	STANDARD
作成	admin、9/10/2018, 12:20:46 PM
最終更新	9/26/2018, 2:01:14 PM、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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [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両方とも [稼動中] 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

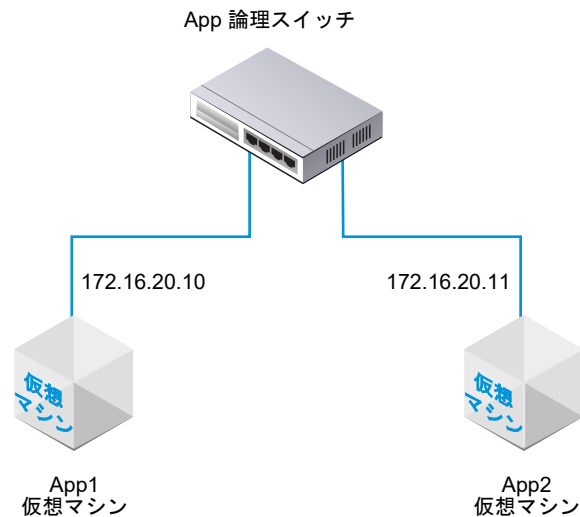
論理ルーターを追加します。

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 Data Center 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 Data Center 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 Data Center 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 Data Center 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 Data Center 管理プレーン (MPA) と NSX-T Data Center 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

NSX Manager のユーザー インターフェイスの [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [ポート] で VIF 接続 ID を検索し、管理および運用の状態が両方とも [稼動中] 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 Data Center 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。

論理スイッチ ポートの作成

論理スイッチには複数のスイッチ ポートがあります。論理スイッチ ポートは、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します。

vCenter Server によって管理されている ESXi ホスト上の論理スイッチに仮想マシンを接続すると、論理スイッチ ポートが自動的に作成されます。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](#)を参照してください。

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。

論理スイッチ ポートでアクティビティを監視するには、[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。

前提条件

論理スイッチが作成されていることを確認します。[13 章 論理スイッチ](#)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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [ポート] - [追加] を選択します。
- 3 [全般] 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 メニューから論理スイッチを選択します。
管理状態	[稼動中] または [停止] を選択します。
添付ファイルの種類	[なし] 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。

API を使用して、接続の種類を追加の値（LOGICALROUTER、BRIDGEENDPOINT、DHCP_SERVICE、METADATA_PROXY、L2VPN_SESSION）に設定できます。接続の種類が DHCP サービス、メタデータ プロキシまたは L2 VPN セッションの場合、ポートのスイッチング プロファイルをデフォルトにする必要があります。ユーザー定義のプロファイルは使用できません。

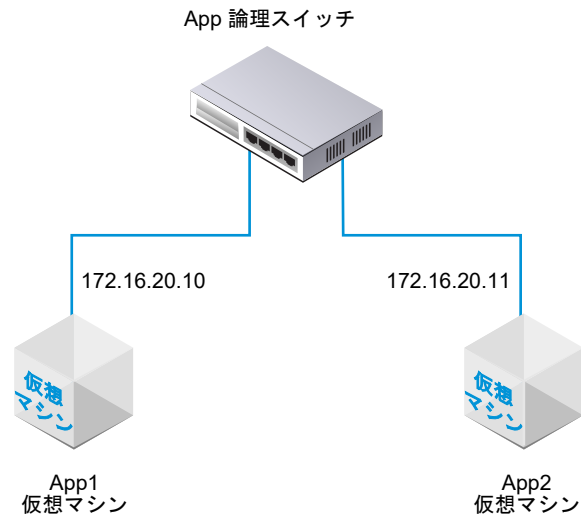
- 4 (オプション) [スイッチング プロファイル] タブで、スイッチング プロファイルを選択します。
- 5 [保存] をクリックします。

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 13-2. 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 で [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [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 次のコマンドを実行して問題のトラブルシューティングを行います。

コマンド	説明
get logical-switch <vni-or-uuid> arp-table	<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-manager1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
get logical-switch <vni-or-uuid> connection-table	<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-manager1> 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>
get logical-switch <vni-or-uuid> mac-table	<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-manager1> 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>
get logical-switch <vni-or-uuid> stats	<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-manager1> 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>
get logical-switch <vni-or-uuid> stats-sample	<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-manager1> 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>
<pre>get logical-switch <vni-or-uuid> vtep</pre>	<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-manager1> 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>

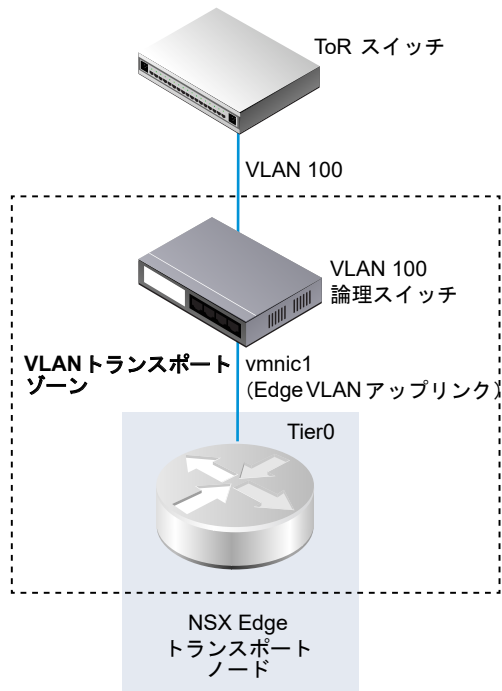
結果

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。

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 Data Center 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
```

- ファブリック ノードが NSX-T Data Center 管理プレーン エージェント (MPA) および NSX-T Data Center 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 Data Center 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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチ] - [追加] を選択します。
- 3 論理スイッチの名前を入力します。
- 4 論理スイッチのトランスポート ゾーンを選択します。
- 5 アップリンク チーミング ポリシーを選択します。
- 6 管理状態は、[稼動中] または [停止] を選択します。
- 7 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。

- 8 (オプション) [スイッチング プロファイル] 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。

論理スイッチおよび論理ポートのスイッチング プロファイル

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

次のタイプのスイッチング プロファイルを使用できます。

- QoS (サービス品質)
- ポート ミラーリング
- IP 検出
- SpoofGuard
- スイッチ セキュリティ
- MAC アドレス管理

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。

デフォルトのプロファイルを使用する前に、適切な設定になっているかどうか確認してください。カスタム プロファイルを作成する場合、一部の設定にはデフォルト値があります。デフォルトのプロファイルで、これらの設定にデフォルト値があるとは限りません。

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と関連付けます。たとえば、デフォルトの QoS スイッチング プロファイルの ID は f313290b-eba8-4262-bd93-fab5026e9495 です。

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

論理スイッチの作成中または更新中にスイッチング プロファイル タイプを関連付けなかった場合は、NSX Manager で、対応するシステム定義のデフォルト スイッチング 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 プロファイルを関連付けできます。スイッチング プロファイルを論理スイッチと関連付けたり、関連付けを解除したりすると、次の基準に従って、子論理ポート用のスイッチング プロファイルが適用されます。

- 親論理スイッチにプロファイルが関連付けられている場合、子論理ポートはその親からスイッチング プロファイルを継承します。
- 親論理スイッチにスイッチング プロファイルが関連付けられていない場合、デフォルト スイッチング 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 スイッチング 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 スイッチング プロファイルを維持する場合は、デフォルト スイッチング プロファイルのコピーを作成し、それを特定の論理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 スイッチング 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 スイッチング 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。

QoS スイッチング 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 Data Center 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 プロファイル構成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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチング プロファイル] - [追加] の選択

3 [QoS] を選択して、QoS スイッチング プロファイルの詳細を入力します。

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 [信頼する] または [信頼しない] のいずれかのオプションを選択します。</p> <p>「信頼する」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。「信頼する」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>「信頼しない」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。「信頼しない」モードの DSCP 値の範囲は 0 ～ 63 です。</p> <p>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。</p>
優先順位	<p>DSCP の値を設定します。</p> <p>優先順位の値の範囲は 0 ～ 63 です。</p>
サービス 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 (Ingress)	<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ます。バースト サイズは、ピーク帯域幅の期間に基づいて設定されます。バースト サイズの設定でバースト期間を設定します。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に、平均、ピーク、バースト サイズの設定を使用できます。</p> <p>たとえば、平均帯域幅が 30 Mbps、ピーク帯域幅が 60 Mbps、許可された期間が 0.1 秒の場合、バースト サイズは $60 * 1,000,000 * 0.10/8 = 750,000$ バイトになります。</p> <p>デフォルト値は 0 で、入力方向トラフィックのレート制限を無効にします。</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>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。たとえば、論理スイッチの平均帯域幅が 3,000 Kbps、ピーク帯域幅が 6,000 Kbps、許可された期間が 0.1 秒の場合、バースト サイズは $6,000 * 1,000 * 0.10/8 = 75,000$ バイトになります。</p> <p>デフォルト値は 0 で、入力方向ブロードキャスト トラフィックのレート制限を無効にします。</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、出力方向トラフィックのレート制限を無効にします。</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、デフォルト値が使用されます。

4 [保存] 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。

ポート ミラーリングはトラブルシューティングにのみ使用することをお勧めします。

注： 監視にポート ミラーリングを使用することは推奨されていません。長期間使用すると、パフォーマンスに影響が生じます。

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 Data Center 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチング プロファイル] - [追加] の選択
- 3 [ポート ミラーリング] を選択して、ポート ミラーリングのスイッチング プロファイルの詳細を入力します。

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、このプロファイルを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롭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な 32 ビット値を入力します。 このキーの値は、ミラーリングされた各パケットの GRE ヘッダー内の [キー] フィールドにコピーされます。キーの値を 0 にセットすると、デフォルトの定義が GRE ヘッダーの [キー] フィールドにコピーされます。 デフォルトの 32 ビット値は次の値で設定されます。 <ul style="list-style-type: none"> ■ 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。 ■ 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。 ■ 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。 ■ 残りの 6 ビットは未使用です。
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 Data Center 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。

- 4 [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かを確認します。

前提条件

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

手順

- 1 ポート ミラーリング用に設定された論理ポートに接続している、VIF を持つ 2 台の仮想マシンを見つけます。
たとえば、VM1 10.70.1.1 と VM2 10.70.1.2 には VIF が接続され、同じ論理ネットワークにあります。
- 2 ターゲット IP アドレスで tcpdump コマンドを実行します。

sudo tcpdump -n -i eth0 dst host destination_IP_address and proto gre
たとえば、ターゲット IP アドレスは 10.24.123.196 です。
- 3 最初の仮想マシンにログインして、2 番目の仮想マシンに ping を送信し、対応する ECHO リクエストと応答がターゲット アドレスで受信されることを確認します。

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 アドレス検出では、DHCP と DHCPv6 スヌーピング、ARP (Address Resolution Protocol) スヌーピング、ネイバー検出 (ND) スヌーピング、および仮想マシン ツールを使用して、MAC および IP アドレスを学習します。

検出された MAC アドレスおよび IP アドレスを使用すると、ARP/ND 抑制が実現されるため、同じ論理スイッチに接続されている仮想マシン間のトラフィックが最小限に抑えられます。また、このアドレスは、SpoofGuard および分散ファイアウォール (DFW) のコンポーネントでも使用可能です。DFW はアドレス割り当てを使用し、ファイアウォール ルール内のオブジェクトの IP アドレスを決定します。

DHCP/DHCPv6 スヌーピングは、DHCP/DHCPv6 クライアントとサーバ間で交換された DHCP/DHCPv6 パケットを検査し、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 (Gratuitous ARP) パケットを検査し、IP アドレスと MAC アドレスを学習します。

仮想マシン ツールは、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 アドレスおよび IP または IPv6 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。

ND スヌーピングは ARP スヌーピングに相当する IPv6 です。Neighbor Solicitation (NS) と Neighbor Advertisement (NA) メッセージを検査し、IP アドレスと MAC アドレスを学習します。

重複アドレス検出は、新しく検出された IP アドレスが別のポートの認識済みの割り当てリストにすでに含まれているかどうかを確認します。このチェックは、同じセグメント上のポートに実行されます。アドレスの重複が検出されると、新しく検出されたアドレスは認識済みの割り当てリストではなく、検出リストに追加されます。重複するすべての IP アドレスは検出タイムスタンプに関連付けられます。除外する割り当てリストに追加したり、またはスヌーピングを無効にしたりして、認識済みの割り当てリスト内の IP アドレスが削除されると、最も古いタイムスタンプの重複 IP アドレスが認識済みの割り当てリストに移動します。重複するアドレス情報は API 呼び出しを介して使用できます。

デフォルトでは、ARP スヌーピングと ND スヌーピングの検出方法は、初回使用時に信頼する (TOFU) と呼ばれるモードで動作します。TOFU モードでは、アドレスが検出され、認識済みの割り当てリストに追加されると、その割り当ては認識済みのリストに永久に残ります。TOFU は、ARP/ND スヌーピングを使用して検出された最初の n 個の固有の <IP, MAC, VLAN> の割り当てに適用されます。n は、設定可能な割り当て制限です。ARP/ND スヌーピングの TOFU を無効にすることができます。これは、毎回使用時に信頼する (TOEU) モードで動作します。TOEU モードの場合、アドレスが検出されると、そのアドレスは認識済みの割り当てリストに追加されます。アドレスが削除されるか期限切れになると、認識済みの割り当てリストから削除されます。DHCP スヌーピングと仮想マシン ツールは常に TOEU モードで動作します。

各ポートでは、NSX Manager は、ポートに割り当てられない IP アドレスが含まれる、除外する割り当てリストを保持します。[ネットワークとセキュリティの詳細設定] - [スイッチング] - [ポート] の順に移動してポートを選択することで、検出された割り当てを除外する割り当てリストに追加できます。また、既存の検出済みまたは認識済みの割り当てを削除するには、[除外する割り当て] にコピーします。

注： TOFU は、SpoofGuard と同じではありません。SpoofGuard と同じ方法でトラフィックをブロックしません。詳細については、『[SpoofGuard セグメント プロファイルの理解](#)』を参照してください。

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 検出スイッチング プロファイルの設定

NSX-T Data Center には、いくつかのデフォルトの IP 検出スイッチング プロファイルがあります。追加の IP 検出スイッチング プロファイルを作成することもできます。

前提条件

IP 検出スイッチング プロファイルの概念について理解しておく必要があります。[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>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチング プロファイル] - [追加] を選択します。
- 3 [IP 検出] を選択して、IP 検出スイッチング 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	名前を入力します。必要に応じて説明も入力します。
ARP スヌーピング	IPv4 環境用。仮想マシンに固定 IP アドレスが設定されている場合に適用できます。
ARP 割り当て制限	ポートに割り当てられる IPv4 IP アドレスの最大数。許容されている最小値は 1（デフォルト）、最大値は 256 です。
ARP ND 割り当て制限のタイムアウト	TOFU が無効になっている場合に、ARP/ND 割り当てテーブル内の IP アドレスがタイムアウトになる時間の値（分単位）。アドレスがタイムアウトになった場合は、新たに検出されたアドレスで置き換えられます。
DHCP スヌーピング	IPv4 環境用。仮想マシンに IPv4 アドレスが設定されている場合に適用できます。
DHCP V6 スヌーピング	IPv6 環境用。仮想マシンに IPv6 アドレスが設定されている場合に適用できます。
仮想マシン ツール	ESXi ホストの仮想マシン専用。
IPv6 の仮想マシン ツール	ESXi ホストの仮想マシン専用。
ネイバー検出 (ND) スヌーピング	IPv6 環境用。仮想マシンに固定 IP アドレスが設定されている場合に適用できます。
ネイバー検出割り当ての制限	ポートに割り当てられる IPv6 IP アドレスの最大数。
初回使用時に信頼する	ARP スヌーピングおよび ND スヌーピングに適用できます。
重複 IP アドレスの検出	すべてのスヌーピング方法と IPv4 と IPv6 の両方の環境に使用します。

- 4 [追加] をクリックします。

次のステップ

この IP 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既存の IP アドレスを変更することを防ぐためのツールです。仮想マシンの IP アドレスが対応する論理ポートの IP アドレスおよび SpoofGuard のスイッチ アドレス バインドに一致しない場合、仮想マシンの vNIC からネットワークへのアクセスは完全に遮断されます。SpoofGuard はポートまたはスイッチ レベルで設定することができます。SpoofGuard を導入環境で使用するのにはいくつかの理由があります。

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

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

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

ポート アドレス バインドの設定

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

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

手順

- 1 NSX Manager で [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [ポート] の順に選択します。
- 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 [概要] タブで、[アドレスの割り当て] - [手動割り当て] の順に展開します。
- 4 [追加] 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 アドレス割り当てを適用する論理ポートの IP アドレス (IPv4 アドレス、IPv6 アドレスまたは IPv6 サブネット) と MAC アドレスを指定します。たとえば、IPv6 の場合、IPv6 サブネットに 2001::/64、ホスト IP に 2001::1 を指定できますが、2001::1/64 は無効な入力になります。VLAN ID を指定することもできます。
- 6 [追加] 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。

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。

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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチング プロファイル] - [追加] を選択します。
- 3 [SpoofGuard] を選択します。
- 4 名前を入力します。必要に応じて説明も入力します。
- 5 ポート レベルの SpoofGuard を有効にするには、[ポート割り当て] を [有効] に設定します。
- 6 [追加] 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 プロファイルを関連付けます。[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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] の順に選択します。
- 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、[スイッチ セキュリティ] 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] ボタンを切り替えて BPDU フィルタを有効にします。デフォルトは無効です。 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。このリストから選択できるようにするには、[BPDU フィルタ] を有効にする必要があります。

オプション	説明
DHCP フィルタ	<p>[サーバ ブロック] ボタンおよび [クライアント ブロック] ボタンを切り替えて、DHCP フィルタを有効にします。どちらもデフォルトは無効です。</p> <p>DHCP サーバのブロックにより、DHCP サーバから DHCP クライアントへのトラフィックがブロックされます。DHCP サーバから DHCP リレー エージェントへのトラフィックはブロックされないことに注意してください。</p> <p>DHCP クライアントのブロックでは DHCP 要求がブロックされるため、仮想マシンによる DHCP IP アドレスの取得を防止できます。</p>
DHCPv6 フィルタ	<p>[V6 サーバ ブロック] ボタンおよび [V6 クライアント ブロック] ボタンを切り替えて、DHCP フィルタを有効にします。どちらもデフォルトは無効です。</p> <p>DHCPv6 サーバのブロックにより、DHCPv6 サーバから DHCPv6 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。UDP 送信元ポート番号が 547 のパケットがフィルタされます。</p> <p>DHCPv6 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。UDP 送信元ポート番号が 546 のパケットがフィルタされます。</p>
非 IP トラフィックをブロック	<p>[非 IP トラフィックをブロック] ボタンを切り替えて、IPv4、IPv6、ARP および BPDU トラフィックのみを許可します。</p> <p>それ以外のトラフィックはブロックされます。IPv4、IPv6、ARP、GARP および BPDU トラフィックは、アドレスの割り当ておよび SpoofGuard に設定されたその他のポリシーに基づいて許可されます。</p> <p>デフォルトではこのオプションは無効で、非 IP トラフィックは通常のトラフィックとして処理されます。</p>
RA ガード	<p>入力方向の IPv6 ルーター アドバタイズを除外するには、[RA ガード] ボタンを切り替えます。ICMPv6 タイプ 134 パケットが除外されます。このオプションはデフォルトで有効です。</p>
レート制限	<p>ブロードキャスト トラフィックとマルチキャスト トラフィックのレート制限を設定します。このオプションはデフォルトで有効です。</p> <p>レート制限は、ブロードキャストの大量発生などのイベントから論理スイッチや仮想マシンを保護するために使用できます。</p> <p>接続の問題を回避するため、レートの制限の最小値は 10 pps 以上にする必要があります。</p>

6 [追加] 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。ゲスト仮想マシンが VMware Integrated OpenStack で展開されている場合、このプロパティはデフォルトで有効になります。

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

学習可能な MAC アドレスの数は設定可能です。最大値は 4,096 で、これがデフォルトです。また、制限に達したときのポリシーを設定することもできます。次のオプションがあります。

- [ドロップ]: 不明な送信元 MAC アドレスからのパケットをドロップします。この MAC アドレスへの受信パケットは、不明なユニキャストとして扱われます。ポートは、不明なユニキャストのフラッドが有効になっている場合にのみ、パケットを受信します。
- [許可]: アドレスは学習されませんが、不明な送信元 MAC アドレスからのパケットは転送されます。この MAC アドレスへの受信パケットは、不明なユニキャストとして扱われます。ポートは、不明なユニキャストのフラッドが有効になっている場合にのみ、パケットを受信します。

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

MAC 管理スイッチング プロファイルの設定

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチング プロファイル] - [追加] を選択します。
- 3 [MAC 管理] を選択して、MAC 管理プロファイルの詳細を入力します。

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。デフォルトは無効です。
ステータス	MAC 学習機能を有効または無効にします。デフォルトは無効です。
不明なユニキャスト フラッディング	不明なユニキャスト フラッディング機能を有効または無効にします。デフォルトは有効です。 MAC ラーニングを有効にする場合は、このオプションを使用できます。
MAC の制限	MAC アドレスの最大数を設定します。デフォルトは 4096 です。MAC ラーニングを有効にする場合は、このオプションを使用できます。
MAC の制限ポリシー	[許可] または [ドロップ] を選択します。デフォルトは [許可] です。MAC ラーニングを有効にする場合は、このオプションを使用できます。

- 4 [追加] をクリックします。

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 プロファイルに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1つでデフォルト スwitchング プロファイルを維持したい場合は、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。[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>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [スイッチ] を選択します。
- 3 カスタムのスイッチング プロファイルを適用する論理スイッチをクリックします。
- 4 [管理] タブをクリックします。
- 5 ドロップダウン メニューからカスタムのスイッチング プロファイルのタイプを選択します。

- [QoS]
- [ポート ミラーリング]
- [IP 検出]
- [SpoofGuard]
- [スイッチ セキュリティ]
- [MAC 管理]

- 6 [変更] をクリックします。
- 7 ドロップダウン メニューから以前に作成されたカスタムのスイッチング プロファイルを選択します。
- 8 [保存] 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。

- 9 設定を変更した新しいカスタム スイッチング プロファイルが [管理] タブに表示されることを確認します。
- 10 (オプション) [関連] タブをクリックし、ドロップダウン メニューから [ポート] を選択して、子論理ポートにカスタム スイッチング 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 スイッチング 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、および論理リンクの状態を公開します。

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、子の論理ポート用の別のカスタム スイッチング 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。[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>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] - [ポート] を選択します。
- 3 カスタムのスイッチング プロファイルを適用する論理ポートをクリックします。
- 4 [管理] タブをクリックします。
- 5 ドロップダウン メニューからカスタムのスイッチング プロファイルのタイプを選択します。
 - [QoS]
 - [ポート ミラーリング]
 - [IP 検出]
 - [SpoofGuard]
 - [スイッチ セキュリティ]
 - [MAC 管理]
- 6 [変更] をクリックします。
- 7 ドロップダウン メニューから以前に作成されたカスタムのスイッチング プロファイルを選択します。
- 8 [保存] 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。

- 9 設定を変更した新しいカスタム スwitchング プロファイルが [管理] 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 Data Center 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。

拡張ネットワーク スタック

拡張データ パスはネットワーク スタック モードであり、これを構成することで優れたネットワーク パフォーマンスを実現します。これは主に NFV ワークロードを対象としています。NFV ワークロードでは、このモードで実現するパフォーマンス上の利点を活用する必要があります。

N-VDS スイッチは、ESXi ホスト上でのみ拡張データ パス モードで設定できます。ENS は、Edge 仮想マシンを通過するトラフィックもサポートします。拡張データ パス モードでは、オーバーレイ トラフィックと VLAN トラフィックを設定できます。

ENS 論理コアの自動割り当て

専用の論理コアが vNIC からの受信トラフィックと送信トラフィックを管理するように、論理コアを自動的に vNIC に割り当てます。

拡張データパス モードで設定された N-VDS スイッチを使用する場合、単一の論理コアが vNIC に関連付けられていると、その論理コアが vNIC の双方向のトラフィックを処理します。複数の論理コアが設定されている場合、ホストは、vNIC のトラフィックを処理する論理コアを自動的に決定します。

次のいずれかのパラメータに基づいて、vNIC を論理コアを割り当てます。

- **vNIC-count** : ホストは、vNIC の一方向の受信または送信トラフィックの転送で同じ量の CPU リソースが必要になることを想定します。各論理コアには、論理コアの使用可能なプールに基づいて同じ数の vNIC が割り当てられます。これがデフォルトのモードです。vNIC-count モードは信頼性が高くなりますが、非対称トラフィックには最適ではありません。
- **CPU-usage** : ホストは、内部統計を使用して vNIC の各方向で受信トラフィックまたは送信トラフィックに使用される CPU 使用率を予測します。ホストは、トラフィックの転送に使用される CPU 使用率に基づいて、論理コアの割り当てを変更し、論理コア間でロード バランシングを行います。CPU-usage モードは vNIC-count よりも適していますが、トラフィックが安定しない場合は信頼性が低くなります。

CPU-usage モードの場合、転送されるトラフィック量が頻繁に変化すると、必要になる CPU リソースの予測と vNIC の割り当ても頻繁に変更される可能性があります。割り当てが頻繁に変更されると、パケットがドロップされる可能性があります。

トラフィック パターンが vNIC 間で対称である場合、vNIC-count モードを使用すると、動作の信頼性が高くなり、頻繁な変更に対する影響も少なくなります。ただし、トラフィック パターンが非対称の場合、vNIC-count モードを使用すると、vNIC 間でトラフィックの違いが識別されず、パケットがドロップする可能性があります。

vNIC-count モードでは、各論理コアに同じ数の vNIC が割り当てられるように、適切な数の論理コアを設定することをおすすめします。各論理コアに関連付けられている vNIC の数が異なる場合、CPU の割り当てが一定でなくなり、パフォーマンスは予測できません。

vNIC が接続または切断された場合、または論理コアが追加または削除された場合、ホストは自動的に変更を検出して再調整します。

手順

- ◆ モードを切り替えるには、次のコマンドを実行します。

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

<ens-lc-mode> は **vNIC-count** または **cpu-usage** に設定します。

vNIC-count は vNIC/方向のカウントに基づいて論理コアを割り当てます。

cpu-usage は、CPU 使用率に基づいて論理コアを割り当てます。

ゲスト VLAN 間ルーティングの設定

オーバーレイ ネットワークでは、NSX-T は L3 ドメインでの VLAN 間トラフィックのルーティングをサポートします。仮想分散論理ルーター (VDR) は、VLAN ID を使用して VLAN サブネット間のパケットをルーティングします。

VLAN 間のルーティングにより、仮想マシンごとに使用可能な vNIC の上限（最大 10 個まで）が解消されます。NSX-T では、VLAN 間のルーティングがサポートされているため、vNIC に多くの VLAN サブインターフェイスを作成し、異なるネットワーク サービスで使用できます。たとえば、仮想マシンの 1 つの vNIC を複数のサブインターフェイスに分割できます。各サブインターフェイスをサブネットに追加し、SNMP や DHCP などのネットワーク サービスをホストできます。たとえば、VLAN 間のルーティングでは、VLAN-10 のサブインターフェイスは、VLAN-10 またはその他の VLAN のサブインターフェイスに到達できます。

仮想マシン上の各 vNIC は、親論理ポートを介して N-VDS に接続します。これにより、タグのないパケットを管理します。

サブインターフェイスを作成するには、前述の API 呼び出しを行い、関連する VIF を使用して拡張 N-VDS スイッチに子ポートを作成します。VLAN ID を使用してタグ付けされたサブインターフェイスは、新しい論理スイッチに関連付けられます。たとえば、VLAN10 は論理スイッチ LS-VLAN-10 に接続されます。VLAN10 のすべてのサブインターフェイスは、LS-VLAN-10 に接続する必要があります。サブインターフェイスの VLAN ID とそれに関連する論理スイッチは 1 対 1 でマッピングされている必要があります。たとえば、VLAN-10 にマッピングされている論理スイッチ LS-VLAN-10 に VLAN20 の子ポートを追加すると、VLAN 間のパケット ルーティングが機能しなくなります。このような構成エラーがあると、VLAN 間のルーティングは機能しません。

前提条件

- VLAN サブインターフェイスを論理スイッチに関連付ける前に、論理スイッチが別の VLAN サブインターフェイスと関連付けられていないことを確認します。不一致があると、オーバーレイ ネットワークで VLAN 間のルーティングが機能しない可能性があります。
- ホストで ESXi v 6.7 U2 以降のバージョンが実行されていることを確認します。

手順

- 1 vNIC にサブインターフェイスを作成する場合は、vNIC が親ポートに更新されていることを確認してください。次の REST API 呼び出しを実行します。

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "vif_type": "PARENT"
    },
    "id" : "<Attachment UUID of the vNIC>"
  },
  "admin_state" : "UP",
  "logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
  "_revision" : 0
}
```

- 2 仮想マシンのサブインターフェイスに関連付けられた N-VDS で、vNIC の親ポートに子ポートを作成するには、API 呼び出しを実行します。API 呼び出しを実行する前に、子ポートを仮想マシンのサブインターフェイスに接続するための論理スイッチが存在することを確認してください。

```
POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
```

```

    "resource_type" : "VifAttachmentContext",
    "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
    "traffic_tag" : <VLAN ID>,
    "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be
unique.
    "vif_type" : "CHILD"
  },
  "id" : "<ID of the CHILD port>"
},

  "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
to which Child port would be connected to>",
  "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
  "admin_state" : "UP"
}

```

結果

NSX-T Data Center が仮想マシンにサブインターフェイスを作成します。

レイヤー 2 ブリッジ

NSX-T Data Center 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 Data Center 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 Data Center レイヤー 2 ブリッジを使用することができます。このレイヤー 2 ブリッジは、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 ブリッジに関連する NSX-T Data Center の概念は、Edge クラスタと Edge ブリッジ プロファイルです。NSX Edge トランスポート ノードを使用して、レイヤー 2 ブリッジを設定できます。ブリッジに NSX Edge のトランスポート ノードを使用するには、Edge ブリッジ プロファイルを作成します。Edge ブリッジ プロファイルには、ブリッジに使用する Edge クラスタと、プライマリおよびバックアップ ブリッジとして機能する Edge トランスポート ノードを指定します。

Edge ブリッジ プロファイルは論理スイッチに接続し、マッピング サービスがブリッジに使用される Edge の物理アップリンクと、論理スイッチに関連付けられる VLAN ID を指定します。1 つの論理スイッチを複数のブリッジ プロファイルに接続できます。

Edge ブリッジ プロファイルの作成

Edge ブリッジ プロファイルを使用すると、NSX Edge クラスタが論理スイッチへのレイヤー 2 ブリッジを提供できるようになります。

Edge ブリッジ プロファイルを作成するときに、フェイルオーバー モードをプリエンプティブに設定すると、フェイルオーバーの発生時にスタンバイ ノードがアクティブ ノードになります。障害が発生したノードが復旧すると、再びアクティブ ノードになります。フェイルオーバー モードを非プリエンプティブに設定した場合、フェイルオーバー発生時にスタンバイ ノードがアクティブ ノードになります。障害が発生したノードが復旧すると、そのノードはスタンバイ ノードになります。スタンバイ Edge ノードで CLI コマンド `set l2bridge-port <uuid> state active` を実行することにより、スタンバイ Edge ノードをアクティブ ノードに手動で設定できます。こ

のコマンドは、非ブリエンプティブ モードでのみ適用できます。それ以外の場合、エラーが発生します。非ブリエンプティブ モードでスタンバイ ノードに適用すると、このコマンドにより HA フェイルオーバーがトリガーされます。アクティブ ノードに適用すると、このコマンドは無視されます。詳細については、『NSX-T Data Center Command-Line Interface Reference』を参照してください。

前提条件

- 2 台の NSX Edge トランスポート ノードを持つ NSX Edge クラスタがあることを確認します。

手順

- 1 [システム] - [ファブリック] - [プロファイル] - [Edge ブリッジ プロファイル] - [追加] を選択します。
- 2 Edge ブリッジ プロファイルの名前と、必要に応じて説明を入力します。
- 3 NSX Edge クラスタを選択します。
- 4 プライマリ ノードを選択します。
- 5 バックアップ ノードを選択します。
- 6 フェイルオーバー モードを選択します。
[ブリエンプティブ] および [非ブリエンプティブ] のオプションがあります。
- 7 [追加] ボタンをクリックします。

次のステップ

これで、論理スイッチをブリッジ プロファイルに関連付けることができます。

Edge ベースのブリッジの設定

Edge ベースのブリッジを設定する場合、Edge クラスタに Edge ブリッジ プロファイルを作成した後に、追加の設定が必要になります。

同じ Edge ノードで論理スイッチを 2 回ブリッジすることはできません。2 つの異なる Edge ノードの場合、同じ論理スイッチに 2 つの VLAN をブリッジできます。

3 つの構成オプションがあります。

オプション 1: 無作為検出モードの設定

- ポートグループに無作為検出モードを設定します。
- ポートグループで偽装転送を許可します。
- 次のコマンドを実行して、Edge 仮想マシンが実行されている ESXi ホストでリバース フィルタを有効にします。

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```

次に、以下の手順でポートグループの無作為検出モードを無効にして有効にします。

- ポートグループの設定を編集します。
- 無作為検出モードを無効にして、設定を保存します。

- ポートグループの設定を再度編集します。
- 無作為検出モードを有効にして、設定を保存します。
- 同じ VLAN のセットを共有する同じホスト上に、無作為検出モードのポート グループが他にないことを確認します。
- アクティブ モードの Edge 仮想マシンとスタンバイ モードの Edge 仮想マシンは、異なるホスト上に配置する必要があります。両方の仮想マシンが同じホスト上にあると、VLAN のトラフィックを両方の仮想マシンに無作為検出モードで転送する必要があるため、スループットが低下する可能性があります。

オプション 2：MAC アドレスの学習の設定

NSX-T がインストールされているホストに Edge が展開されている場合、VLAN 論理スイッチまたはセグメントに接続できます。論理スイッチの MAC 管理プロファイルで、MAC アドレスの学習が有効になっている必要があります。同様に、セグメントの MAC 検出プロファイルで、MAC アドレスの学習が有効になっている必要があります。

オプション 3：シンク ポートの設定

- 1 シンク ポートとして設定するトランク vNIC のポート番号を取得します。
 - a vSphere Web Client にログインして、[ホーム] - [ネットワーク] の順に移動します。
 - b NSX Edge のトランク インターフェイスが接続している分散ポート グループをクリックし、[ポート] をクリックして、仮想マシンが接続しているポートを確認します。トランク インターフェイスに関連付けられているポート番号をメモします。不明なデータを取得して更新する場合は、このポート番号を使用します。
- 2 VDS の dvsUuid 値を取得します。
 - a vCenter Server Mob ユーザー インターフェイス <https://<vc-ip>/mob> にログインします。
 - b [内容] をクリックします。
 - c [rootFolder] に関連付けられたリンクをクリックします (例: *group-d1 (Datacenters)*)。
 - d [childEntity] に関連付けられたリンクをクリックします (例: *datacenter-1*)。
 - e [networkFolder] に関連付けられたリンクをクリックします (例: *group-n6*)。
 - f NSX Edge に関連付けられた vSphere Distributed Switch の分散仮想スイッチ名のリンクをクリックします (例: *dvs-1 (Mgmt_VDS)*)。
 - g uuid 文字列の値をコピーします。不明なデータを取得して更新する場合は、dvsUuid にこの値を使用します。
- 3 指定されたポートに不明なデータが存在するかどうか確認します。
 - a <https://<vc-ip>/mob/?moid=DVSManager&vmodl=1> に移動します。
 - b [fetchOpaqueDataEx] をクリックします。

- c [selectionSet] 値ボックスに、次の XML 入力を貼り付けます。

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

NSX Edge のトランク インターフェイスに取得したポート番号と dvsUuid 値を使用します。

- d `isRuntime` を `false` に設定します。
- e [メソッドの起動] をクリックします。 `vim.dvs.OpaqueData.ConfigInfo` の値が表示された場合、不明なデータ セットが存在します。シンク ポートを設定するときに、`edit` 操作を使用します。
`vim.dvs.OpaqueData.ConfigInfo` の値が空の場合は、シンク ポートを設定するときに `add` 操作を使用します。

- 4 vCenter Server 管理対象オブジェクト ブラウザ (MOB) でシンク ポートを構成します。

- a <https://<vc-ip>/mob/?moid=DVSManager&vmdl=1> に移動します。
- b [updateOpaqueDataEx] をクリックします。
- c [selectionSet] 値ボックスに、次の XML 入力を貼り付けます。次はその例です。

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

vCenter Server 管理対象オブジェクト ブラウザから取得した dvsUuid 値を使用します。

- d `opaqueDataSpec` 値ボックスで、次のいずれかの XML 入力を貼り付けます。

不明なデータが設定されていない場合 (operation が add に設定されている場合)、この入力を使用してシンクポートを有効にします。

```
<opaqueDataSpec>  
  <operation>add</operation>  
  <opaqueData>  
    <key>com.vmware.etherswitch.port.extraEthFRP</key>  
    <opaqueData  
xsi:type="vmobl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>  
    </opaqueData>  
</opaqueDataSpec>
```

不明なデータはすでに設定されている場合（operation が edit に設定されている場合）、この入力を使用してシンク ポートを有効にします。

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmidl.Binary">AAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>
```

この入力を使用してシンク ポートを無効にします。

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmidl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>
```

- e isRuntime を false に設定します。
- f [[Invoke Method]] をクリックします。

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 Data Center オーバーレイに接続されている場合、NSX-T Data Center 環境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 接続ができるように、ブリッジでバックアップされる論理スイッチを設定できます。

前提条件

- Edge ブリッジ プロファイルがあることを確認します。
- 通常のトランスポート ノードとして機能する 1 台以上の ESXi または KVM ホスト。このノードは、NSX-T Data Center 展開環境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 Data Center 展開環境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 NSX Manager (<https://<nsx-mgr>>) にログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] の順に選択します。
- 3 オーバーレイ スイッチの名前をクリックします (トラフィック タイプ: オーバーレイ)。
- 4 [関連] > [Edge ブリッジ プロファイル] の順にクリックします。
- 5 [接続] をクリックします。
- 6 ブリッジ プロファイルに接続するには、次の操作を行います。
 - a Edge ブリッジ プロファイルを選択します。
 - b トランスポート ゾーンを選択します。
 - c VLAN ID を入力します。
 - d [保存] をクリックします。
- 7 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、Edge ブリッジ プロファイル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 Data Center の内部仮想マシンから NSX-T Data Center の外部にあるノードに ping を送信します。

[監視] タブをクリックして、ブリッジ スイッチ上のトラフィックを監視できます。

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もできます。


```
{
  "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-T Data Center は、2 階層のルーティング モデルをサポートします。

上位層には Tier-0 論理ルーターがあります。North バウンドでは、Tier-0 論理ルーターは 1 つ以上の物理ルーターまたはレイヤー 3 スイッチに接続し、物理インフラストラクチャへのゲートウェイとして機能します。South バウンドでは、論理ルーターは 1 つ以上の Tier-0 論理ルーターまたは 1 つ以上の論理スイッチに直接接続します。

下位層には Tier-1 論理ルーターがあります。North バウンドでは、Tier-1 論理ルーターは Tier-0 論理ルーターに接続します。South バウンドでは、1 つ以上の論理スイッチに接続します。

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 [NSX Manager の概要](#) 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。

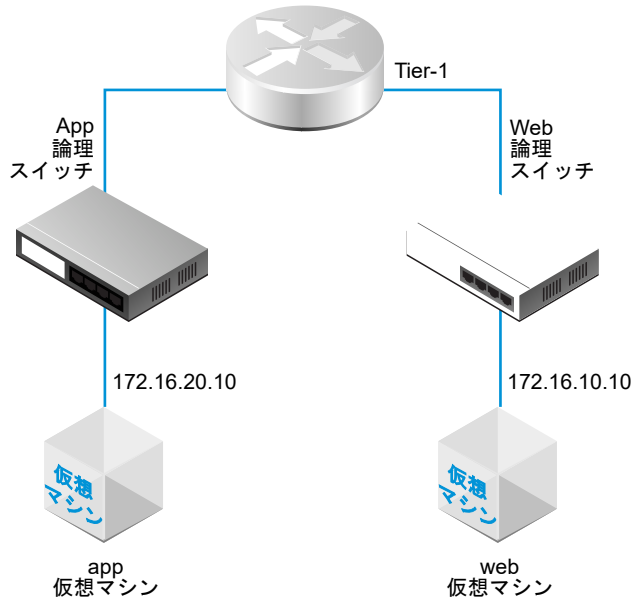
- [Tier-1 論理ルーター](#)
- [Tier-0 論理ルーター](#)

Tier-1 論理ルーター

Tier-1 論理ルーターには、論理スイッチに接続するダウンリンク ポートと、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 14-1. 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。

一部のシナリオでは、外部クライアントから、LB VIP ポートに割り当てられた MAC アドレスを照会する ARP クエリが送信されます。ただし、LB VIP ポートには MAC アドレスが設定されていないため、このようなクエリを処理できません。LB VIP ポートに代わって ARP クエリを処理するために、Tier-1 論理ルーターの統合サービス ポートにプロキシ ARP が実装されています。

Tier-1 論理ルーターに DNAT、Edge ファイアウォール、ロード バランサを指定すると、他の Tier-1 論理ルーターと送受信するトラフィックは、DNAT、Edge ファイアウォール、ロード バランサの順に処理されます。Tier 1 論理ルーター内のトラフィックは、最初に DNAT で処理され、次にロード バランサ経由で処理されます。Edge ファイアウォールの処理はスキップされます。

Tier-0 または Tier-1 論理ルーターで、さまざまなタイプのポートを設定できます。その 1 つが中央のサービス ポート (CSP) です。VLAN でバックアップされた論理スイッチに接続するか、スタンドアロンの Tier-1 論理ルーターを作成する場合は、アクティブ/スタンバイ モードの Tier-0 論理ルーターまたは Tier-1 論理ルーターで CSP を設定する必要があります。CSP は、アクティブ/スタンバイ モードの Tier-0 論理ルーターまたは Tier-1 論理ルーターで次のサービスをサポートします。

- NAT
- ロード バランシング
- ステートフル ファイアウォール
- VPN (IPsec および L2VPN)

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 Data Center 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。[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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ルーター] - [ルーター] - [追加] を選択します。
- 3 [Tier-1 ルーター] を選択して、論理ルーターの名前と、必要に応じて説明を入力します。
- 4 (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。

- 5 (オプション) NSX Edge クラスタを選択します。

選択したクラスタの選択を解除するには、[x] アイコンをクリックします。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。NSX 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、後でルーターの設定を編集できます。

- 6 (オプション) [スタンバイの再配置] 切り替えボタンをクリックして、スタンバイの再配置を有効または無効にします。

スタンバイの再配置とは、アクティブまたはスタンバイ状態の論理ルーターが稼動している Edge ノードに障害が発生した場合に、別の Edge ノード上に新しいスタンバイ論理ルーターを作成し、高可用性を維持することを意味します。アクティブな論理ルーターが実行されている Edge ノードで障害が発生した場合、元のスタンバイ論理ルーターがアクティブになり、新しいスタンバイ論理ルーターが作成されます。スタンバイ論理ルーターが実行されている Edge ノードで障害が発生した場合は、このルーターが新しいスタンバイ論理ルーターに置き換わります。

- 7 (オプション) NSX Edge クラスタを選択した場合は、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。

- 8 (オプション) [詳細] タブをクリックし、[Tier1 内中継サブネット] の値を入力します。
- 9 [追加] をクリックします。

結果

論理ルーターの作成後、ルーターの構成から Edge クラスタを削除する場合は、次の手順を行います。

- ルーターの名前をクリックして、構成の詳細を表示します。
- [サービス] - [Edge ファイアウォール] の順に選択します。
- [ファイアウォールの無効化] をクリックします。
- [概要] タブをクリックして、[編集] をクリックします。
- [Edge クラスタ] フィールドで、[x] アイコンをクリックします。
- [保存] をクリックします。

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、NSX 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 論理ルーターへのダウンリンク ポートの追加](#)を参照してください。

Tier-1 論理ルーターへのダウンリンク 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 ゲートウェイとして動作します。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 ルーターの名前をクリックします。
- 4 [設定] タブをクリックし、[ルーター ポート] を選択します。
- 5 [追加] をクリックします。
- 6 ルーター ポートの名前と、必要に応じて説明を入力します。
- 7 [タイプ] フィールドで、[ダウンリンク] を選択します。
- 8 [uRPF モード] では、[厳密] または [なし] を選択します。

uRPF (unicast Reverse Path Forwarding) は、セキュリティ機能です。

- 9 (オプション) 論理スイッチを選択します。
- 10 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。
- 11 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。
- 12 (オプション) DHCP リレー サービスを選択します。
- 13 [追加] をクリックします。

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のルートのアドバタイズの設定](#) を参照してください。

Tier-0 または Tier-1 論理ルーターへの VLAN ポートの追加

VLAN でバックアップされている論理スイッチのみを配置している場合、NSX-T Data Center がレイヤー 3 サービスを提供できるように、Tier-0 または Tier-1 ルーター上の VLAN ポートにスイッチを接続することができます。

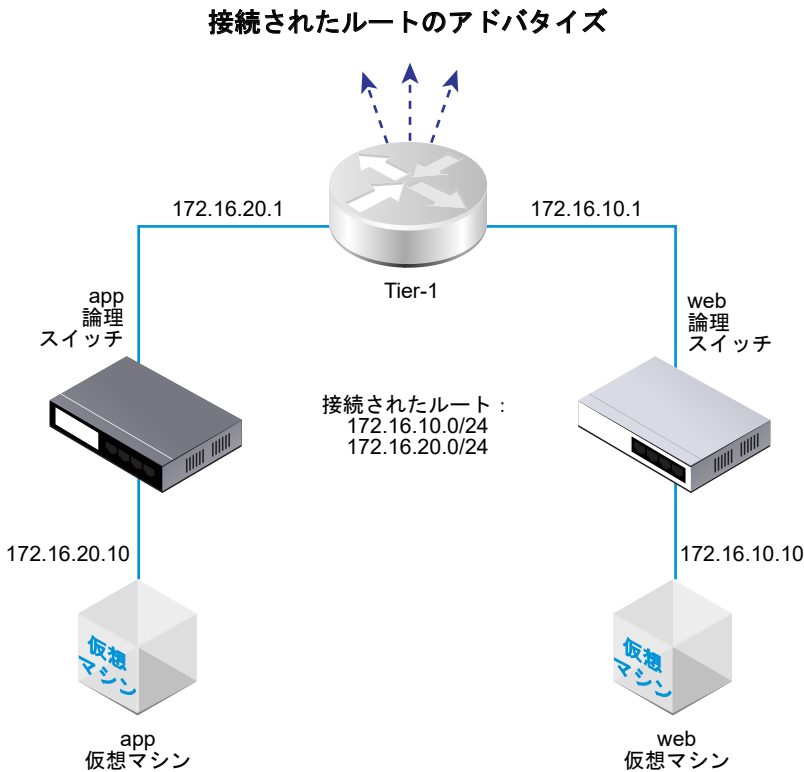
手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 ルーターの名前をクリックします。
- 4 [設定] タブをクリックし、[ルーター ポート] を選択します。
- 5 [追加] をクリックします。
- 6 ルーター ポートの名前と、必要に応じて説明を入力します。
- 7 [タイプ] フィールドで、[統合] を選択します。
- 8 [uRPF モード] では、[厳密] または [なし] を選択します。
uRPF (unicast Reverse Path Forwarding) は、セキュリティ機能です。
- 9 (必須) 論理スイッチを選択します。
- 10 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。
- 11 ルーター ポート IP アドレスを CIDR 表記で入力します。
- 12 [追加] をクリックします。

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

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 Data Center は NSX-T Data Center スタティック ルートを自動的に作成します。

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



前提条件

- 仮想マシンが論理スイッチに接続されていることを確認します。[13 章 論理スイッチ](#) 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 論理ルーターへのダウンリンク 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 Tier-1 ルーターの名前をクリックします。
- 4 [ルーティング] ドロップダウン メニューから [ルート アドバタイズ] を選択します。

5 [編集]をクリックしてルートのアドバタイズの設定を編集します。

次のスイッチを切り替えることができます。

- [状態]
- [全ての NSX 接続ルートのアドバタイズ]
- [全ての NAT ルートのアドバタイズ]
- [全てのスタティック ルートのアドバタイズ]
- [全てのロードバランサ VIP ルートのアドバタイズ]
- [全てのロードバランサ SNAT IP ルートのアドバタイズ]
- [DNS フォワーダのすべてのルートをアドバタイズ]
- a [保存] をクリックします。

6 [追加] をクリックしてルートをアドバタイズします。

- a 名前を入力します。必要に応じて説明も入力します。
- b ルート プリフィックスを CIDR 形式で入力します。
- c [フィルタの適用] をクリックし、次のオプションを設定します。

[アクション]	[許可] または [拒否] を指定します。
[ルート タイプの一致]	次から 1 つ以上を選択します。 <ul style="list-style-type: none"> ■ [任意] ■ [NSX 直接接続] ■ [Tier-1 LB VIP] ■ [静的] ■ [Tier-1 NAT] ■ [Tier-1 LB SNAT]
[プリフィックス演算子]	[GE] または [EQ] を選択します。

- d [追加] 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。[Tier-0 論理ルーター](#) を参照してください。

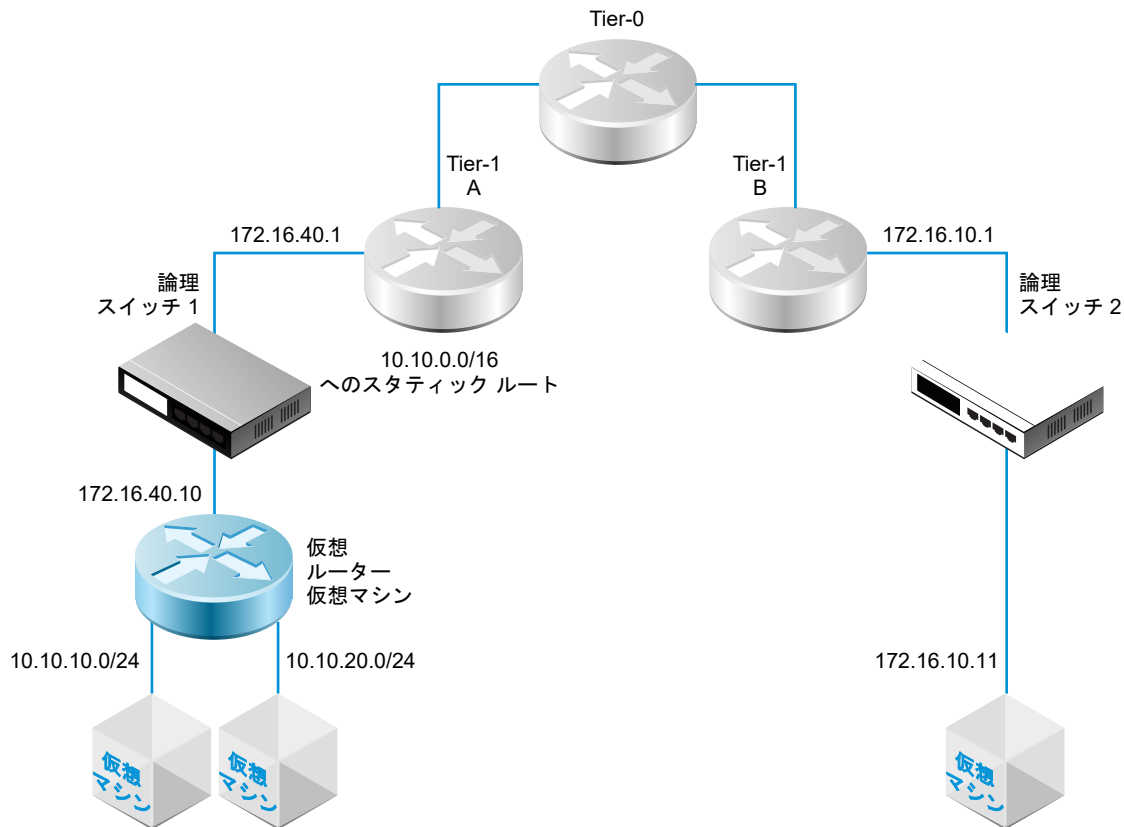
Tier-0 分散論理ルーターがすでに Tier-1 分散論理ルーターに接続されている場合は、Tier-0 ルーターが Tier-1 ルーターに接続されたルートを学習していることを確認することができます。[Tier-0 ルーターが Tier-1 ルーターからルートを学習したことの確認](#) を参照してください。

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 Data Center 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 Data Center 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 Data Center 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 14-2. Tier-1 論理ルーターのスタティック ルート トポロジ



再帰的なスタティック ルートがサポートされています。

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 論理ルーターへのダウンリンク 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 Tier-1 ルーターの名前をクリックします。
- 4 [ルーティング] 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] を選択します。
- 5 [追加] 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。

IPv6 ベースのスタティック ルートがサポートされています。IPv6 プリフィックスに指定できるのは、IPv6 ネクスト ホップのみです。

たとえば、10.10.10.0/16 または IPv6 アドレスを指定できます。

7 [追加] 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] をクリックします。

8 ダイアログ ボックスの下部にある [追加] 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] > [ルート アドバタイズ] の順に選択します。

10 [編集] をクリックし、[全てのスタティック ルートのアドバタイズ] を選択します。

11 [保存] をクリックします。

スタティック ルートが NSX-T Data Center オーバーレイ全体に伝達されます。

スタンドアローン Tier-1 論理ルーターの作成

スタンドアローン Tier-1 論理ルーターにはダウンリンクがなく、Tier-0 ルーターに接続されていません。サービス ルーターはありますが、分散ルーターはありません。1 台の NSX Edge ノード、またはアクティブ/スタンバイ モードの 2 台の NSX Edge ノード上でサービス ルーターを展開することができます。

スタンドアローン Tier-1 論理ルーターには以下の条件が必要です。

- Tier-0 論理ルーターに接続されていない。
- ダウンリンクがない。
- 統合サービス ポート (CSP) は、ロード バランサ (LB) サービスの接続に使用する場合に 1 つのみ設定可能。
- オーバーレイ論理スイッチまたは VLAN 論理スイッチにのみ接続可能。
- サービスの IPsec、DNAT、ファイアウォール、ロード バランサ、サービス挿入の任意の組み合わせがサポートされます。入力方向の場合、処理の順序は IPsec、DNAT、ファイアウォール、ロード バランサ - サービス挿入の順になります。出力方向の場合、処理の順序は、サービス挿入、ロード バランサ、ファイアウォール、DNAT、IPsec の順になります。

通常、スタンドアローン Tier-1 論理ルーターは、標準 Tier-1 論理ルーターが接続されている論理スイッチに接続されます。スタティック ルートおよびルート アドバタイズを設定すると、スタンドアローン Tier-1 論理ルーターは標準 Tier-1 論理ルーターを介して他のデバイスと通信できるようになります。

スタンドアローン Tier-1 論理ルーターを使用する前に、次の点に注意します。

- スタンドアローン Tier-1 論理ルーターのデフォルト ゲートウェイを指定するには、スタティック ルートを追加する必要があります。サブネットには 0.0.0.0/0 を指定する必要があります。ネクスト ホップは、同じスイッチに接続されている標準 Tier-1 ルーターの IP アドレスになります。

- スタンドアローン ルーター上の ARP プロキシはサポートされています。CSP のサブネットでは、LB 仮想サーバの IP アドレスまたは LB SNAT IP アドレスを設定します。たとえば、CSP IP アドレスが 1.1.1.1/24 の場合、仮想 IP アドレスは 1.1.1.2 にできます。また、2.2.2.2 のトラフィックがスタンドアローン ルーターに到達するようにルーティングが適切に設定されている場合は、2.2.2.2 などの別のサブネット内の IP アドレスに使用できます。
- NSX Edge 仮想マシンの場合、VLAN でバックアップされている同じ論理スイッチ、または VLAN でバックアップされている、同じ VLAN ID を持つ論理スイッチに複数の CSP を接続することはできません。

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 [ネットワークとセキュリティの詳細設定] - [ルーター] - [ルーター] - [追加] を選択します。
- 3 [Tier-1 ルーター] を選択して、論理ルーターの名前と、必要に応じて説明を入力します。
- 4 (必須) この Tier-1 論理ルーターに接続する NSX Edge クラスタを選択します。
- 5 (必須) フェイルオーバー モードおよびクラスタ メンバーを選択します。

オプション	説明
プリエンブティブ	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。
非プリエンブティブ	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。

- 6 [追加] をクリックします。
- 7 作成したルーターの名前をクリックします。
- 8 [設定] タブをクリックし、[ルーター ポート] を選択します。
- 9 [追加] をクリックします。
- 10 ルーター ポートの名前と、必要に応じて説明を入力します。
- 11 [タイプ] フィールドで、[統合] を選択します。
- 12 [uRPF モード] では、[厳密] または [なし] を選択します。
URPF (Unicast Reverse Path Forwarding) はセキュリティ機能です。
- 13 (必須) 論理スイッチを選択します。
- 14 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。
- 15 ルーター ポート IP アドレスを CIDR 表記で入力します。
- 16 [追加] をクリックします。

Tier-0 論理ルーター

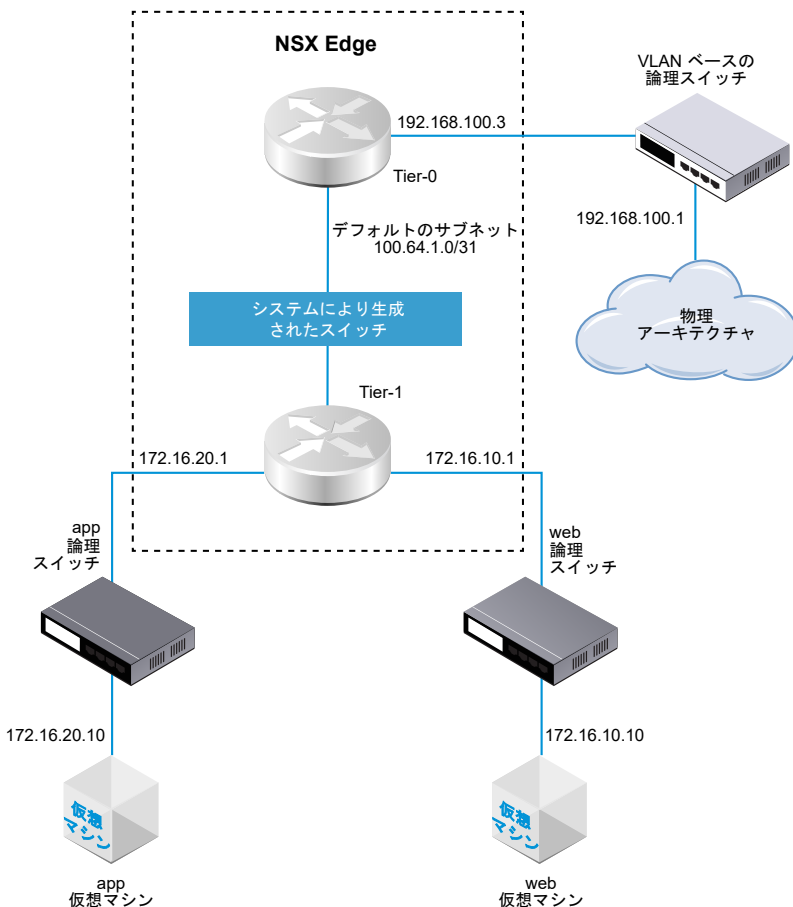
Tier-0 論理ルーターは、論理ネットワークと物理ネットワーク間のゲートウェイ サービスを提供します。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

Edge ノードは、1つの Tier-0 ゲートウェイまたは論理ルーターのみをサポートします。Tier-0 ゲートウェイまたは論理ルーターを作成する場合は、NSX Edge クラスターの Edge ノードの数以上の Tier-0 ゲートウェイまたは論理ルーターを作成しないようにしてください。

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 14-3. 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せん。

一部のシナリオでは、外部クライアントはループバックまたは IKE IP ポートにバインドされた MAC アドレスに ARP 要求を送信します。ただし、ループバックおよび IKE IP ポートでは MAC アドレスを使用しないため、このようなクエリを処理できません。ループバックと IKE IP ポートの代わりに ARP 要求を処理するために、Tier-0 論理ルーターのアップリンクおよび中央のサービス ポートにプロキシ ARP が実装されています。

Tier-0 論理ルーターに DNAT、IPsec、Edge ファイアウォールを設定すると、トラフィックは、IPsec、DNAT、Edge ファイアウォールの順に処理されます。

Tier-0 または Tier-1 論理ルーターで、さまざまなタイプのポートを設定できます。その 1 つが中央のサービス ポート (CSP) です。VLAN でバックアップされた論理スイッチに接続するか、スタンドアローンの Tier-1 論理ルーターを作成する場合は、アクティブ/スタンバイ モードの Tier-0 論理ルーターまたは Tier-1 論理ルーターで CSP を設定する必要があります。CSP は、アクティブ/スタンバイ モードの Tier-0 論理ルーターまたは Tier-1 論理ルーターで次のサービスをサポートします。

- NAT
- ロード バランシング
- ステートフル ファイアウォール
- VPN (IPsec および L2VPN)

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 Data Center 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 Data Center インストール ガイド』を参照してください。
- NSX Edge クラスタが設定されていることを確認します。『NSX-T Data Center 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。[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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ルーター] - [ルーター] - [追加] を選択します。
- 3 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。
- 4 Tier-0 分散論理ルーターの名前を割り当てます。
- 5 この Tier-0 論理ルーターをバックアップする既存の NSX Edge クラスタをドロップダウン メニューから選択します。

6 (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。

7 (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。

8 (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 100.64.0.0/16 になります。Tier-0 から Tier-1 の各ピア接続には、100.64.0.0/16 アドレス空間内で /31 サブネットが提供されます。

9 [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。

10 (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。

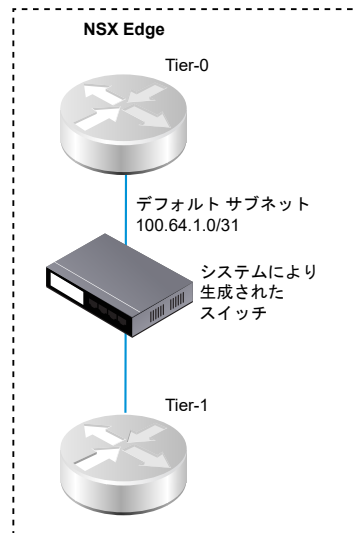
Tier-0 分散論理ルーターを VLAN 論理スイッチに接続するように設定し、外部ネットワークへのアップリンクを作成します。[NSX Edge アップリンク用の VLAN 論理スイッチへの Tier-0 論理ルーターの接続](#) を参照してください。

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 100.64.0.0/16 です。Tier-0 から Tier-1 の各ピア接続には、100.64.0.0/16 アドレス空間内で /31 サブネットが提供されます。アドレス空間を Tier-0 の [サマリ] - [詳細] で設定することもできます。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 NSX 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。NSX 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。

NSX 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 Data Center は指定されたクラスタからバックアップ用の Edge デバイスを設定します。

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

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

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

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

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

次のステップ

Tier-0 ルーターが Tier-1 ルーターによってアド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 Data Center 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 Data Center 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

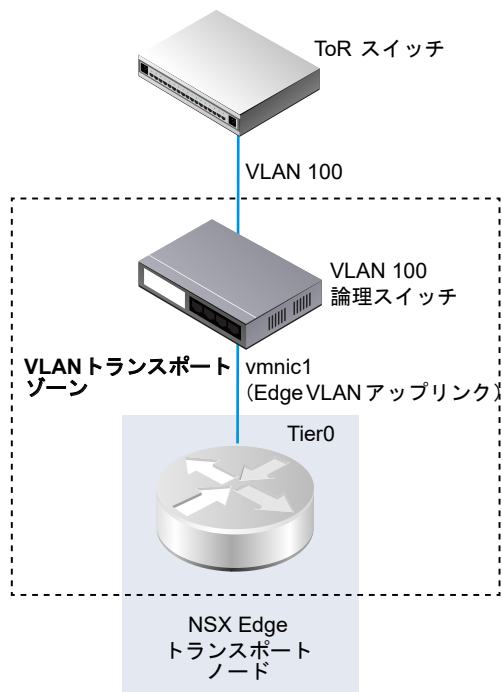
Total number of routes: 7

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
```

NSX Edge アップリンク用の VLAN 論理スイッチへの Tier-0 論理ルーターの接続

NSX Edge アップリンクを作成するには、Tier-0 ルーターを VLAN スイッチに接続する必要があります。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 スイッチに接続しているポートと同じサブネットにある IP アドレスを CIDR 形式で入力します。

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。[NSX Edge アップリンク用の 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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。

Tier-0 または Tier-1 論理ルーターへの VLAN ポートの追加

VLAN でバックアップされている論理スイッチのみを配置している場合、NSX-T Data Center がレイヤー 3 サービスを提供できるように、Tier-0 または Tier-1 ルーター上の VLAN ポートにスイッチを接続することができます。

手順

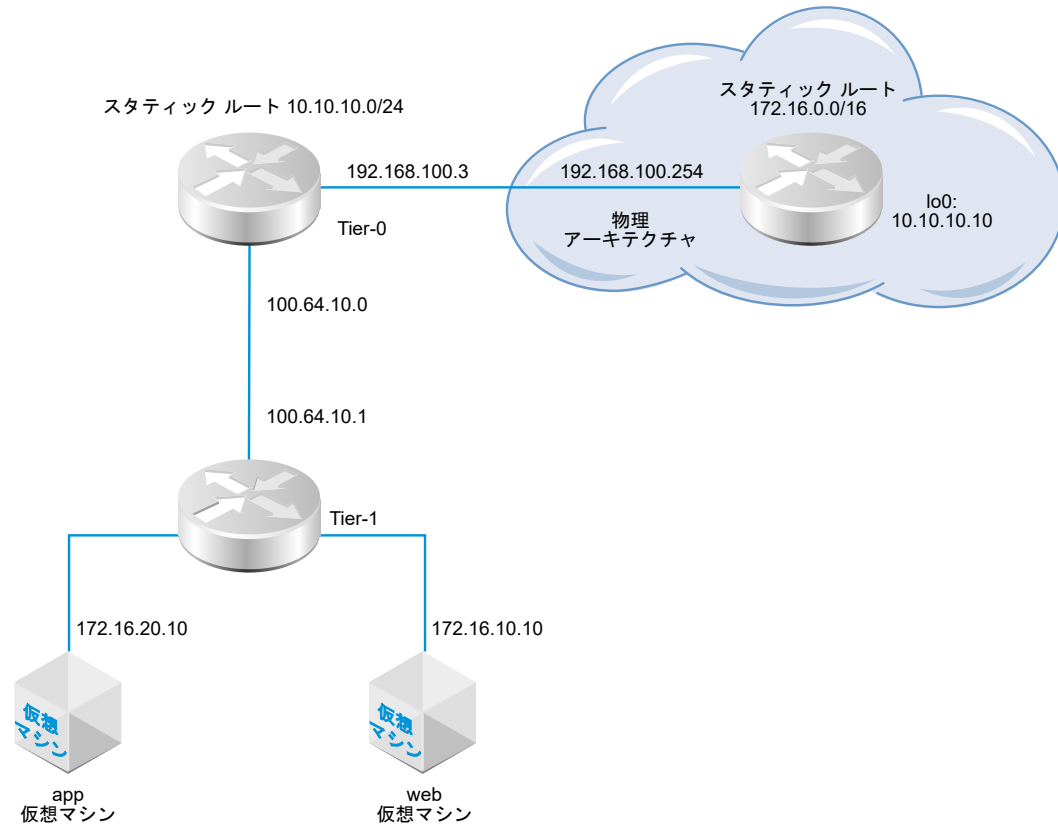
- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 ルーターの名前をクリックします。
- 4 [設定] タブをクリックし、[ルーター ポート] を選択します。
- 5 [追加] をクリックします。
- 6 ルーター ポートの名前と、必要に応じて説明を入力します。
- 7 [タイプ] フィールドで、[統合] を選択します。
- 8 [uRPF モード] では、[厳密] または [なし] を選択します。
uRPF (unicast Reverse Path Forwarding) は、セキュリティ機能です。
- 9 (必須) 論理スイッチを選択します。
- 10 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。
- 11 ルーター ポート IP アドレスを CIDR 表記で入力します。
- 12 [追加] をクリックします。

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、10.10.10.10/32 アドレスは外部ルーターのループバック インターフェイス上で設定されます。外部ルーターには、app 仮想マシンと web 仮想マシンにアクセスするための 172.16.0.0/16 プリフィックスへのスタティック ルートがあります。

図 14-4. スタティック ルート トポロジ



再帰的なスタティック ルートがサポートされています。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 [スタティック ルート] を選択します。
- 5 [追加] 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] 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。

- 8 アドミニストレーティブ ディスタンスを指定します。
- 9 ドロップ ダウン リストから論理ルーター ポートを選択します。

リストには、IPsec 仮想トンネル インターフェイス (VTI) ポートが含まれています。

- 10 [追加] ボタンをクリックします。

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 route 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 Data Center 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。

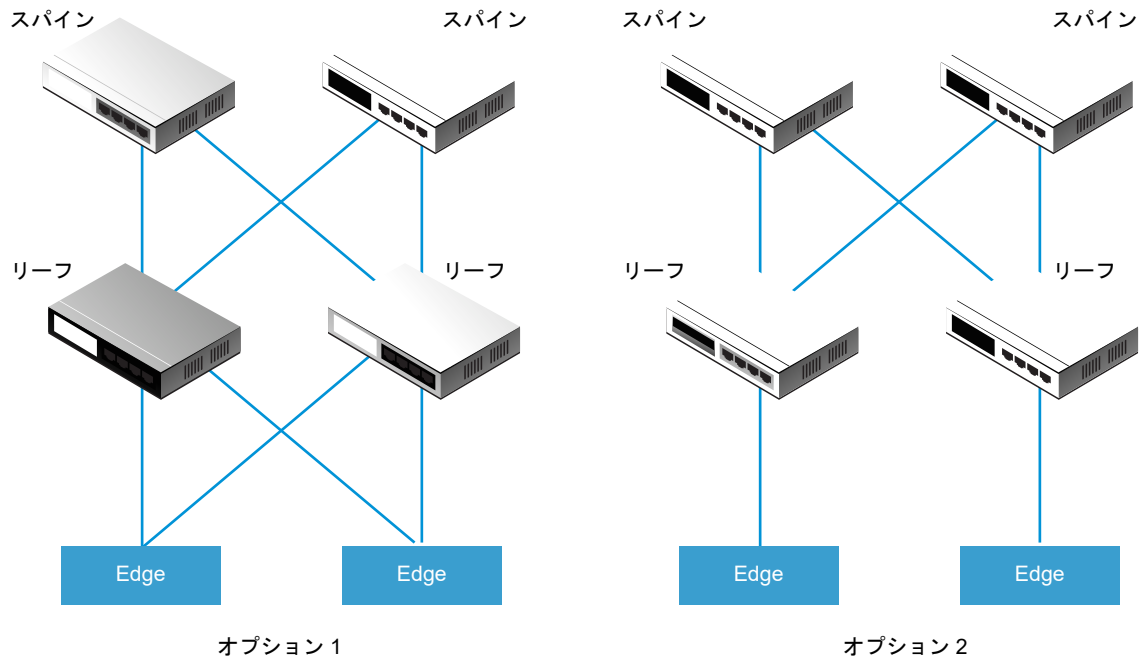
```
ping 10.10.10.10
```

```
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 構成オプション

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 プレフィックスを含める必要があります。Tier-O 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-O 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-O 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-O 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-O 分散論理ルーター設定に Tier-O 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-O 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-O 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または内部 BGP (eBGP/iBGP) 接続を設定します。

iBGP 機能には次の機能と制限があります。

- 再配分、プリフィックス リスト、およびルート マップがサポートされます。
- ルート リフレクタはサポートされません。
- BGP コンフェデレーションはサポートされません。

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、リモート AS 番号を設定する必要があります。EBGP ネイバーは、Tier-0 アップリンクと同じサブネットに直接接続している必要があります。同じサブネット内にない場合は、BGP マルチホップを使用する必要があります。

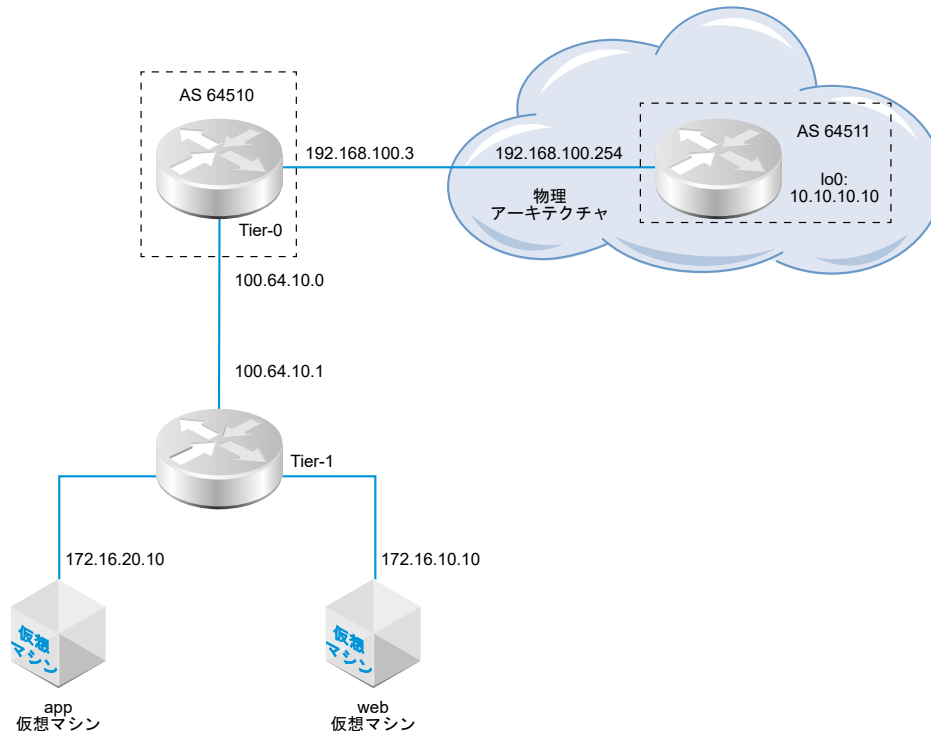
アクティブ/アクティブ モードの Tier-0 論理ルーターは、SR (サービス ルーター) 間をサポートします。ルーター 1 が Northbound 物理ルーターと通信できない場合、トラフィックはアクティブ/アクティブ クラスタ内のルーター 2 に再ルーティングされます。ルーター 2 が物理ルーターと通信できる場合、ルーター 1 と物理ルーター間のトラフィックは影響を受けません。

アクティブ/スタンバイ モードの Tier-1 論理ルーターにアクティブ/アクティブ モードの Tier-0 論理ルーターに接続しているトポロジでは、サービス ルーター (SR) 間のルーティングを有効にして、非対称ルーティングを処理する必要があります。サービス ルーターの 1 つにスタティック ルートを設定している場合や、1 つのサービス ルーターが別のサービス ルーターのアップリンクにアクセスする必要がある場合は、非対称ルーティングを使用します。また、次の点に注意してください。

- 1 つのサービス ルーター (たとえば、Edge ノード #1 の SR) にスタティック ルートが設定されている場合、別のサービス ルーター (たとえば、Edge ノード #2 の SR #2) が eBGP ピアから同じルートを学習し、このルートが SR #1 のスタティック ルートよりも優先される場合があります。これにより、パフォーマンスが向上することもあります。SR #2 が SR #1 で設定されたスタティック ルートを使用するには、Tier-1 論理ルーターをプリエンプティブ モードで設定し、Edge ノード #1 を優先ノードとして設定します。
- Tier-0 論理ルーターに Edge ノード #1 のアップリンク ポートがあり、Edge ノード #2 に別のアップリンク ポートがある場合、この 2 つのアップリンクが異なるサブネットに属していれば、テナント仮想マシンからアップリンクへの ping トラフィックが機能します。2 つのアップリンクが同じサブネットにある場合、ping トラフィックは失敗します。

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 14-5. BGP 接続トポロジ



BGP または BFD に関連する接続で障害が発生した場合は、次のシナリオに注意してください。

- BGP のみが設定されている場合、すべての BGP ネイバーが停止すると、サービス ルーターの状態は「停止」になります。
- BFD のみが設定されている場合、すべての BFD ネイバーが停止すると、サービス ルーターの状態は「停止」になります。
- BGP と BFD が設定されている場合、すべての BGP ネイバーと BFD ネイバーが停止すると、サービス ルーターの状態は「停止」になります。
- BGP とスタティック ルートが設定されている場合、すべての BGP ネイバーが停止すると、サービス ルーターの状態は「停止」になります。
- スタティック ルートのみが設定されている場合は、ノードで障害が発生するか、メンテナンス モードになっている場合を除き、サービス ルーターの状態は常に「稼動中」になります。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 AS 番号を入力します。
例：64510。
 - b BGP の有効化と無効化を切り替えるには、[状態] ボタンをクリックします。
 - c ECMP の有効化と無効化を切り替えるには、[ECMP] をクリックします。
 - d [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 リスタートを有効または無効にします。

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 NSX Edge クラスターの Edge ノードが 1 台の場合のみです。
 - e この論理ルーターがアクティブ/アクティブ モードで動作する場合は、[サービス ルーターのルーティング間] をクリックし、サービス ルーターのルーティングの有効化と無効化を切り替えます。
 - f ルートの集約を設定します。
 - g [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 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 AS の番号を入力します。
たとえば、64511 (eBGP ネイバー) または 64510 (iBGP ネイバー) を使用します。
- 10 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 [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 [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。
- 13 [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。

注： このリリースでは、仮想トンネル インターフェイス (VTI) ポートを経由する BFD はサポートされていません。

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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 [状態] 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、管理状態を [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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 [編集] をクリックして、ルート再配分を有効または無効にします。
- 6 [追加] をクリックして、一連のルート再配分基準を追加します。

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	次の送信元を 1 つ以上選択します。 <ul style="list-style-type: none"> ■ [TO 接続済み] ■ [TO アップリンク] ■ [TO ダウンリンク] ■ [TO CSP] ■ [TO ループバック] ■ [TO スタティック] ■ [TO NAT] ■ [TO DNS フォワーダの IP アドレス] ■ [TO IPsec ローカル IP アドレス] ■ [T1 接続済み] ■ [T1 CSP] ■ [T1 ダウンリンク] ■ [T1 スタティック] ■ [T1 LB SNAT] ■ [T1 NAT] ■ [T1 LB VIP] ■ [T1 DNS フォワーダの IP アドレス]
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。

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 Data Center 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 Data Center 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 Data Center 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 Data Center 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 Data Center 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

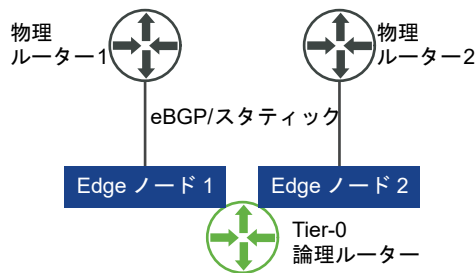
ECMP など、その他のルーティング機能を設定します。

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 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、NSX 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 を使用するには、Tier-0 論理ルーターがアクティブ/アクティブ モードにする必要があります。最大 8 つの ECMP パスがサポートされます。NSX Edge での ECMP の実装は、プロトコル番号、送信元アドレス、宛先アドレス、送信元ポートと宛先ポートの 5-tuple に基づいています。ECMP パス間でデータを転送するアルゴリズムはラウンド ロビン方式ではありません。そのため、一部のパスで他のパスよりも多くのトラフィックが発生することがあります。プロトコルが IPv6 で、IPv6 ヘッダーに複数の拡張ヘッダーがある場合、ECMP は送信元アドレスと宛先アドレスにのみ基づきます。

図 14-6. ECMP ルーティング トポロジ



たとえば、上記のトポロジでは、2 ノード NSX Edge クラスタで 1 台の Tier-0 論理ルーターがアクティブ/アクティブ モードで実行されています。2 個のアップリンク ポートが各 Edge ノードに 1 個ずつ設定されています。

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 Data Center 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 Data Center 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>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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。
MTU	このフィールドを空のままにすると、デフォルトの 1500 が使用されます。
トランスポート ノード	ドロップダウン メニューから Edge のトランスポート ノードを割り当てます。
uRPF モード	Unicast Reverse Path Forwarding はセキュリティ機能です。複数のアクティブ/アクティブ Edge ノードが ECMP モードになっている場合は、[なし] に設定することをおすすめします。デフォルトは、[厳密] です。
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>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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。
- 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。

```
vrf 5
```

```
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 分散ルーターが接続されていることを確認します。
- 8 2 つの Edge ノードで SSH セッションを開始します。

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

UUID のルート タイプは NSX_CONNECTED と表示されます。

- 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>
```

- Tier-0 ルーターに接続された送信元仮想マシンから宛先仮想マシンへのトラフィックを生成できる任意のツールを使用します。
- 2 台の Edge ノード上のトラフィックを確認します。

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。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 リストを作成する際は、特定のネットワーク アドレスを指定しない IP プリフィックス（ドロップダウン リストから [任意] を選択）を作成し、それ以外のすべてのルートを許可するには、[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

- 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。
- [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- Tier-0 論理ルーターを選択します。
- [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。
- [追加] をクリックします。
- IP プリフィックス リストの名前を入力します。

- 7 プリフィックスを指定するには、[追加] をクリックします。
 - a IP アドレスを CIDR 形式で入力します。
例 : 192.168.100.3/27。
 - b 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。
 - c (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。
- 8 追加のプリフィックスを指定するには、前の手順を繰り返します。
- 9 ウィンドウの下部にある [追加] をクリックします。

コミュニティ リストの作成

コミュニティ リストに基づいたルート マップを設定できるように、BGP コミュニティ リストを作成できます。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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 [コミュニティ リスト] を選択します。
- 5 [追加] をクリックします。
- 6 コミュニティ リストの名前を入力します。
- 7 aa:nn 形式を使用してコミュニティを指定し (例 : 300:500)、Enter キーを押します。同じ手順を繰り返して、コミュニティをさらに追加します。

また、ドロップダウン メニューの矢印をクリックして、次のうち 1 つ以上を選択することもできます。
 - NO_EXPORT_SUBCONFED : EBGp ピアにアドバタイズしません。
 - NO_ADVERTISE : どのピアにもアドバタイズしません。
 - 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。
- 8 [追加] をクリックします。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 Tier-0 論理ルーターを選択します。
- 4 [ルーティング] - [ルート マップ]の順に選択します。
- 5 [追加] 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] 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 [IP プリフィックス リストとコミュニティ リストとの一致] 列を編集して、IP プリフィックス リストとコミュニティ リストのどちらか一方を選択します。
- 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"> ■ NO_EXPORT_SUBCONFED：EBGP ピアにアドバタイズしません。 ■ NO_ADVERTISE：どのピアにもアドバタイズしません。 ■ 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。

- 10 [アクション] 列で、[許可] または [拒否] 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] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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。

NAT を構成するには、[ネットワークとセキュリティの詳細設定] タブを使用します。

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 [NSX Manager の概要](#) 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。

- [ネットワーク アドレス変換](#)

ネットワーク アドレス変換

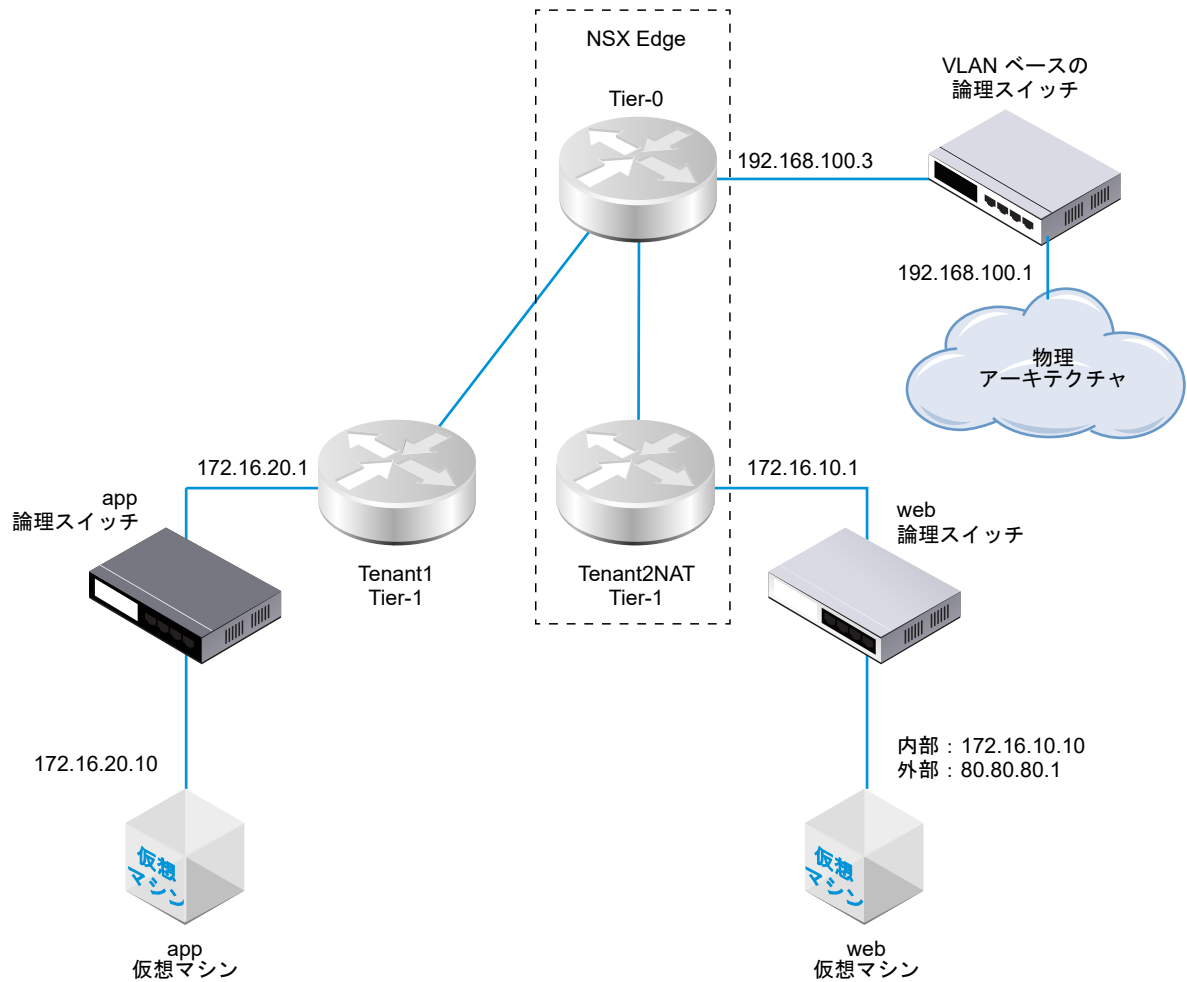
NSX-T Data Center のネットワークアドレス変換 (NAT) は、Tier-0 および Tier-1 分散論理ルーター上で設定することができます。

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。

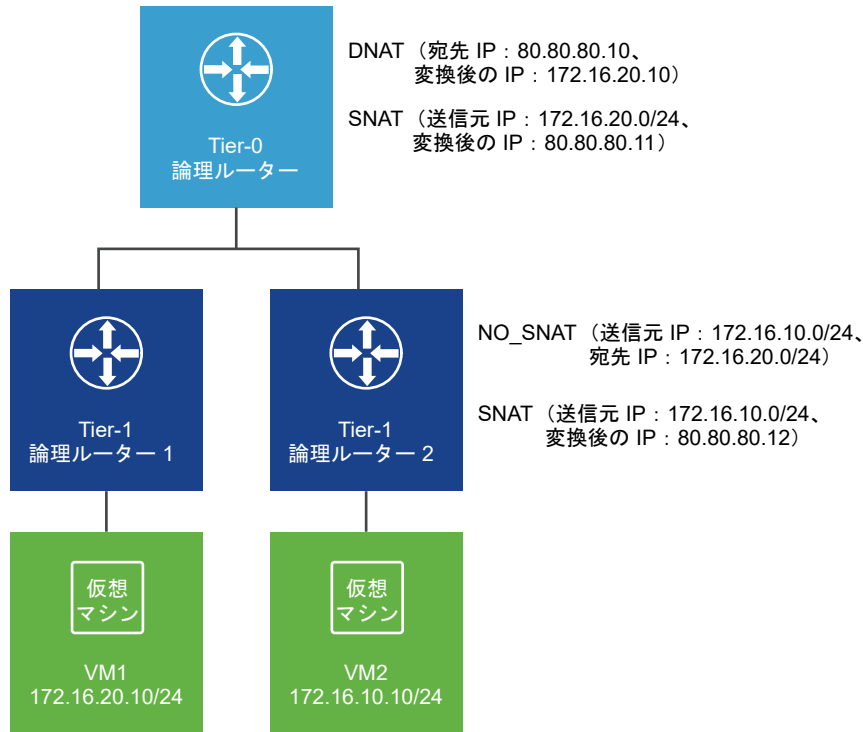
NAT は、Tier-0 分散論理ルーターへの接続時に Tenant2NAT 分散論理ルーターのアップリンクで適用されます。

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 15-1. NAT トポロジ



注：次のシナリオでは、NAT ヘアピンはサポートされていません。Tier-0 論理ルーターには DNAT と SNAT が設定されています。Tier-1 論理ルーター 2 には NO_SNAT と SNAT が設定されています。VM2 は、VM1 の外部アドレス 80.80.80.10 を使用して VM1 にアクセスできません。



次のセクションでは、マネージャ UI を使用して NAT ルールを作成する方法について説明します。また、API 呼び出し (POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple) を使用して、同時に複数の NAT ルールを作成することもできます。詳細については、『NSX-T Data Center API ガイド』を参照してください。

Tier-1 NAT

Tier-1 論理ルーターは、送信元 NAT (SNAT)、宛先 NAT (DNAT)、および再帰 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。

送信元 NAT を有効または無効にするルールを作成できます。

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 IP アドレスを 172.16.10.10 から 80.80.80.1 に変更します。送信元のパブリック IP 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。NSX Edge アップリンク用の 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、NSX 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 論理ルーターへのダウンリンク 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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] - [NAT] の順に選択します。
- 5 [追加] 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] で、[SNAT] を選択して送信元 NAT を有効にするか、[NO_SNAT] を選択して送信元 NAT を無効にします。
- 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] が選択されます。
- 9 (オプション) [送信元の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。
このフィールド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、送信元の IP アドレスは 172.16.10.10 です。
- 10 (オプション) [宛先の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。
このフィールド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 [アクション] を [SNAT] に設定している場合は、[変換された IP アドレス] に IP アドレスまたは IP アドレスの範囲を CIDR 形式で指定します。
この例では、変換された IP アドレスは 80.80.80.1 です。
- 12 (オプション) [適用先] にはルーター ポートを選択します。
- 13 (オプション) ルールの状態を設定します。
ルールはデフォルトで有効になっています。

14 （オプション） ログの収集状態を変更します。

ログの記録は、デフォルトで無効になっています。

15 （オプション） ファイアウォールのバイパス設定を変更します。

設定はデフォルトで有効になっています。

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。



The screenshot shows the 'Tenant2NAT' configuration page with the 'サービス' (Services) tab selected. Below the 'NAT' header, there is a message '統計情報は収集されませんでした' (Statistics information was not collected) and buttons for '+ 追加' (Add), '編集' (Edit), and '削除' (Delete). A table lists NAT rules. The first rule has ID 1031, action SNAT, and is enabled (green checkmark). The table columns are: ID, アクション (Action), 一致 (Match) with sub-columns for protocol, source IP, source port, destination IP, and destination port, 変換 (Translation) with sub-columns for IP address and port, 適用先 (Destination), and 統計 (Statistics).

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		
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。

宛先 NAT の有効/無効を切り替えるルールを作成できます。

この例ではアプリケーション仮想マシンからパケットを受信すると、Tenant2NAT Tier-1 ルーターは、パケットの宛先 IP アドレスを 172.16.10.10 から 80.80.80.1 に変更します。宛先のパブリック IP 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。 [NSX Edge アップリンク用の 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、NSX 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 論理ルーターへのダウンリンク 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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] - [NAT] の順に選択します。
- 5 [追加] 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] で、宛先 NAT を有効にする場合は [DNAT]、宛先 NAT を無効にする場合は [NO_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] が選択されます。
- 9 (オプション) [送信元の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。
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。
- 10 [宛先の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。
この例では、宛先の IP アドレスは 80.80.80.1 です。
- 11 [アクション] が [DNAT] の場合、[変換された IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。
この例では、内部/変換後 IP アドレスは 172.16.10.10 です。
- 12 (オプション) [アクション] が [DNAT] の場合、[変換されたポート] に、変換されたポートを指定します。
- 13 (オプション) [適用先] にはルーター ポートを選択します。
- 14 (オプション) ルールの状態を設定します。
ルールはデフォルトで有効になっています。
- 15 (オプション) ログの収集状態を変更します。
ログの記録は、デフォルトで無効になっています。
- 16 (オプション) ファイアウォールのバイパス設定を変更します。
設定はデフォルトで有効になっています。

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-O 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-O ルーターを設定します。

アップストリームの Tier-O 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-O 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 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] > [ルート アドバタイズ] の順に選択します。
- 5 [編集]をクリックしてルートのアドバタイズの設定を編集します。

次のスイッチを切り替えることができます。

- [状態]
- [全ての NSX 接続ルートのアドバタイズ]
- [全ての NAT ルートのアドバタイズ]
- [全てのスタティック ルートのアドバタイズ]
- [全てのロードバランサ VIP ルートのアドバタイズ]
- [全てのロードバランサ SNAT IP ルートのアドバタイズ]
- [DNS フォワーダのすべてのルートをアドバタイズ]

- 6 [保存] をクリックします。

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>>) に管理者権限でログインします。
- 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 [編集] をクリックして、ルート再配分を有効または無効にします。
- 6 [追加] をクリックして、一連のルート再配分基準を追加します。

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	次の送信元を 1 つ以上選択します。 <ul style="list-style-type: none"> ■ [TO 接続済み] ■ [TO アップリンク] ■ [TO ダウンリンク] ■ [TO CSP] ■ [TO ループバック] ■ [TO スタティック] ■ [TO NAT] ■ [TO DNS フォワーダの IP アドレス] ■ [TO IPsec ローカル IP アドレス] ■ [T1 接続済み] ■ [T1 CSP] ■ [T1 ダウンリンク] ■ [T1 スタティック] ■ [T1 LB SNAT] ■ [T1 NAT] ■ [T1 LB VIP] ■ [T1 DNS フォワーダの IP アドレス]
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。

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 `get 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

アクティブ/スタンバイ モードの Tier-0 論理ルーターは、送信元 NAT (SNAT)、宛先 NAT (DNAT)、および再帰 NAT をサポートします。アクティブ/アクティブ モードの Tier-0 論理ルーターは、再帰 NAT のみをサポートします。

Tier-0 論理ルーター上での送信元および宛先 NAT の設定

アクティブ/スタンバイ モードで実行されている Tier-0 論理ルーター上で送信元および宛先 NAT を設定できます。

また、IP アドレスやアドレス範囲の SNAT または DNAT を無効にすることもできます。1 つのアドレスに複数の NAT ルールが適用されている場合は、優先順位が最も高いルールが適用されます。

Tier-0 論理ルーターのアップリンクで設定された SNAT は、Tier-1 論理ルーターと Tier-0 論理ルーターの別のアップリンクからのトラフィックを処理します。

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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 Tier-0 分散論理ルーターをクリックします。

4 [サービス] - [NAT] の順に選択します。

5 [追加] をクリックして、NAT ルールを追加します。

6 優先順位を指定します。

小さい値ほど、優先順位が高くなります。

7 [アクション] で、[SNAT]、[DNAT]、[Reflexive]、[NO_SNAT]、または [NO_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] が選択されます。

9 (必須) [送信元の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。

このフィールドを空白にしておくと、この NAT ルールはローカル サブネットの外部のすべての送信元に適用されます。

10 [宛先の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。

11 [変換された IP アドレス] に、IP アドレスまたは IP アドレスの範囲を CIDR 形式で指定します。

12 (オプション) [アクション] が [DNAT] の場合、[変換されたポート] に、変換されたポートを指定します。

13 (オプション) [適用先] にはルーター ポートを選択します。

14 (オプション) ルールの状態を設定します。

ルールはデフォルトで有効になっています。

15 (オプション) ログの収集状態を変更します。

ログの記録は、デフォルトで無効になっています。

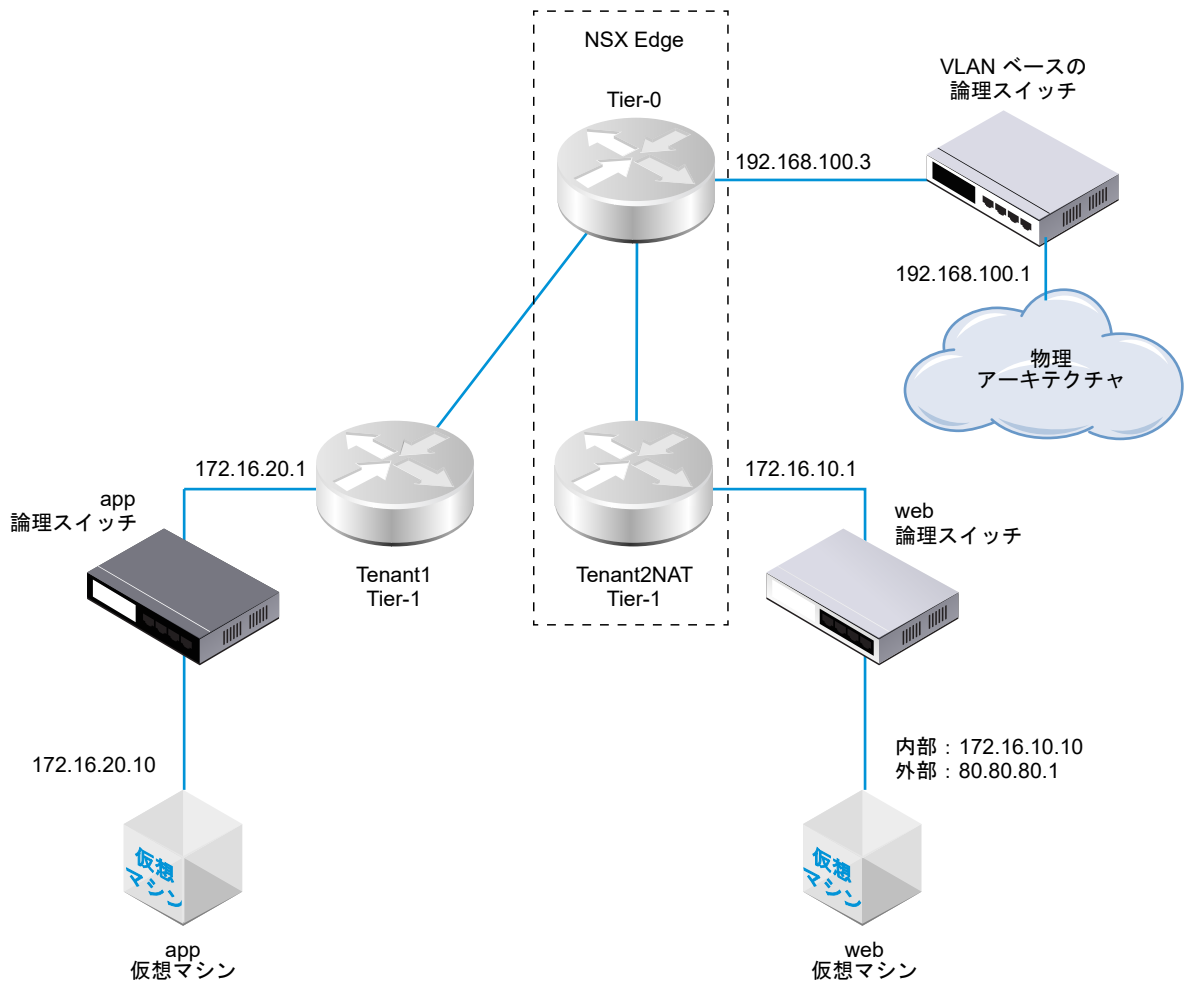
16 (オプション) ファイアウォールのバイパス設定を変更します。

設定はデフォルトで有効になっています。

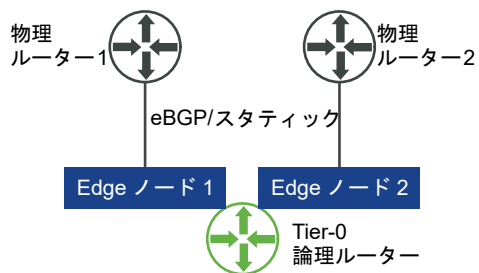
再帰 NAT

Tier-0 論理ルーターがアクティブ/アクティブ 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 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) を設定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 IP アドレスを 172.16.10.10 から 80.80.80.1 に変更します。送信元のパブリック IP 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。



以下に示すように 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 または Tier-1 論理ルーター上の再帰 NAT の設定

Tier-0 または Tier-1 論理ルーターがアクティブ/アクティブ 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 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。

再帰 NAT の場合は、変換される 1 つの送信元アドレスまたはアドレスの範囲を設定できます。送信元アドレスの範囲を設定する場合は、変換先アドレスの範囲も設定する必要があります。2 つの範囲のサイズは同じである必要があります。アドレス変換は確定的です。つまり、送信元アドレスの範囲内の最初のアドレスは変換先アドレスの範囲内の最初のアドレスに、送信元アドレスの範囲内の 2 番目のアドレスは変換先アドレスの範囲内の 2 番目のアドレスに変換され、以下同様に変換されます。

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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 再帰 NAT を設定する Tier-0 または Tier-1 論理ルーターをクリックします。
- 4 [サービス] - [NAT] の順に選択します。
- 5 [追加] 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] で、[再帰] を選択します。
- 8 [送信元の IP アドレス] に、IP アドレスまたは IP アドレス範囲を CIDR 形式で指定します。
- 9 [変換された IP アドレス] に、IP アドレスまたは IP アドレスの範囲を CIDR 形式で指定します。
- 10 (オプション) ルールの状態を設定します。
ルールはデフォルトで有効になっています。
- 11 (オプション) ログの収集状態を変更します。
ログの記録は、デフォルトで無効になっています。
- 12 (オプション) ファイアウォールのバイパス設定を変更します。
設定はデフォルトで有効になっています。

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。

Tier0-LR-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: 2019年3月6日 18:20:11

0

アクティブセッション

0

パケットの数

0

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		
▼ 優先度: 1024										
2048	再帰	任意	80.80.80.1	任意	任意	任意	172.16.10.10	任意		

高度なグループ オブジェクト

16

IP セット、IP アドレス プール、MAC セット、NS グループ、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。

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 NSX Manager の概要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 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 NS グループのメンバーである場合があります。この方法で作成された IP セットは、ポリシー モードで表示されません。ポリシー モードでは、グループを作成して、IP アドレス、範囲、ネットワーク アドレス、または MAC アドレスとしてメンバーを追加できます。この操作を行うには、[インベントリ] - [グループ] - [メンバーの設定] の順に移動し、IP または MAC アドレスを指定します。

注： IPv4 アドレスと IPv6 アドレスは、ファイアウォール ルールの送信元または宛先の範囲でサポートされます。

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 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [グループ] - [IP セット] - [追加] を選択します。
- 3 名前を入力します。
- 4 (オプション) 説明を入力します。
- 5 [メンバー] には、個々の IP アドレス、IP アドレス範囲、およびサブネットをカンマ区切りのリストで入力します。
- 6 [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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [グループ] - [IP アドレス プール] - [追加] を選択します。
- 3 新規 IP アドレス プールの名前を入力します。
- 4 (オプション) 説明を入力します。
- 5 [追加] をクリックします。
- 6 IP アドレス範囲のセルをクリックし、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。
- 7 (オプション) ゲートウェイを入力します。
- 8 CIDR IP アドレスをサフィックス付きで入力します。
- 9 (オプション) DNS サーバを入力します。
- 10 (オプション) DNS サフィックスを入力します。
- 11 [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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [グループ] - [MAC セット] - [追加] を選択します。
- 3 名前を入力します。

- 4 (オプション) 説明を入力します。
- 5 MAC アドレスをカンマ区切りのリストで入力します。
- 6 [追加] 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。論理スイッチ、論理ポート、および仮想マシンを含む NSGroup は送信元および宛先として指定するほか、ファイアウォール ルールの Applied To フィールドに指定することができます。IPset および MACSet を含む NSGroup は、分散ファイアウォールの Applied To フィールドでは無視されます。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

NSGroup には次の特性があります。

- 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。メイン グループのテーブルから、グループをクリックして [関連] - [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。これらの 3 つのグループではすべて、直接的または間接的に LogicalSwitch-1 がメンバーとして含まれているためです。
- 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。NSX Manager 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。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。
 - NSGroup の有効なメンバーの数が 5,000 の 80% を超えると、「NSGroup xyz is about to exceed the maximum member limit.」ログ ファイルには「Total number in NSGroup is ...」と記録されます。数が 5,000 を超えると、警告メッセージ「NSGroup xyz has reached the maximum numbers limit.Total number in NSGroup = ...」が表示されます。
 - NSGroup 内の変換された VIF/IP/MAC の数が 5,000 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。
- サポートされる仮想マシンの最大数は 10,000 です。

- 最大 1 万までの NSGroup を作成できます。

NSGroup にメンバーとして追加できるオブジェクトの場合、任意のオブジェクトの画面に移動して [関連] - [NSGroups] の順に選択します。

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 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [グループ] - [追加] を選択します。
- 3 NSGroup の名前を入力します。
- 4 (オプション) 説明を入力します。
- 5 (オプション) [メンバーシップ基準] をクリックします。

各基準に、最大で 5 つのルールを論理 AND 演算子と組み合わせて指定することができます。利用可能なメンバー基準は以下に適用できます。

- [論理ポート] - タグとオプションのスコープを指定できます。
 - [論理スイッチ] - タグとオプションのスコープを指定できます。
 - [仮想マシン] - 名前、タグ、コンピュータの OS 名、または、一定の条件を満たすコンピュータ名（特定の文字列と等しい、特定の文字列で開始または終了する、特定の文字列と等しくないなど）を指定できます。
 - [トランスポート ノード] - Edge ノードまたはホスト ノードと等しいノード タイプを指定できます。
 - [IP セット] - タグとオプションのスコープを指定できます。
- 6 (オプション) [メンバー] をクリックしてメンバーを選択します。

使用可能なメンバー タイプは次のとおりです。

- [Active Directory グループ] - ADGroup を含む NSGroup は、分散ファイアウォール ルールの extended_source フィールドでのみ使用でき、グループ内の唯一のメンバーである必要があります。たとえば、ADGroup と IPSet の両方をメンバーに含む NSGroup は使用できません。
- [IP セット] - IPv4 アドレスと IPv6 アドレスの両方を含めることができます。
- [論理ポート] - IPv4 アドレスと IPv6 アドレスの両方を含めることができます。
- [論理スイッチ] - IPv4 アドレスと IPv6 アドレスの両方を含めることができます。
- [MAC セット]
- [NSGroup]
- [トランスポート ノード]
- [VIF]
- [仮想マシン]

7 [追加] をクリックします。

グループのテーブルに、このグループが追加されます。グループ名をクリックして概要を表示し、メンバーシップ基準、メンバー、アプリケーション、および関連グループを含むグループ情報を編集します。タグを追加および削除するには、[概要] タブの一番下までスクロールします。詳細については[オブジェクトへのタグの追加](#)を参照してください。[関連] > [NSGroups] の順に選択すると、選択した NSGroup をメンバーに含むすべての NSGroup が表示されます。

サービスとサービス グループの設定

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

NSService には、次のようなタイプがあります。

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

L4 ポート セットは、送信元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 ルールでブロックまたは許可するトラフィックのタイプを定義したりすることができます。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [サービス] - [追加] を選択します。
- 3 名前を入力します。
- 4 (オプション) 説明を入力します。

- 5 [プロトコルの指定] を選択して個々のサービスを設定するか、[既存サービスのグループ化] を選択して NSService のグループを設定します。
- 6 個々のサービスに対して、サービスのタイプとプロトコルを選択します。
使用可能なタイプは、[Ether]、[IP アドレス]、[IGMP]、[ICMP]、[ALG]、および [L4 ポート セット] です。
- 7 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。
- 8 [追加] 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 [ネットワークとセキュリティの詳細設定] - [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して、リストをフィルタします。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 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。
- 4 仮想マシンを選択します。
- 5 [タグの管理] をクリックします。
- 6 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。

NSX Manager から仮想マシンに割り当てることができるタグの最大数は 25 です。論理スイッチやポートなどの、他のすべての管理対象オブジェクトのタグの最大数は 30 です。

- 7 [保存] をクリックします。

DHCP を構成するには、[ネットワークとセキュリティの詳細設定] タブを使用します。

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 [NSX Manager の概要](#) 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。

- [DHCP](#)
- [メタデータ プロキシ](#)

DHCP

Dynamic Host Configuration Protocol (DHCP) を使用すると、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、DNS 構成などのネットワーク構成をクライアントが 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。

このリリースでは、DHCP サーバはゲスト VLAN のタグ付けをサポートしていません。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [サーバ プロファイル] - [追加] を選択します。
- 3 名前を入力します。オプションで説明を入力できます。
- 4 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。
- 5 (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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [サーバ] - [追加] を選択します。
- 3 名前を入力します。オプションで説明を入力できます。
- 4 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。
- 5 (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。
- 6 (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。
- 7 (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。
- 8 (オプション) 他のオプションを入力します。
- 9 [保存] をクリックします。
- 10 新しく作成した DHCP サーバを選択します。
- 11 IP アドレス プールのセクションを展開します。
- 12 [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。
- 13 静的バインドのセクションを展開します。
- 14 [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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] の順に選択します。
 - a 論理スイッチのチェックボックスをクリックします。
 - b [アクション] - [DHCP サーバを接続] の順にクリックします。
- 3 または、[ネットワークとセキュリティの詳細設定] - [DHCP] の順に選択します。
 - a [サーバ] タブをクリックします。
 - b DHCP サーバのチェックボックスをクリックします。
 - c [アクション] - [論理スイッチに接続] の順にクリックします。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [スイッチング] 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 サーバまたは DHCPv6 サーバを指定します。DHCP/DHCPv6 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [リレー プロファイル] - [追加] を選択します。
- 3 名前を入力します。オプションで説明を入力できます。
- 4 1 つ以上の外部 DHCP/DHCPv6 サーバ アドレスを入力します。

次のステップ

DHCP/DHCPv6 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 Data Center 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [リレー サービス] - [追加] を選択します。
- 3 名前を入力します。オプションで説明を入力できます。
- 4 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。[論理ルーター ポートへの DHCP リレー サービスの追加](#) を参照してください。

論理ルーター ポートへの DHCP リレー サービスの追加

論理ルーター ポートに DHCP リレー サービスを追加します。このポートに接続されている論理スイッチの仮想マシンは、リレー サービスで設定されている DHCP サーバと通信できます。

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。
- ルーター ポートの種類が [ダウンリンク] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 詳細情報と設定オプションを表示するには、該当する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 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。
- 6 [リレー 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。
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。

DHCP リースの削除

DHCP リースの削除が必要になることがあります。たとえば、DHCP クライアントで異なる IP アドレスを取得する場合や、クライアントが IP アドレスを解放せずにシャットダウンし、他のクライアントがそのアドレスを使用できるようにする場合に、この操作が必要になります。

DHCP リースを削除するには、次の API を使用します。

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```

リースの削除状況を確認するには、DELETE API の前後で次の API を呼び出します

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

DELETE API を呼び出した後、削除されたリースが GET API の出力に含まれていないことを確認します。

詳細については、『NSX-T Data Center API リファレンス』を参照してください。

メタデータ プロキシ

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。

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

NSX 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 Data Center 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>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [メタデータ プロキシ] - [追加] の順に選択します。
- 3 メタデータ プロキシ サーバの名前を入力します。
- 4 (オプション) 説明を入力します。
- 5 Nova サーバの URL とポートを入力します。
有効なポートの範囲は 3000 ～ 9000 です。
- 6 [シークレット キー] の値を入力します。
- 7 ドロップダウン リストから NSX Edge クラスタを選択します。
- 8 (オプション) NSX Edge クラスタのメンバーを選択します。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [メタデータ プロキシ] を選択します。
- 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] - [論理スイッチに接続] 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] > [スイッチ] 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] - [メタデータ プロキシを接続] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [DHCP] - [メタデータ プロキシ] を選択します。

- 3 メタデータ プロキシ サーバを選択します。
- 4 [アクション] - [論理スイッチから切断] 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] > [スイッチ] の順に選択し、スイッチを選択して、[アクション] - [メタデータ プロキシの切り離し] 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 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。

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 NSX Manager の概要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 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [IP アドレス管理] を選択します。
- 3 IP アドレス ブロックを追加するには、[追加] 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] タブで [編集] 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] タブで [管理] 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] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [IP アドレス管理] を選択します。
- 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] 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] 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] をクリックします。

高度なロード バランシング

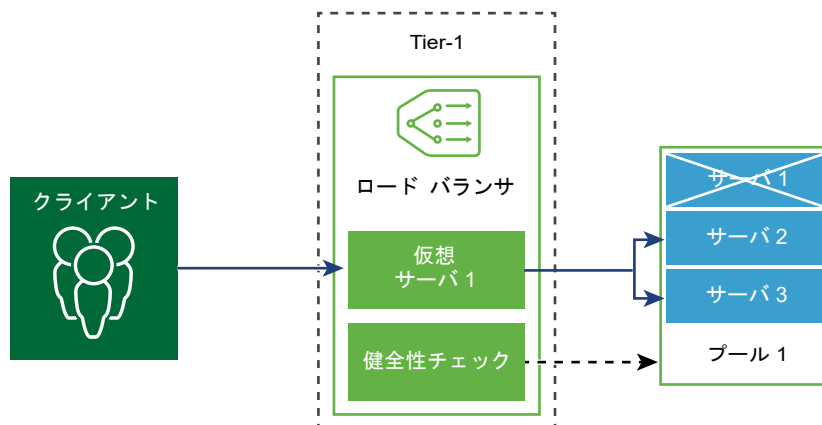
19

この情報では、[ネットワークとセキュリティの詳細設定] タブにある NSX-T Data Center ロード バランシングの構成について説明します。

NSX Advanced Load Balancer (Avi Networks) の詳細については、<https://www.vmware.com/products/nsx-advanced-load-balancer.html> を参照してください。

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 NSX Manager の概要を参照してください。

NSX-T Data Center 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。

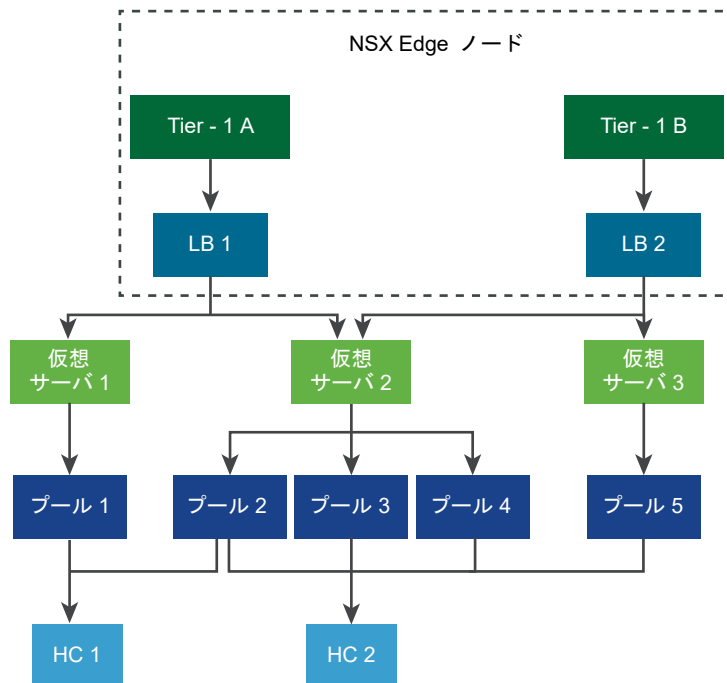
- キー ロード バランサの概念
- ロード バランサ コンポーネントの構成

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。

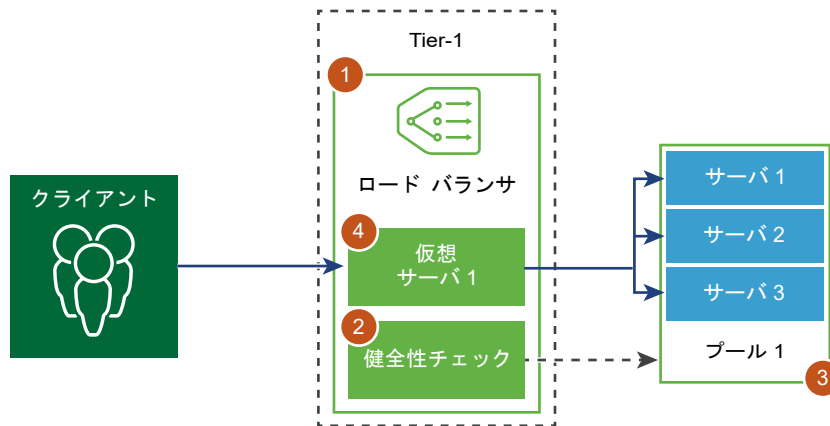
サーバの健全性を確認する健全性チェック モニターを追加すると、各サーバでアプリケーションが正しく実行されているかどうかを確認できます。



ロード バランサ 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。

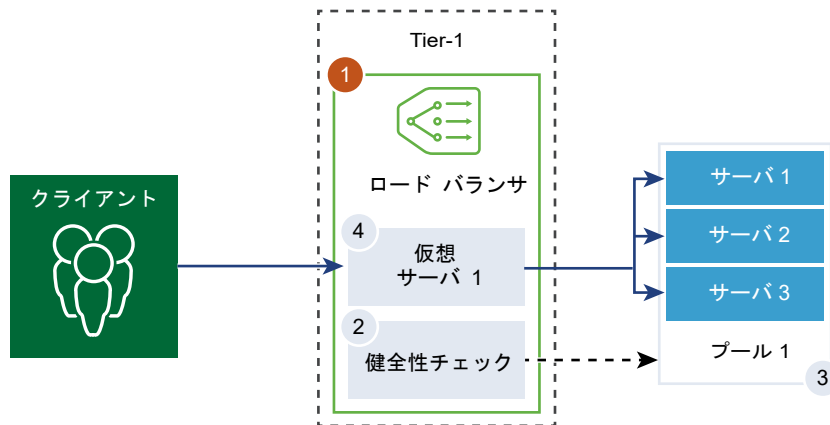


ロード バランサの作成

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [追加]の順に選択します。
- 3 ロード バランサの名前と説明を入力します。

- 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] - [仮想サーバに接続] 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] - [論理ルーターに接続] 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。
- 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

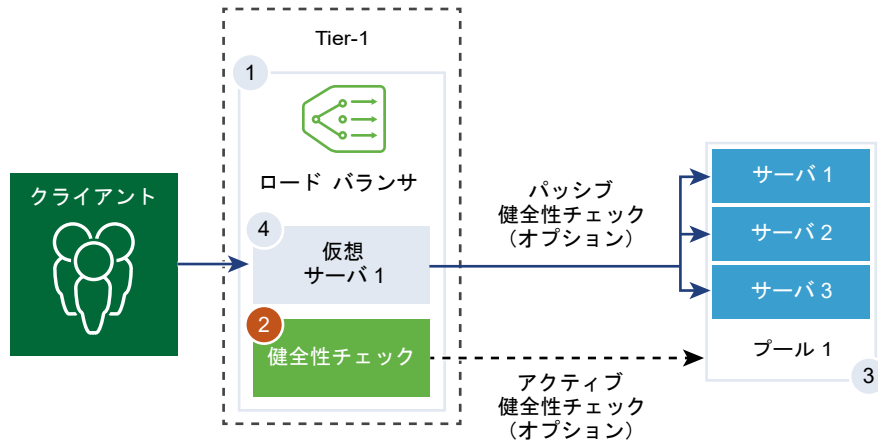
アクティブ健全性モニターは、サーバが使用可能かどうかをテストする際に使用します。アクティブ健全性モニターでは、基本的なサーバへの ping 送信や高度な HTTP の要求などのさまざまなタイプのテストを使用してアプリケーションの健全性を監視します。

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 ゲートウェイ（以前の 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。

Tier-1 ゲートウェイが Tier-0 ゲートウェイに接続している場合、ルーター リンク ポートが作成され、その IP アドレス（通常は 100.64.x.x の形式）がロード バランサ サービスの健全性チェックで使用されます。Tier-1 ゲートウェイがスタンドアローンの場合（中央のサービス ポートが1つだけ存在し、Tier-0 ゲートウェイに接続していない場合）、中央のサービス ポートの IP アドレスがロード バランサ サービスの健全性チェックに使用されます。スタンドアローンの Tier-1 ゲートウェイについては、[スタンドアローン Tier-1 論理ルーターの作成](#)を参照してください。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [モニター] - [アクティブ健全性モニター] - [追加] の順に選択します。
- 3 アクティブ健全性モニターの名前と説明を入力します。
- 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 で事前定義のプロトコル (`http-monitor`、`https-monitor`、`Icmp-monitor`、`Tcp-monitor`、`Udp-monitor`) を使用することもできます。

- 5 モニタリング 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
モニタリング間隔	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。
起動回数	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、モニタリング間隔が 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見なされます。

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 メニューからサーバの状態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 Body	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 応答本文の状態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。
TLS1.0 は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。

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。

c デフォルトの SSL 暗号を割り当てるか、カスタムの SSL 暗号を作成します。

d 健全性チェック プロトコルとして、以下に HTTP 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 メニューからサーバの状態の検出方法 (GET、OPTIONS、POST、HEAD または PUT) を選択します。
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 Body	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 応答本文の状態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。

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。

送信済みと予測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
UDP 送信データ	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。
UDP 予測データ	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、サーバが稼動状態と見なされます。

- 12 [終了] 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [モニター] - [パッシブ健全性モニター] - [追加] 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。

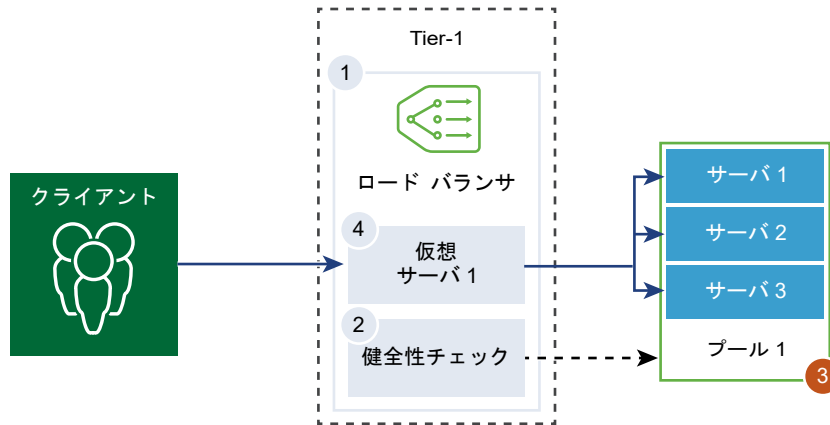
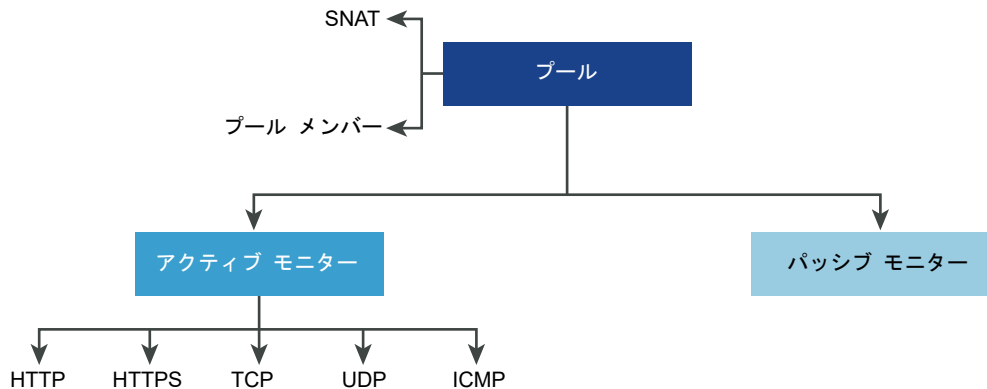


図 19-1. サーバ プール パラメータの設定



前提条件

- 動的プールのメンバーを使用する場合は、NS グループ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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [サーバ プール] - [追加] 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数の上限に達した

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。
WEIGHTED_LEAST_CONNECTION	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、重み値を使用して、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。 値が設定されず、スロー スタートが有効になっている場合、デフォルトで重み値は 1 となります。
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 最適化では、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 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。

バックアップ メンバーとしてプール メンバーを指定すると、アクティブ/スタンバイ状態を提供する健全性モニターを活用できます。アクティブ メンバーが健全性チェックに失敗すると、バックアップ メンバーでトラフィックのフェイルオーバーが発生します。

オプション	説明
静的	[追加] 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 NS グループを選択します。 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。

サーバ プールに対するアクティブまたはパッシブ健全性モニターの設定はオプションです。アクティブ健全性モニターを選択したときに、Tier-1 ゲートウェイが Tier-0 ゲートウェイに接続すると、ルーター リンク ポートが作成されます。ロード バランサ サービスの健全性チェックには、ルーター リンク ポートの IP アドレス（通常は 100.64.x.x 形式）が使用されます。Tier-1 ゲートウェイがスタンドアローンの場合（中央のサービス ポートが 1 つだけ存在し、Tier-0 ゲートウェイに接続していない場合）、中央のサービス ポートの IP アドレスがロード バランサ サービスの健全性チェックに使用されます。スタンドアローンの Tier-1 ゲートウェイについては、[スタンドアローン Tier-1 論理ルーターの作成](#)を参照してください。

IP アドレスでロード バランサ サービスの健全性チェックを実行できるように、ファイアウォール ルールを追加します。

11 [終了] 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 ルールなど、設定可能なコンポーネントがあります。

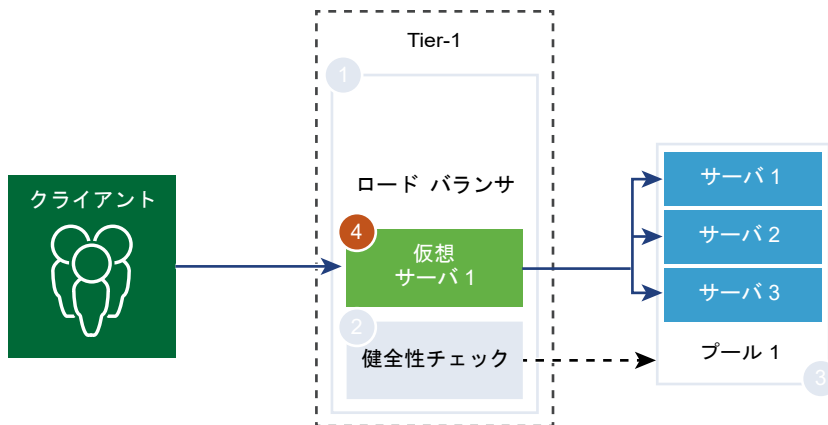
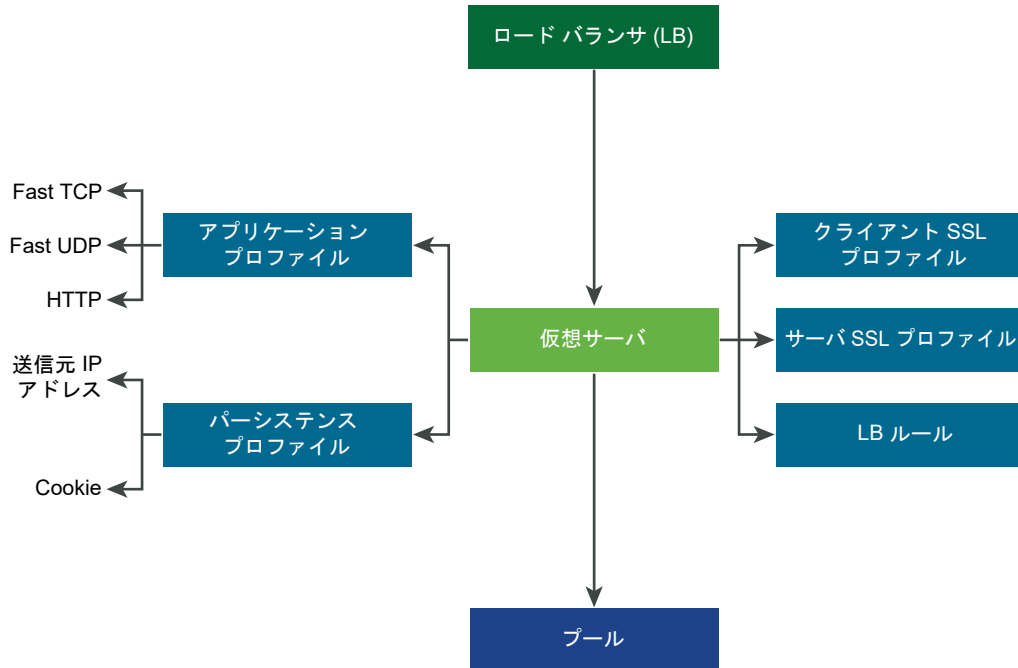


図 19-2. 仮想サーバ コンポーネント



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 19-3. 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

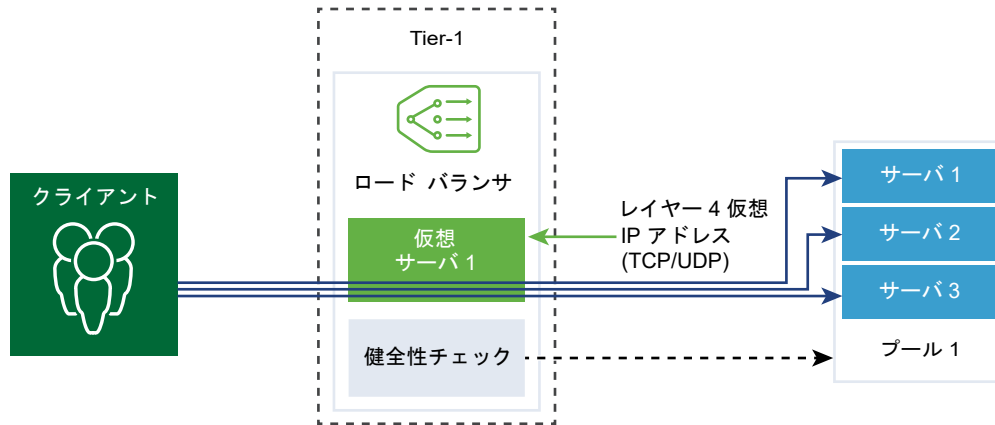
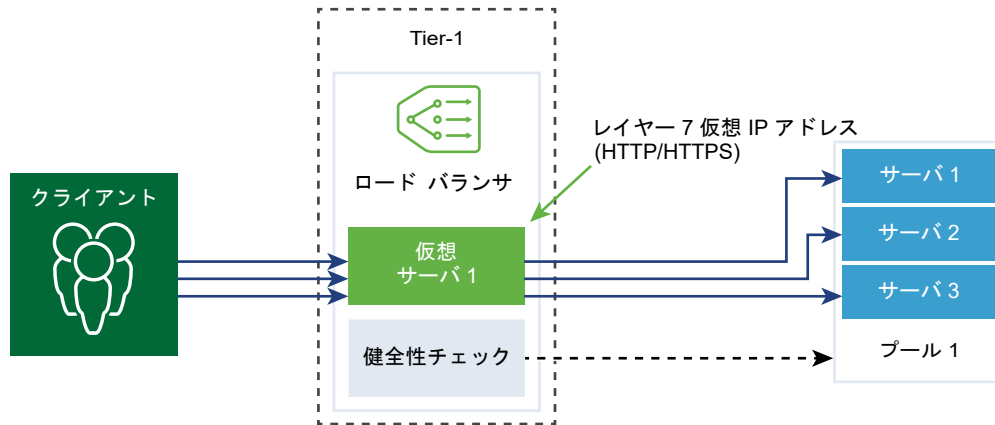


図 19-4. レイヤー 7 の HTTPS アプリケーション プロファイル



手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [プロファイル] - [アプリケーション プロファイル] 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"> ■ [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。 ■ [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。 <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"> ■ [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。 <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"> ■ [挿入] - 受信した要求に 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。受信された要求に XFF HTTP ヘッダーが存在する場合は、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 ヘッダーを追加します。 ■ [置き換え] - 受信した要求に 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ます。 <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	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。

オプション	説明
	<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> <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せん。</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。

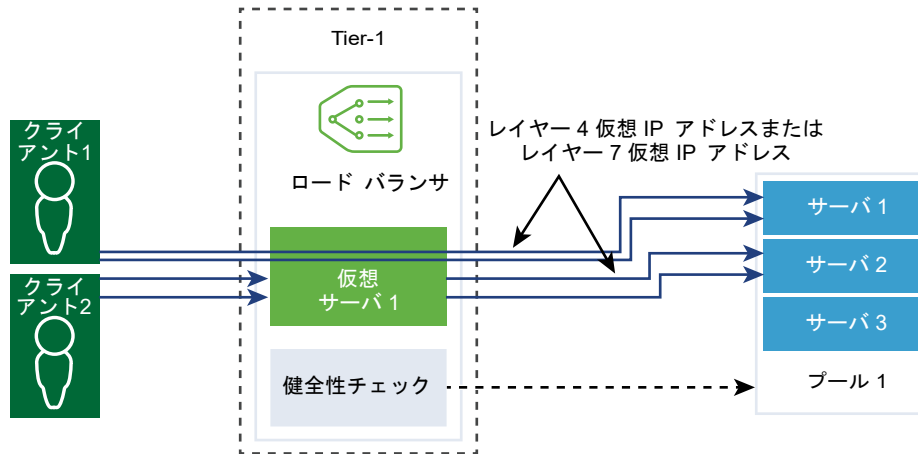
パーシステンス プロファイルの設定

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 のパーシステンス 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 のパーシステンス 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 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 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。Cookie 名に空白は使用[できません]。



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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [プロファイル] - [パースステンス プロファイル] の順に選択します。
- 3 送信元 IP のパースステンス 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] - [送信元 IP のパースステンス] の順に選択します。
 - b 送信元 IP のパースステンス 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
パーシステンスの共有	<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 のパーシステンス 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"> ■ 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。 ■ 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。 <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 の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] - [Cookie パーシステンス] 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 [パーシステンスの共有] 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] 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	<p>ドロップダウン メニューからモードを選択します。</p> <ul style="list-style-type: none"> ■ [挿入] - セッションを識別する一意の Cookie を追加します。 ■ [プリフィックス] - 既存の HTTP Cookie 情報に新しい情報を追加します。 ■ [書き換え] - 既存の HTTP Cookie 情報を書き換えます。
Cookie 名	Cookie 名を入力します。Cookie 名に空白は使用[できません]。
Cookie ドメイン	<p>ドメイン名を入力します。</p> <p>HTTP Cookie ドメインは、挿入モードの場合にのみ設定できます。</p>
Cookie のパス	<p>Cookie の URL パスを入力します。</p> <p>HTTP Cookie のパスは、挿入モードの場合にのみ設定できます。</p>
Cookie の暗号化	<p>Cookie サーバの IP アドレスとポート情報を暗号化します。</p> <p>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。</p>
Cookie のフォールバック	<p>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。</p> <p>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。</p>

- 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	<p>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。</p> <p>[セッション Cookie] は保存されません。ブラウザを閉じると失われます。</p> <p>[パーシステンス Cookie] はブラウザによって保存されます。ブラウザを閉じても失われません。</p>
最大アイドル時間	Cookie が期限切れにな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] のみ。Cookie の有効期間を秒単位で入力します。

- g [終了] 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 Data Center Limited Export Release 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 19-5. SSL オフロード

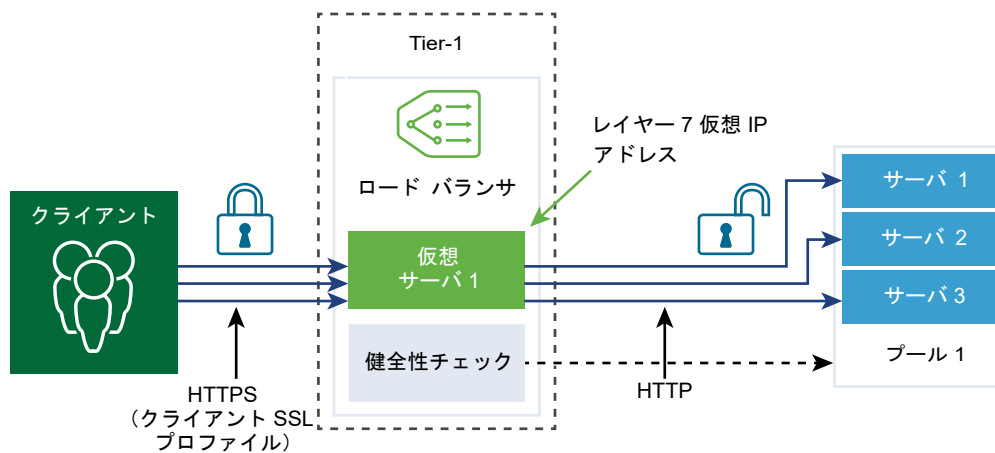
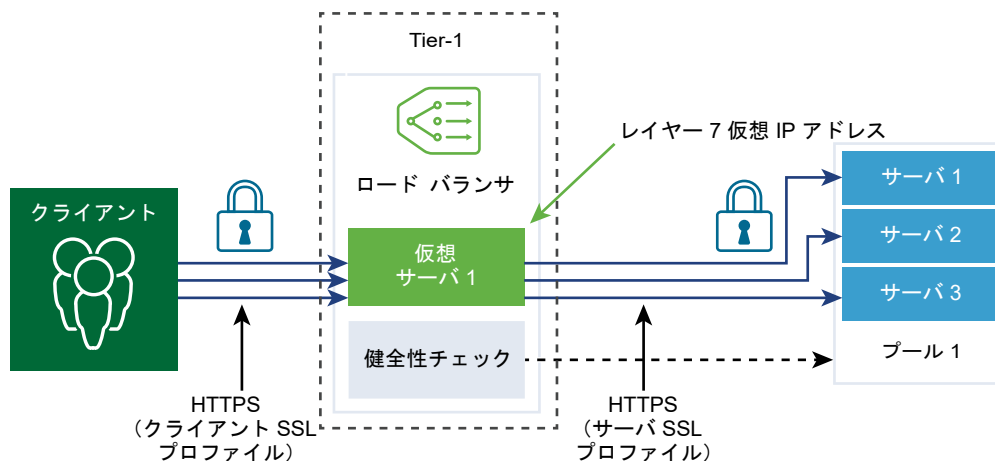


図 19-6. エンド ツー エンドの SSL



手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。

- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [プロファイル] - [SSL プロファイル] 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] - [クライアント側 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 暗号を割り当てます。
カスタムの SSL 暗号を作成することもできます。
- 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] 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。

- a ドロップダウン メニューから [追加] - [サーバ側 SSL] の順に選択します。
- b サーバ SSL プロファイルの名前と説明を入力します。
- c サーバ SSL プロファイルに含める SSL 暗号を選択します。
カスタムの SSL 暗号を作成することもできます。
- 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] タブをクリックします。

- f 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。

- 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 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。

仮想サーバの状態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

- 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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [仮想サーバ] - [追加] 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 [アクセス ログ] ボタンを切り替え、レイヤー 4 仮想サーバのログを有効にします。

6 [次へ] をクリックします。

7 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。

8 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。
最大新規接続レート	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。

9 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。

10 ドロップダウン メニューから既存のソーリー サーバ プールを選択します。

ソーリー サーバ プールは、ロード バランサがデフォルト プールからの要求を処理するバックエンド サーバを選択できない場合に要求を処理します。

11 [次へ] をクリックします。

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。

仮想サーバでパーシステンス 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。

13 [終了] 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。

仮想サーバの状態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。
- 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。
- [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。
- [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。

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 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ロード バランサ] - [仮想サーバ] - [追加] 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] 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] 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。

ロード バランサのルールは、一致のタイプとして正規表現をサポートします。高度な使用方法ではいくつかの制限がありますが、PCRE スタイルの正規表現パターンがサポートされています。一致条件に正規表現を使用する場合、名前付きキャプチャ グループがサポートされます。

正規表現には以下の制限事項があります。

- 文字を和集合および共通部分で表現することはサポートされません。たとえば、`[a-z[0-9]]` および `[a-z&&[aeiou]]` と表現せず、それぞれ `[a-z0-9]` および `[aeiou]` と表現します。
- 後方参照は 9 までサポートされ、`\1` ~ `\9` を使用して参照できます。
- 8 進数に一致させるには、`\ddd` 形式ではなく `\Odd` 形式を使用します。
- 最上位のレベルでは組み込みフラグはサポートされません。グループ内でのみサポートされます。たとえば、「`Case (?i:s)ensitive`」は使用せずに、「`Case ((?i:s)ensitive)`」を使用します。
- 前処理演算子 `\l`、`\u`、`\L`、`\U` はサポートされません。ここで、`\l` は次の文字を小文字にする演算子、`\u` は次の文字を大文字にする演算子、`\L` は `\E` までの文字を小文字にする演算子、`\U` は `\E` までの文字を大文字にする演算子です。
- `(?(condition)X)`、`(? {code})`、`(??{Code})` および `(?#comment)` はサポートされません。
- 事前定義済みの Unicode 文字クラス `\X` はサポートされません。
- Unicode 文字の名前付き構文を使用した参照はサポートされません。たとえば、`\N{name}` は使用せずに `\u2018` を使用します。

一致条件に正規表現を使用する場合、名前付きキャプチャ グループがサポートされます。たとえば、正規表現による一致パターン「`/news/(?<year>\d+)-(?(month>\d+)-(?(day>\d+)/?(article>.*))`」は、「`/news/2018-06-15/news1234.html`」のような URI との一致に使用されます。

ここで変数を以下のように設定します：`$year = "2018" $month = "06" $day = "15" $article = "news1234.html"`。設定後の変数は、ロード バランサ ルールのアクションで使用できます。たとえば、URI は一致する変数を使用して「`/news.py?year=$year&month=$month&day=$day&article=$article`」のように書き換えることができます。したがって URI は「`/news.py?year=2018&month=06&day=15&article=news1234.html`」と書き換えられます。

書き換えアクションにより、名前付きキャプチャ グループと組み込みの変数を組み合わせて使用できます。たとえば、URI は「/news.py?

year=\$year&month=\$month&day=\$day&article=\$article&user_ip=\$_remote_addr」と記述できます。したがって例の URI は「/news.py?

year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1」と書き換えられます。

注： 名前付きキャプチャ グループの名前は、「_」文字で開始できません。

名前付きキャプチャ グループのほか、書き換えアクションでは次の組み込みの変数も使用できます。組み込みの変数の名前はすべて「_」で始まります。

- \$_args : 要求からの引数
- \$_arg_<name> : 要求行の <name> 引数
- \$_cookie_<name> : <name> Cookie の値
- \$_upstream_cookie_<name> : アップストリーム サーバによって送信された Cookie。Set-Cookie 応答ヘッダー フィールドに名前が指定されます。
- \$_upstream_http_<name> : 任意の応答ヘッダー フィールドで、<name> は小文字に変換され、ダッシュをアンダースコアで置き換えたフィールド名
- \$_host : 優先順位で、要求行からのホスト名、「Host」要求のヘッダーフィールドからのホスト名、または要求に一致するサーバ名
- \$_http_<name> : 任意の要求のヘッダー フィールドで、<name> は小文字に変換され、ダッシュをアンダースコアで置き換えたフィールド名
- \$_https : 接続が SSL モードで機能している場合は "on"、それ以外の場合は ""
- \$_is_args : 要求行に引数がある場合は "?" それ以外の場合は ""
- \$_query_string : \$_args と同じ
- \$_remote_addr : クライアント アドレス
- \$_remote_port : クライアント ポート
- \$_request_uri : 元の完全な要求 URI (引数を含む)
- \$_scheme : 要求のスキーム、"http" または "https"
- \$_server_addr : 要求を承認したサーバのアドレス
- \$_server_name : 要求を承認したサーバの名前
- \$_server_port : 要求を承認したサーバのポート
- \$_server_protocol : 申請プロトコル、通常、"HTTP/1.0" または "HTTP/1.1"
- \$_ssl_client_cert : 確立された SSL 接続に対し、クライアント証明書を最初の行以外の各行で先頭にタブ文字を追加した PEM 形式で返します
- \$_ssl_server_name : SNI で要求されたサーバ名を返します
- \$_uri : 要求内の URI パス

- `$_ssl_ciphers` : クライアントの SSL 暗号を返します
- `$_ssl_client_i_dn` : RFC 2253 に従って確立された SSL 接続のクライアント証明書の issuer DN 文字列を返します
- `$_ssl_client_s_dn` : RFC 2253 に従って確立された SSL 接続のクライアント証明書の subject DN 文字列を返します
- `$_ssl_protocol` : 確立された SSL 接続のプロトコルを返します
- `$_ssl_session_reused` : SSL セッションが再利用された場合は「r」、それ以外の場合は「.」を返します

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 [仮想サーバの識別子] ページに移動します。
- 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。
最大新規接続レート	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] 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 ルールを構成します。

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
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] をクリックして、HTTP 要求の転送にロード バランサ ルールを構成します。

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

サポートされている一致条件	説明
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
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、状態を 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 状態コード 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。状態コードは、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 状態コード 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] をクリックして、HTTP 応答の書き換えにロード バランサ ルールを構成します。

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 （オプション） [次へ] をクリックして、ロード バランシング プロファイルを構成します。

10 [終了] 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。

注： SSL プロファイルは NSX-T Data Center Limited Export Release ではサポートされていません。

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 アドレスのパーシステンス プロファイルまたは Cookie 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] 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] 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、同じ IP アドレスを持つ複数のホストにサーバが対応しない場合、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、信頼する 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] をクリックします。

高度なファイアウォール

20

注： ポリシー インターフェイスで作成されたオブジェクトを [ネットワークとセキュリティの詳細設定] ユーザー インターフェイスで変更すると、一部の設定を行うことができない場合があります。このような読み取り専用の設定の場合、その横にこのアイコン  が表示されます。詳細については、1 章 [NSX Manager の概要](#) 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。

- 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
- 論理スイッチのブリッジ ポートへのファイアウォールの構成
- 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
- ファイアウォール ルールについて

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。

Edge ファイアウォールはアップリンク ルーター ポートに実装されます。つまり、トラフィックが Edge のアップリンク ルーター ポートに到達した場合にのみ、ファイアウォール ルールが適用されます。特定の宛先 IP にファイアウォール ルールを適用するには、/32 ネットワークを使用してグループを設定する必要があります。/32 以外のサブネットを指定すると、ファイアウォール ルールがサブネット全体に適用されます。

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター] の順に選択します。
- 3 まだ選択していない場合は、[ルーター] 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] - [Edge ファイアウォール] 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] をクリックして、[ルールを上に加] または [ルールを下に加] 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 [ルールを上に加] または [ルールを下に加] 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 [削除] 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] 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。

論理スイッチのブリッジ ポートへのファイアウォールの構成

レイヤー 2 ブリッジでバックアップされた論理スイッチのブリッジ ポートにファイアウォール セクションとファイアウォール ルールを構成することができます。ブリッジは、NSX Edge ノードを使用して作成する必要があります。

前提条件

スイッチがブリッジ プロファイルに接続されていることを確認します。[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](#) 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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [ブリッジ ファイアウォール] を選択します。
- 3 論理スイッチを選択します。

スイッチはブリッジ プロファイルに接続する必要があります。

- 4 レイヤー 2 またはレイヤー 3 ファイアウォールを構成するには、前のセクションの同じ手順を実行します。

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

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構成済みのアクションが適用され、ルールの構成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。

注： 論理スイッチには N-VDS モードと呼ばれるプロパティがあります。このプロパティは、スイッチが属するトランスポート ゾーンからのものです。N-VDS モードが ENS（Enhanced Datapath と呼ばれる）の場合、Source、Destination、または Applied To フィールドでスイッチまたはそのポートに対してファイアウォール ルールまたはセクションを作成することはできません。

分散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、ファイアウォール ルールはデータ プレーン レベルで適用されません。有効に戻すと、ルールは再適用されます。

手順

- 1 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] に移動します。
- 2 [設定] タブをクリックします。
- 3 分散ファイアウォールの [編集] 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状態を緑色（有効）または灰色（無効）に切り替えます。
- 5 [保存] をクリックします。

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構成をテナントに適用するために使用されます。

手順

- 1 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 レイヤー 3 (L3) ルールの場合には [全般] タブを、レイヤー 2 (L2) ルールの場合には、[イーサネット] 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 バーのセクションのアイコンをクリックし、[セクションを上追加] または [セクションを下追加] 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、複数のルールがある場合にこの優先順位によって、パケット処理の決定に影響します。

- 5 セクション名を入力します。
- 6 ファイアウォールをステートレスにするには、[ステートレス ファイアウォールを有効にする] を選択します。このオプションは L3 の場合にのみ適用できます。

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。TCP と UDP のフローでファイアウォールの結果が ALLOW の場合、最初のパケットの後、いずれかの方向でトラフィック タプルにキャッシュが作成され、維持されます。つまり、トラフィックをファイアウォール ルールで確認する必要がなくなるため、遅延が短くなります。通常、ステートレス ファイアウォールはより高速で、トラフィックの負荷が高くなっても適切に動作します。

ステートフル ファイアウォールはトラフィックの状況をエンドツーエンドで監視できます。状態とシーケンス番号を検証するため、すべてのパケットでファイアウォールが参照されます。ステートフル ファイアウォールは、承認されていない偽装された通信の特定に適しています。

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] は、そのセクションのルールのすべての [適用先] 設定を上書きします。

- 8 [OK] をクリックします。

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 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。

- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] 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、[セクションの削除] を選択します。

または、セクションを選択し、メニュー バーの削除アイコンをクリックします。

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 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] 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] または [すべてのルールを無効にする] を選択します。
- 4 [発行] 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 ESXi および KVM ホストの /var/log/dfwptlogs.log ファイルに保存されます。

手順

- 1 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] 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、[ログを有効にする] または [ログを無効にする] を選択します。
- 4 [発行] をクリックします。

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 NS グループ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 Data Center 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。

注： NSX-T Data Center は、NSX Manager と NSX Edge ノードの仮想マシンを自動的にファイアウォール除外リストに追加します。

手順

- 1 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] - [除外リスト] - [追加] を選択します。

2 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]、[論理スイッチ]、[NS グループ] です。

3 [OK] をクリックします。

4 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] 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 Data Center は、ファイアウォール ルールを使用してネットワークの送信受信トラフィックの処理方法指定します。

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。ファイアウォールを適用しない論理スイッチ、論理ポート、またはグループを含む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。

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、詳細な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 Strict をセクションごとに有効にして、中間セッションのピックアップをオフにし、3 ウェイ ハンドシェイクの要件を適用できます。特定の分散ファイアウォール セクションで TCP Strict モードを有効にし、デフォルトの ANY-ANY Block ルールを使用すると、3 ウェイ ハンドシェイクの接続要件を満たしていないパケットと、このセクションの TCP ベースのルールに一致するパケットがドロップされます。Strict はステートフル TCP ルールにのみ適用され、分散ファイアウォール セクション レベルで有効になります。TCP Strict は、TCP サービスが指定されていないデフォルトの ANY-ANY Allow と一致するパケットには適用されません。

表 20-1. ファイアウォール ルールのプロパティ

プロパティ	説明
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 20-1. ファイアウォール ルールのプロパティ（続き）

プロパティ	説明
送信元	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、送信元はすべてに一致します。送信元または宛先の範囲には IPv4 と IPv6 の両方がサポートされます。
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 IPv4 と IPv6 の両方がサポートされます。
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、サービスはすべてに一致します。
適用先	このルールを適用する範囲を定義します。定義しない場合、範囲はすべての論理ポートになります。セクションに [適用先] を追加した場合、ルールが上書きされます。
ログに記録	ログへの記録を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/ dfwpktlogs.log ファイルに保存されます。
アクション	ルールによって適用されるアクションには、 許可 、 ドロップ 、または 却下 があります。デフォルトは 許可 です。
IP プロトコル	オプションは、 IPv4 、 IPv6 、および IPv4_IPv6 です。デフォルトは IPv4_IPv6 です。このプロパティにアクセスするには、[詳細設定] アイコンをクリックします。
方向	オプションは、 受信 、 送信 、および 受信/送信 です。デフォルトは 受信/送信 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。 受信 はオブジェクトへのトラフィックのみ、 送信 はオブジェクトからのトラフィックのみ、 受信/送信 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。このプロパティにアクセスするには、[詳細設定] アイコンをクリックします。
ルール タグ	ルールに追加されているタグです。このプロパティにアクセスするには、[詳細設定] アイコンをクリックします。
フロー統計	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。このプロパティにアクセスするには、グラフのアイコンをクリックします。

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割り当ての信頼性は保証されません。SpoofGuard が有効な場合、検出された割り当てがすべて検証され、承認された割り当て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 アドレスを論理スイッチに手動で関連付けます。

手順

- 1 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] 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 ルールの最初の列のメニュー アイコンをクリックし、[ルールを上追加] または [ルールを下追加] 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、複数ルールがある場合の優先順位が、パケットの処理を決定に重要になります。

- 5 [名前] 列で、ルール名を入力します。
- 6 [送信元] 列で、編集アイコンをクリックし、ルールのソースを選択します。定義しない場合、送信元はすべてに一致します。

オプション	説明
IP 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 と IPv6 形式の両方がサポートされています。
コンテンツオブジェクト	使用可能なオブジェクトは、IP セット、論理ポート、論理スイッチ、および NS グループです。オブジェクトを選択し、[OK] をクリックします。

- 7 [宛先] 列で編集アイコンをクリックし、宛先を選択します。定義しない場合は、すべての宛先と一致します。

オプション	説明
IP 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 と IPv6 形式の両方がサポートされています。
コンテンツオブジェクト	使用可能なオブジェクトは、IP セット、論理ポート、論理スイッチ、および NS グループです。オブジェクトを選択し、[OK] をクリックします。

- 8 [サービス] 列で編集アイコンをクリックし、サービスを選択します。サービスを定義しない場合は、そのすべてと一致します。
- 9 事前定義済みサービスを選択するには、利用可能なサービスから 1 つ選択します。

- 10 新しいサービスを定義するには、[Raw ポート/プロトコル] タブをクリックし、[追加] をクリックします。

オプション	説明
サービスのタイプ	<ul style="list-style-type: none"> ■ ALG ■ ICMP ■ IGMP ■ IP アドレス ■ L4 ポート セット
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。

- 11 [適用先] 列で編集アイコンをクリックし、オブジェクトを選択します。

- 12 [ログ] 列で、ログの記録オプションを設定します。

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

- 13 [アクション] 列で、アクションを選択します。

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。

- 14 [詳細設定] アイコンをクリックして、IP プロトコル、方向、ルール タグ、コメントを指定します。

- 15 [発行] をクリックします。

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 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。

- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] タブをクリックします。
- 3 ルールの最初の列のメニュー アイコンをクリックして、[ルールの削除] を選択します。
- 4 [発行] をクリックします。

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] タブに表示され、デフォルトのレイヤー 2 ルールは [イーサネット] タブに表示されます。

デフォルトのファイアウォール 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] 要素を [許可] から [ドロップ] または [却下] (推奨されません) に変更し、そのルールのトラフィックをログ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] を [ドロップ] または [却下] 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 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] タブをクリックします。
- 3 [名前] 列で、新しい名前を入力します。
- 4 [アクション] 列で、いずれか 1 つ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] を使用するメトリックの 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] を選択することは推奨されません。

- 5 [ログ] で、ログを有効または無効にします。

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。

- 6 [発行] 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、複数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 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] タブをクリックします。
- 3 ルールを選択し、メニュー バーの [上へ移動] または [下へ移動] アイコンをクリックします。
- 4 [発行] 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 [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] を選択します。
- 2 L3 ルールの場合には [全般] タブを、L2 ルールの場合には、[イーサネット] 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、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

- 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。

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 Data Center 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 Data Center 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。

- モニタリング ダッシュボードの表示
- カテゴリごとのオブジェクトの使用量と容量の表示
- 設定変更の認識された状態の確認
- オブジェクトの検索
- オブジェクト属性によるフィルタリング
- コンピュート マネージャの追加
- Active Directory の追加
- LDAP サーバの追加
- Active Directory の同期
- 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 Manager のバックアップとリストア
- vCenter Server からの NSX-T Data Center の拡張機能の削除
- NSX Manager クラスタの管理
- NSX Edge クラスタでの NSX Edge トランSPORT ノードの置き換え
- vCenter Server が失われ、リカバリできない場合の NSX-T のリカバリ
- NSX-T Data Center の複数サイトの展開
- アプライアンスの設定
- ライセンス キーの追加とライセンス使用レポートの生成
- 証明書の設定
- コンプライアンス ベースの設定

- サポート バンドルの収集
- ログ メッセージとエラー コード
- カスタマー エクスペリエンス向上プログラム
- オブジェクトへのタグの追加
- リモート サーバの SSH フィンガープリントの検索
- 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
- 外部ロード バランサの構成

モニタリング ダッシュボードの表示

NSX Manager インターフェイスには、システムの状態、ネットワークとセキュリティ、コンプライアンス レポートに関する詳細を表示する多くのモニタリング ダッシュボードが用意されています。これらの情報は、NSX Manager インターフェイスのどこからでも表示またはアクセスできますが、[ホーム] - [モニタリング ダッシュボード] ページでアクセスできます。

モニタリング ダッシュボードには、NSX Manager インターフェイスのホーム ページからアクセスできます。ダッシュボードから、ダッシュボードのデータを表示したいソース ページをクリックして、アクセスします。

手順

- 1 管理者として NSX Manager インターフェイスにログインします。
- 2 ホームページをまだ表示していない場合は、[ホーム] をクリックします。
- 3 [モニタリング ダッシュボード] をクリックし、ドロップダウン メニューからダッシュボードのカテゴリを選択します。

選択したカテゴリのダッシュボードがページに表示されます。ダッシュボードのグラフィックは色分けされています。ダッシュボードのすぐ上にカラー コード キーが表示されます。

- 4 より詳細なレベルの情報にアクセスするには、ダッシュボードのタイトルをクリックするか、ダッシュボードのいずれかの要素（有効になっている場合）をクリックします。

次の表に、デフォルトのダッシュボードとそのソースを示します。

表 21-1. システム ダッシュボード

ダッシュボード	送信元	説明
システム	[システム] - [アプライアンス] - [概要]	NSX Manager クラスタの状態とリソース（CPU、メモリ、ディスク）の消費量が表示されます。
ファブリック	[システム] - [ファブリック] - [ノード] [システム] - [ファブリック] - [トランスポート ゾーン] [システム] - [ファブリック] - [コンピュート マネージャ]	ホストと Edge トランスポート ノード、トランスポート ゾーン、コンピュート マネージャなどの NSX-T ファブリックの状態が表示されます。

表 21-1. システム ダッシュボード（続き）

ダッシュボード	送信元	説明
バックアップ	[システム] - [バックアップとリストア]	設定されている場合、NSX-T バックアップの状態が表示されます。リモートの SFTP サイトにバックアップを保存するスケジュールの設定を強くおすすめします。
エンドポイントの保護	[システム] - [サービス展開]	エンドポイント保護の展開状態が表示されます。

表 21-2. ネットワークとセキュリティのダッシュボード

ダッシュボード	送信元	説明
セキュリティ	[インベントリ] - [グループ] [セキュリティ] - [分散ファイアウォール]	グループとセキュリティ ポリシーの状態が表示されます。グループは、ワークロード、セグメント、セグメント ポート、IP アドレスの集合です。ここには、East-West ファイアウォール ルールなどのセキュリティ ポリシーが適用されます。
ゲートウェイ	[ネットワーク] - [Tier-0 ゲートウェイ] [ネットワーク] - [Tier-1 ゲートウェイ]	Tier-0 および Tier-1 ゲートウェイの状態が表示されます。
セグメント	[ネットワーク] - [セグメント]	ネットワーク セグメントの状態を表示します。
ロード バランサ	[ネットワーク] - [ロード バランシング]	ロード バランサ仮想マシンの状態が表示されます。
VPN	[ネットワーク] - [VPN]	仮想プライベート ネットワークの状態が表示されます。

表 21-3. ネットワークとセキュリティの詳細設定のダッシュボード

ダッシュボード	送信元	説明
ロード バランサ	[ネットワークとセキュリティの詳細設定] - [ロード バランサ]	ロード バランサ サービス、ロード バランサ仮想サーバ、ロード バランサ サーバ プールの状態が表示されます。ロード バランサは、1つ以上の仮想サーバをホストできます。仮想サーバは、アプリケーションをホストするメンバーを含むサーバ プールに割り当てられます。
ファイアウォール	[ネットワークとセキュリティの詳細設定] - [セキュリティ] - [分散ファイアウォール] [ネットワークとセキュリティの詳細設定] - [セキュリティ] - [ブリッジファイアウォール] [ネットワークとセキュリティの詳細設定] - [ネットワーク] - [ルーター]	ファイアウォールが有効になっているかどうかが表示されます。また、ポリシー数、ルール数、除外リストのメンバー数が表示されます。 注： このダッシュボードに表示される詳細情報は、引用されたソース ページの特定のサブタブから取得されます。
VPN	該当なし。	仮想プライベート ネットワークの状態と、開いている IPsec と L2 VPN セッションの数が表示されます。
スイッチング	[ネットワークとセキュリティの詳細設定] - [スイッチング]	仮想マシンとコンテナ ポートの両方を含む論理スイッチと論理ポートの状態が表示されます。

表 21-4. コンプライアンス レポートのダッシュボード

列	説明
非遵守を表すコード	非遵守を表す特定のコードが表示されます。
説明	非遵守状態の原因。
リソース名	非準拠状態の NSX-T リソース（ノード、スイッチ、プロファイル）。
リソース タイプ	問題の原因となっているリソースの種類。
影響を受けるリソース	影響を受けるリソースの数。数値をクリックすると、リストが表示されます。

コンプライアンス レポートのコードの詳細については、[コンプライアンスの状態レポートのコード](#)を参照してください。

カテゴリごとのオブジェクトの使用量と容量の表示

NSX-T Data Center 環境内のさまざまなカテゴリのオブジェクトの使用量と容量を表示できます。使用量が特定のしきい値に達したときに簡単に確認できるように、アラートを設定することもできます。

さまざまなカテゴリのオブジェクトの使用量と容量を表示するには、次のいずれかのタブをクリックします。

- [ネットワーク] - [ネットワークの概要] - [キャパシティ]
- [セキュリティ] - [セキュリティの概要] - [キャパシティ]
- [インベントリ] - [インベントリの概要] - [キャパシティ]
- [システム] - [システム概要] - [キャパシティ]

[プランとトラブルシューティング] - [統合されたキャパシティ] の順に移動すると、1つの画面ですべてのオブジェクト カテゴリを確認できます。

それぞれの容量画面では、オブジェクトのカテゴリごとに次の情報が表示されます。

- 最大容量 - この値は、大規模なアプライアンスの容量に基づきます。
- 現在のインベントリ (認識済み) - 正常に作成または設定されたオブジェクトの数。この数は、[ネットワークとセキュリティの詳細設定] タブに表示される NSX Manager オブジェクトの数を反映しています。これらのオブジェクトには、[ネットワーク]、[セキュリティ]、[インベントリ] または [システム] タブで作成したオブジェクトが含まれる場合があります。使用率を示す色付きのバーが表示されます。使用量が警告アラート レベルよりも低い場合、緑色で表示されます。使用量が警告アラート レベルを超え、重大アラート レベルを下回っている場合、オレンジ色で表示されます。使用量が重大アラート レベル以上の場合、赤色で表示されます。
- 警告アラート - この使用量に達すると、上記のバーがオレンジ色で表示されます。この値は変更できます。
- 重大アラート - この使用量に達すると、上記のバーが赤色で表示されます。この値は変更できます。

警告アラートまたは重大アラートの値を変更するときに、[元に戻す] をクリックすると、最後に保存した値に戻すことができます。[値のリセット] をクリックすると、すべてのオブジェクト カテゴリのデフォルト値をリストアできます。

ネットワークの容量画面には、次のオブジェクト カテゴリが表示されます。

- Tier-0 論理ルーター
- Tier-1 論理ルーター
- プリフィックス リスト
- システム全体の NAT ルール
- DHCP サーバ インスタンス
- システム全体の DHCP 範囲/プール
- NAT が有効になっている Tier-1 論理ルーター
- 論理スイッチ
- システム全体の論理スイッチ ポート

セキュリティの容量画面には、次のオブジェクト カテゴリが表示されます。

- システム全体でエンドポイント保護が有効になっているホスト
- システム全体でエンドポイント保護が有効になっている仮想マシン
- Active Directory グループ
- Active Directory ドメイン
- 分散ファイアウォール ルール
- システム全体のファイアウォール ルール
- システム全体のファイアウォール セクション
- 分散ファイアウォール セクション

インベントリの容量画面には、次のオブジェクト カテゴリが表示されます。

- ネットワーク グループとセキュリティ グループ
- IP セット
- IP セットに基づくグループ
- vCenter Server クラスタ
- ハイパーバイザー ホスト

システムの容量画面には、次のオブジェクト カテゴリが表示されます。

- システム全体の仮想インターフェイス
- Edge クラスタ
- システム全体の Edge ノード

設定変更の認識された状態の確認

構成を変更すると、NSX Manager は通常、変更の実装を求める要求を別のコンポーネントに送信します。レイヤー 3 エンティティによっては、API を使用して設定を変更した場合に、要求の状態を追跡して、変更が正常に実装されたかどうかを確認できることがあります。

ユーザーが開始した設定の変更は、最適な状態と呼ばれます。変更を実装した結果は、認識された状態と呼ばれます。NSX Manager が変更を正常に実装した場合は、認識された状態が最適な状態と同じになります。エラーがある場合は、認識された状態が最適な状態と同じになりません。

レイヤー 3 エンティティによっては、API を呼び出して設定を変更した場合、応答にパラメータ `request_id` が含まれることがあります。パラメータ `request_id` および `entity_id` を使用して API 呼び出しを行い、要求の状態を特定することができます。

この機能は、次のエンティティおよび API をサポートしています。

```
EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
```

AdvertisementConfig

```
PUT /logical-routers/<logical-router-id>/routing/advertisement
```

AdvertiseRouteList

```
PUT /logical-routers/<logical-router-id>/routing/advertisement/rules
```

NatRule

```
POST /logical-routers/<logical-router-id>/nat/rules
```

```
PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>
```

```
DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>
```

DhcpRelayService

```
POST /dhcp/relays
```

```
PUT /dhcp/relays/<relay-id>
```

```
DELETE /dhcp/relays/<relay-id>
```

DhcpRelayProfile

```
POST /dhcp/relay-profiles
```

```
PUT /dhcp/relay-profiles/<relay-profile-id>
```

```
DELETE /dhcp/relay-profiles/<relay-profile-id>
```

StaticHopBfdPeer

```
POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
```

```
PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
```

IPPrefixList

```
POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
```

```
PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

RouteMap

```
POST /logical-routers/<logical-router-id>/routing/route-maps
```

```
PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

RedistributionConfig

```
PUT /logical-routers/<logical-router-id>/routing/redistribution
```

RedistributionRuleList

```
PUT /logical-routers/<logical-router-id>/routing/redistribution/rules
```

BfdConfig

```
PUT /logical-routers/<logical-router-id>/routing/bfd-config
```

MplsConfig

```
PUT /logical-routers/<logical-router-id>/routing/mps
```

RoutingGlobalConfig

```
PUT /logical-routers/<logical-router-id>/routing
```

IPSecVPNIKEProfile

```
POST /vpn/ipsec/ike-profiles
```

```
PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
```

```
DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>
```

IPSecVPNPDProfile

```
POST /vpn/ipsec/dpd-profiles
PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>
```

IPSecVPNTunnelProfile

```
POST /vpn/ipsec/tunnel-profiles
PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
```

IPSecVPNLocalEndpoint

```
POST /vpn/ipsec/local-endpoints
PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>
```

IPSecVPNPeerEndpoint

```
POST /vpn/ipsec/peer-endpoints
PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
```

IPSecVPNService

```
POST /vpn/ipsec/services
PUT /vpn/ipsec/services/<service-id>
DELETE /vpn/ipsec/services/<service-id>
```

IPSecVPNSession

```
POST /vpn/ipsec/sessions
PUT /vpn/ipsec/sessions/<session-id>
DELETE /vpn/ipsec/sessions/<session-id>
```

DhcpServer

```
POST /dhcp/servers
PUT /dhcp/servers/<server-id>
DELETE /dhcp/servers/<server-id>
```

DhcpStaticBinding

```
POST /dhcp/servers/static-bindings
PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>
```

DhcpIpPool

```
POST /dhcp/servers/ip-pools
PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>
```

DnsForwarder

```
POST /dns/forwarders
PUT /dns/forwarders/<forwarder-id>
DELETE /dns/forwarders/<forwarder-id>
```

次の API を呼び出して、認識された状態を取得できます。

```
EdgeCluster
Request - GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>
Response - An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the
edge cluster is deleted then the state will be unknown and it will return the common entity
not found error.

LogicalRouter / All L3 Entites - All L3 entities can use this API to get realization state
Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of
logical router but if the logical router itself is deleted then the state will be unknown and
it will return the common entity not found error.

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API
to get the realization state
Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-
id>
Response - An instance of LogicalServiceRouterClusterState which will inherit
ConfigurationState.

LogicalRouterPort / DhcpRelayService / DhcpRelayProfile
Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint /
IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession
Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>
Response - An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If
the session is deleted then the state will be unknown and it will return the common entity
not found error. When IPSecVPNService is disabled, IKE itself is down and it does not
respond. It will return unknown state in such a case.

DhcpServer
Request - GET /dhcp/servers/<server-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpStaticBinding
Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?
request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpIpPool
Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DnsForwarder
Request - GET /dns/forwarders/<forwarder-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.
```

API の詳細については、『NSX-T Data Center API リファレンス』を参照してください。

オブジェクトの検索

さまざまな条件を使用して、NSX-T Data Center 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>>) に管理者権限でログインします。
- 2 ホームページでオブジェクトまたはオブジェクト タイプの検索パターンを入力します。

検索パターンを入力すると、検索機能でキーワードを表示する補助機能を使用できます。

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\!

関連する検索結果がリスト表示され、リソース タイプ別に異なるタブにグループ化されます。

タブをクリックすると、リソース タイプに対する特定の検索結果が表示されます。

- 3 (オプション) 検索条件の絞り込みを保存するには、検索バーの [保存] アイコンをクリックします。
- 4 検索バーで、 アイコンをクリックすると、検索を絞り込むことができる詳細検索列が開きます。
- 5 1 つ以上の条件を指定して、検索を絞り込みます。

- 名前
- リソース タイプ
- 説明
- ID
- 作成者
- 更新者
- タグ
- 作成日
- 変更日

最近の検索結果および保存された検索条件を表示することもできます。

- 6 (オプション) [すべてをクリア] をクリックして、詳細検索条件をリセットします。

オブジェクト属性によるフィルタリング

NSX Manager 内のオブジェクトを表示するときに、オブジェクトを 1 つまたは複数の属性でフィルタリングできます。たとえば、Tier-0 ゲートウェイの詳細を表示する場合、フィルタに [状態] を選択して、状態が **Down** のゲートウェイのみを表示できます。


次のタイプのフィルタを使用できます。

- 事前定義のフィルタ：オブジェクトに適用できる一般的なフィルタのリストです。
- テキストベースのフィルタ：入力した属性値に基づくフィルタです。このフィルタは、オブジェクトの [名前]、[タグ]、[パス]、[説明] 属性にのみ適用できます。
- 属性と値のペア：フィルタの属性と値のペアを指定できる属性のドロップダウン メニュー。

オブジェクトの複数の属性を使用するか、単一属性の複数の値を使用して、オブジェクトをフィルタリングできます。複数の属性を選択すると、AND 演算子が適用されます。単一属性の複数の値を指定すると、OR 演算子が使用されます。

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 必要なオブジェクトが表示されているタブに移動します。
- 3 オブジェクトのフィルタリングに使用する属性を指定します。

-  をクリックして、事前定義フィルタのリストから選択します。
- [名前]、[タグ]、[パス] または [説明] 属性に値を入力します。
- ドロップダウン メニューから属性を選択して、その値を指定します。たとえば、[状態] で **Down** を指定します。

フィルタ条件を満たすオブジェクトが表示されます。

- 4 (オプション) フィルタをリセットするには、[クリア] をクリックします。

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 Data Center は、コンピュート マネージャをポーリングし、vCenter Server からクラスタ情報を収集します。

vCenter Server コンピュート マネージャを追加する場合は、vCenter Server ユーザーの認証情報を指定する必要があります。vCenter Server 管理者認証情報を指定することも、NSX-T Data Center 専用のロールとユーザーを作成して、このユーザーの認証情報を指定することもできます。このロールには、次の vCenter Server 権限が必要です。

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

vCenter Server ロールと権限の詳細については、vSphere Security のドキュメントを参照してください。

前提条件

- サポート対象の vSphere バージョンを使用していることを確認します。[サポート対象の vSphere バージョン](#) を参照してください。
- IPv6 および IPv4 は vCenter Server と通信します。
- 推奨される数のコンピュート マネージャを使用していることを確認します。<https://configmax.vmware.com/home> を参照してください。

注： NSX-T Data Center では、同じ vCenter Server を複数の NSX Manager に登録できません。

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 [システム] - [ファブリック] - [コンピュート マネージャ] - [追加] を選択します。

3 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 Data Center 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。

4 進行状況アイコンが [処理中] から [未登録] 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] 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] 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

vCenter Server にコンピュート マネージャを登録し、接続状態が「稼動中」と表示されるまでしばらく時間がかかります。

コンピュート マネージャの名前をクリックすると、詳細の表示、コンピュート マネージャの編集、コンピュート マネージャに適用するタグの管理を行うことができます。

vCenter Server が正常に登録されたら、コンピュート マネージャを削除する前に、NSX Manager 仮想マシンをパワーオフして削除しないでください。削除の順序が異なると、新しい NSX Manager を展開するときに、同じ vCenter Server を再度登録できなくなります。vCenter Server が別の NSX Manager に登録されているというエラーが表示されます。

Active Directory の追加

Active Directory は、ユーザーベースの Identity Firewall ルールを作成するときに使用されます。

Windows 2008 は、Active Directory サーバまたは RDSH サーバ OS としてサポートされていません。

NSX Manager に 1 つ以上の Windows ドメインを登録できます。NSX Manager は、グループ、ユーザー情報、およびこれらの関係を登録された各ドメインから取得します。NSX Manager は、Active Directory (AD) の認証情報も取得します。

Active Directory と NSX Manager の同期が完了すると、ユーザー ID に基づいてセキュリティ グループを作成し、ID ベースのファイアウォール ルールを作成できるようになります。

注： Identity Firewall ルールを適用する場合、Active Directory を使用するすべての仮想マシンで Windows Time サービスを [有効] にする必要があります。これにより、Active Directory と仮想マシン間で日付と時刻が同期されるようになります。ユーザーの有効化や削除などの Active Directory グループ メンバーシップの変更は、ログインしているユーザーにすぐに反映されません。ユーザーに変更を反映させるには、ログオフして再度ログインする必要があります。グループ メンバーシップが変更されたときに、Active Directory 管理者がログアウトを強制的に実行することをおすすめします。これは、Active Directory の制限が原因で発生しています。

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 [システム] - [Active Directory] に移動します。
- 3 [Active Directory の追加] をクリックします。
- 4 Active Directory の名前を入力します。
- 5 [NetBIOS 名] および [基本識別名] を入力します。

ドメインの netBIOS 名を取得するには、ドメインまたはドメイン コントローラに属する Windows ワークステーションのコマンド ウィンドウで `nbtstat -n` と入力します。NetBIOS のローカル名テーブルでは、プリフィックスが <00> でタイプがグループのエントリが NetBIOS 名です。

Active Directory ドメインを追加するには、基本識別名（ベース DN）が必要です。ベース DN は、Active Directory ドメイン内のユーザー認証を検索するときに LDAP サーバが使用する開始点となります。たとえば、ドメイン名が corp.local の場合、Active Directory のベース DN の DN は DC=corp,DC=local になります。

- 6 必要に応じて [差分同期の間隔] を設定します。差分同期は、前回の同期イベント以降に変更されたローカル Active Directory オブジェクトを更新します。

Active Directory に加えられた変更は、差分同期または完全同期が実行されるまで NSX Manager に表示されません。

- 7 [保存] をクリックします。

LDAP サーバの追加

LDAP (Lightweight Directory Access Protocol) サーバの設定と機能は、Identity Firewall でのみ使用できます。LDAP は、認証のための一元的な場所を提供します。つまり、LDAP サーバとの接続を設定するときに、ユーザー レコードが外部 LDAP サーバに保存されます。

前提条件

ドメイン アカウントには、ドメイン ツリー内のすべてのオブジェクトでの Active Directory 読み取り権限が必要です。イベント ログ リーダーのアカウントには、セキュリティ イベント ログに対する読み取り権限が必要です。

NSX Manager のクラスタがある場合、すべてのノードが LDAP サーバにアクセスできる必要があります。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [Active Directory] に移動します。
- 3 [LDAP サーバ] タブを選択します。
- 4 [LDAP サーバの追加] をクリックします。
- 5 LDAP サーバの [ホスト] 名を入力します。
- 6 [接続先 (ディレクトリ)] ドロップダウン メニューから、LDAP サーバが接続されている Active Directory を選択します。
- 7 (オプション) [プロトコル] を、LDAP (保護されていない) または LDAPS (保護されている) の中から選択します。
- 8 LDAPS が選択されている場合は、NSX Manager によって提案される SHA-256 のサムプリントを選択するか、SHA-256 サムプリントを入力します。
- 9 LDAP サーバの [ポート] 番号を入力します。
ローカルのドメイン コントローラの場合、デフォルトの LDAP ポート 389 と LDAPS ポート 636 は Active Directory の同期に使用されます。デフォルト値は変更できません。
- 10 Active Directory ドメインに対して少なくとも読み取り専用アクセス権を持つ Active Directory アカウントの [ユーザー名] と [パスワード] を入力します。
- 11 [保存] をクリックします。
- 12 LDAP サーバに接続できることを確認するには、[接続のテスト] をクリックします。

Active Directory の同期

Active Directory オブジェクトを使用すると、ユーザー ID や ID ベースのファイアウォール ルールに基づいてセキュリティ グループを作成できます。

開始後に API を使用して完全同期を手動で終了すると、同期統計が正しく更新されません。

注： IDFW は、ゲスト OS のセキュリティと整合性に依存します。悪意のあるローカル管理者がファイアウォールルールを回避するために ID を偽装する方法は1つではありません。ユーザー ID 情報は、ゲスト仮想マシン内のゲスト イントロスペクション エージェントによって提供されます。セキュリティ管理者は、NSX ゲスト イントロスペクション エージェントが各ゲスト仮想マシンにインストールされ、実行されていることを確認する必要があります。ログイン ユーザーには、エージェントの削除または停止を行う権限を付与してはなりません。

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 [システム] - [Active Directory] に移動します。

- 3 同期する Active Directory の横にある 3 つのボタンのメニュー アイコンをクリックして、次のいずれかを選択します。

メニュー項目	説明
差分の同期	最後の同期以降に変更されたローカル Active Directory オブジェクトが更新される差分同期を実行します。
すべて同期	すべての Active Directory オブジェクトのローカル状態が更新される完全同期を実行します。

- 4 [同期状態の表示] をクリックして、Active Directory の現在の状態、以前の同期状態、同期の状態、および最終同期時刻を表示します。

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 Data Center 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 Data Center 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 Data Center の認証ポリシーではありません。

ユーザーのパスワードの管理

各 NSX Manager および NSX Edge アプライアンスには、3 つのローカル アカウント (admin、audit、および root) があります。これらのユーザーのパスワードを管理することはできますが、ユーザーの追加や削除はできません。

デフォルトでは、audit ユーザーはアクティブになっていません。有効にするには、admin としてログインし、set user audit コマンドを実行して新しいパスワードを入力します。現在のパスワードの入力を求められたら、Enter キーを押します。

デフォルトでは、ユーザーのパスワードは 90 日で有効期限が切れます。パスワードの有効期限は、ユーザーごとに変更または無効にすることができます。

NSX Manager のローカル ユーザーのパスワードが 30 日以内に期限切れになると、NSX Manager Web インターフェイスにパスワードの有効期限の通知が表示されます。ローカル ユーザーのパスワード有効期限を 30 日以下に設定した場合、通知は常に表示されます。

NSX-T Data Center 2.5.1 以降では、通知に「パスワードの変更」リンクが含まれています。リンクをクリックして、Web インターフェイスからローカル ユーザーのパスワードを変更できます。

前提条件

NSX Manager と NSX Edge のパスワードの強度要件について理解しておく必要があります。『NSX-T Data Center インストール ガイド』で「NSX Manager のインストール」と「NSX Edge のインストール」を参照してください。

手順

- 1 アプライアンスの CLI にログインします。

- 2 パスワードを変更するには、`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>
```

- 3 パスワードの有効期限を確認するには、`get user <username> password-expiration` コマンドを実行します。次はその例です。

```
nsx> get user admin password-expiration
Password expires 90 days after last change
nsx>
```

- 4 パスワードの有効期限を日数で設定するには、`set user <username> password-expiration <number of days>` コマンドを実行します。次はその例です。

```
nsx> set user admin password-expiration 120
nsx>
```

- 5 パスワードの有効期限を無効にするには、`clear user <username> password-expiration` コマンドを実行します。次はその例です。

```
nsx> clear user admin password-expiration
nsx>
```

アプライアンスのパスワードのリセット

次の手順は、NSX Manager、NSX Edge と Cloud Service Manager アプライアンスに適用されます。

注： NSX Manager クラスタがある場合、1つの NSX Manager で `root`、`admin`、または `audit` ユーザーのパスワードをリセットすると、クラスタ内の他の NSX Manager のパスワードも自動的にリセットされます。パスワードの同期には数分以上かかることがあります。

ユーザー `admin` または `audit` の名前を変更した場合は、次の手順で新しい名前を使用します。

デフォルトでは、アプライアンスを再起動したときに GRUB 起動メニューが表示されません。次の手順を行う前に、GRUB 起動メニューを表示するように GRUB を設定しておく必要があります。GRUB の設定と GRUB `root` パスワードの変更方法については、『NSX-T Data Center インストール ガイド』の「起動時に GRUB メニューを表示する NSX-T Data Center の設定」を参照してください。

NSX-T Data Center 2.5.2 以降を実行しているときに、`root` のパスワードがわかっている場合、`admin` または `audit` のパスワードを忘れた場合は、次の手順でパスワードをリセットできます。

- 1 `root` としてアプライアンスにログインします。
- 2 NSX Edge の場合は、`/etc/init.d/nsx-edge-api-server stop` コマンドを実行します。それ以外の場合は、`/etc/init.d/nsx-mp-api-server stop` コマンドを実行します。
- 3 `admin` のパスワードをリセットするには、`passwd admin` コマンドを実行します。

- 4 `audit` のパスワードをリセットするには、`passwd audit` コマンドを実行します。
- 5 コマンド `touch /var/vmware/nsx/reset_cluster_credentials` を実行します。
- 6 NSX Edge の場合は、`/etc/init.d/nsx-edge-api-server start` コマンドを実行します。それ以外の場合は、`/etc/init.d/nsx-mp-api-server start` コマンドを実行します。

root ユーザーのパスワードを忘れてしまった場合は、次の手順でパスワードをリセットできます。NSX-T Data Center 2.5.0 または 2.5.1 を実行しているときに、`admin` と `audit` のパスワードをリセットする場合は、次の手順も行います。NSX-T Data Center 2.5.2 以降を実行している場合は、`root` のパスワードをリセットした後、上記の手順で `admin` または `audit` のパスワードをリセットできます。

手順

- 1 アプライアンスのコンソールに接続します。
- 2 システムを再起動します。
- 3 GRUB ブート メニューが表示されたら、すばやく左 **SHIFT** キーまたは **ESC** キーを押します。キーを押すのが遅く、ブート シーケンスが一時停止されなかった場合は、もう一度システムを再起動する必要があります。
- 4 **e** キーを押して、メニューを編集します。

ユーザー名 `root` と `root` の GRUB パスワードを入力します（アプライアンスのユーザー `root` とは異なります）。
- 5 Ubuntu を選択した状態で、カーソルを維持します。
- 6 **e** キーを押して、選択したオプションを編集します。
- 7 `linux` で始まる行を検索します。
- 8 NSX-T Data Center 2.5.0 または 2.5.1 を実行する場合は、次の手順を実行します。
 - a `root=UUID=<ID number>` の後にあるオプションをすべて削除し、UUID の後に `rw single init=/bin/bash` を追加します。
 - b **Ctrl-X** キーを押して、起動します。
 - c ログ メッセージが停止したら、**Enter** キーを押します。

プロンプト `root@(none) :/#` が表示されます。
 - d `root` のパスワードをリセットする場合には、`passwd` コマンドを実行します。

`admin` または `audit` のパスワードをリセットする場合には、`passwd <admin or audit user ID>` コマンドを実行します。

`passwd` コマンドは複数回実行できます。
 - e 新しいパスワードを入力し、再入力して確定します。
 - f NSX Manager でパスワードをリセットする場合には、`touch /var/vmware/nsx/reset_cluster_credentials` コマンドを実行します。

- g コマンド `sync` を実行します。
- h コマンド `reboot -f` を実行します。

9 NSX-T Data Center 2.5.2 以降を実行している場合は、次の手順を実行します。

- a 行の末尾に `systemd.wants=PasswordRecovery.service` を追加します。
- b **Ctrl-X** キーを押して、起動します。
- c `root` の新しいパスワードを入力し、同じパスワードを再入力して確定します。

起動プロセスの完了後、新しいパスワードを使用して `root` としてログインし、パスワードの変更を確認します。

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 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。

サムプリントには、OpenSSL バージョン 1.x 以降を使用する必要があります。vIDM ホストで、`openssl` コマンドは OpenSSL の古いバージョンを実行するため、vIDM ホストで `openssl1` コマンドを使用する必要があります。このコマンドは、vIDM ホストからのみ使用できます。

vIDM ホスト以外のサーバでは、OpenSSL バージョン 1.x 以降を実行している `openssl` コマンドを使用できます。

手順

- 1 vIDM ホストのコンソールにログインするか、ユーザー `sshuser` として vIDM ホストに SSH 接続するか、vIDM ホストに `ping` を実行できる任意のサーバにログインします。
- 2 次のいずれかのコマンドを実行して、vIDM ホストのサムプリントを取得します。
 - vIDM ホストにログインしている場合は、次のように `openssl1` コマンドを実行して、サムプリントを取得します。

```
openssl1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

コマンドの実行中にエラーが発生した場合は、`sudo` コマンドとともに `openssl1`（つまり `sudo openssl1 ...`）を実行する必要があります。

- vIDM ホストを `ping` できるサーバにログインしている場合は、次のように `openssl` コマンドを実行して、サムプリントを取得します。

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

VMware Identity Manager Integration の設定

ID 管理サービスを提供する VMware Identity Manager (vIDM) と NSX-T Data Center を統合することができます。vIDM の展開は、スタンドアローンの vIDM ホストまたは vIDM クラスタのいずれかになります。

vIDM ホストまたはすべての vIDM クラスタのコンポーネントに、認証局 (CA) の署名付き証明書が必要です。これがない場合には、Microsoft Edge や Internet Explorer 11 などの特定のブラウザで NSX Manager から vIDM にログインできないことがあります。vIDM に CA 署名証明書をインストールする方法については、<https://docs.vmware.com/jp/VMware-Identity-Manager/index.html> にある VMware Identity Manager のドキュメントを参照してください。

vIDM に NSX Manager を登録する際には、NSX Manager を参照するリダイレクト URI を指定します。完全修飾ドメイン名 (FQDN) または IP アドレスのいずれかを指定することができます。FQDN または IP アドレスのどちらを使用したかを必ず記録しておきます。vIDM を経由して NSX Manager にログインする際は、同様の方法で URL のホスト名を指定する必要があります。つまり、マネージャの vIDM への登録時に FQDN を使用した場合は URL に FQDN を指定し、登録時に IP アドレスを使用した場合には、URL に IP アドレスを指定する必要があります。正しい URL を指定しないとログインに失敗します。

NSX-T API へのアクセスが必要な場合は、次のいずれかの設定の条件を満たしている必要があります。

- vIDM に既知の CA 署名証明書があること。

- vIDM に vIDM サービス側で信頼されたコネクタ CA 証明書があること。
- vIDM が送信コネクタ モードを使用していること。

注： NSX Manager と vIDM は、同じタイムゾーンにする必要があります。UTC の使用をおすすめします。

仮想 IP または外部のロード バランサを使用していない場合に PTR レコードを作成するように DNS サーバを構成する必要があります（これは、マネージャがノードの物理 IP または FQDN で構成されていることを意味します）。

vIDM を外部のロード バランサと統合するように構成する場合は、ページの読み込みエラーや予期しないログアウトが発生しないように、ロード バランサでセッション パーシステンスを有効にする必要があります。

vIDM の展開が vIDM クラスタの場合、SSL ターミネーションと再暗号化のため vIDM ロード バランサを設定する必要があります。

vIDM が有効になっている場合、ローカル ユーザーのアカウントを使用して、URL `https://<nsx-manager-ip-address>/login.jsp?local=true` から NSX Manager にログインできます。

UserPrincipalName (UPN) を使用して vIDM にログインすると、NSX-T の認証に失敗することがあります。この問題を回避するには、別のタイプの認証情報（SAMAccountName など）を使用します。

NSX Cloud を使用している場合は、URL `https://<csm-ip-address>/login.jsp?local=true` を使用して、別の CSM にログインできます。

前提条件

- vIDM の展開タイプ（スタンドアローンの vIDM ホストまたは vIDM クラスタ）に応じて、vIDM ホストまたは vIDM ロード バランサの証明書サムプリントがあることを確認します。サムプリントを取得するコマンドは、どちらの場合も同じです。[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 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 キーをメモしてください。詳細については、<https://docs.vmware.com/jp/VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html> にある VMware Identity Manager のドキュメントを参照してください。クライアントを作成するときに必要な操作は次のとおりです。
 - [アクセス タイプ] を[サービス クライアント トークン] に設定します。
 - クライアント ID を指定します。
 - [詳細] フィールドを展開して、[共有シークレット キーの生成] をクリックします。
 - [追加] をクリックします。

NSX Cloud の注 NSX Cloud を使用している場合は、vIDM で OAuth クライアントとして CSM が登録されていることも確認します。

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 [システム] - [ユーザー] の順に選択します。
- 3 [設定] タブをクリックします。

- 4 [編集] をクリックします。
- 5 外部ロード バランサとの統合を有効にするには、[外部ロード バランサ統合] 切り替えボタンをクリックします。

注： 仮想 IP (VIP) が設定されている場合 ([システム] - [アプライアンス] - [仮想 IP] の順に選択)、[外部ロード バランサ統合] を有効にしても、この設定は使用されません。vIDM を設定した場合、VIP か外部ロード バランサのいずれかを使用できますが、両方は使用できません。外部ロード バランサを使用する場合は、VIP を無効にします。詳細については、『NSX-T Data Center インストール ガイド』の[クラスタの仮想 IP アドレスの設定](#)を参照してください。

- 6 VMware Identity Manager との連携を有効にするには、[VMware Identity Manager との連携] 切り替えボタンをクリックします。
- 7 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 ホストまたは vIDM ロード バランサの完全修飾ドメイン名 (FQDN)。vIDM の展開タイプ (スタンドアローンの vIDM ホストまたは vIDM クラスタ) によって異なります。
OAuth クライアント ID	vIDM に NSX 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 キー	vIDM に NSX Manager を登録するときに作成されるシークレット キー。
SSL 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)。NSX Manager クラスタを使用している場合は、ロード バランサの FQDN を使用するか、クラスタ VIP の FQDN または IP アドレスを使用します。FQDN を指定する場合は、ブラウザの URL に VMware Identity Manager の FQDN を使用して、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。

- 8 [保存] をクリックします。
- 9 NSX Cloud を使用している場合は、NSX Manager ではなく CSM にログインして、CSM アプライアンスから手順 1 ～ 8 を繰り返します。

VMware Identity Manager 機能の検証

VMware Identity Manager を設定したら、機能を検証します。VMware Identity Manager が正しく設定され、検証されていない場合、ユーザーがログインを試みたときに、権限なし (エラー コード 98) のメッセージが表示されることがあります。

VMware Identity Manager が正しく設定され、検証されていない場合、ユーザーがログインを試みたときに、権限なし (エラー コード 98) のメッセージが表示されることがあります。

手順

- 1 ユーザー名とパスワードを base64 でエンコードします。

次のコマンドを実行してエンコーディングを取得し、末尾の「\n」の文字を削除します。次はその例です。

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhZGlpbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

- 2 各ユーザーが各ノードに API 呼び出しを実行できることを確認します。

リモート認証の curl コマンド `curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy` を使用します。次はその例です。

```
curl -k -H 'Authorization: Remote c2ZhZGlpbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

これにより、次のような認証ポリシーの設定が返されます。

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

コマンドがエラーを返さない場合、VMware Identity Manager は正常に動作しています。これ以上の操作は必要ありません。curl コマンドがエラーを返した場合、ユーザーはロックアウトされている可能性があります。

注： アカウント ロックアウト ポリシーが設定され、ノード単位で適用されています。クラスタ内の1つのノードがユーザーをロックアウトしている場合は、他のノードがない可能性があります。

- 3 ノードでのユーザーのロックアウトをリセットするには：

- a ローカルの NSX Manager admin ユーザーを使用して、認証ポリシーを取得します。

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b 現在の作業ディレクトリにある JSON ファイルに出力を保存します。

- c ファイルを変更して、ロックアウト期間の設定を変更します。

たとえば、多くのデフォルトの設定には、ロックアウトと 900 秒のリセット期間が適用されています。これらの値を次のように変更して、即時リセットを有効にします。

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d 影響を受けるノードに変更を適用します。

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e (オプション) 認証ポリシー設定ファイルを以前の設定に戻します。

これにより、ロックアウトの問題が解決されます。リモート認証 API を呼び出すことができて、ブラウザからログインできない場合は、ブラウザに無効なキャッシュまたは Cookie が保存されている可能性があります。キャッシュと Cookie をクリアして、もう一度やり直してください。

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>

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 time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- 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 コントロール

ロールベースのアクセス コントロール (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 Data Center 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
- ロード バランサ管理者
- ロード バランサ監査者
- VPN 管理者
- ゲスト イントロスペクション管理者
- ネットワーク イントロスペクション管理者

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 21-5. [ロールと権限](#)と表 21-6. [\[ネットワークとセキュリティの詳細設定\]](#) のロールと権限には、各ロールの操作権限が表示されます。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
- LB Adm - ロード バランサ管理者
- LB Aud - ロード バランサ監査者
- VPN Adm - VPN 管理者
- GI Adm - ゲスト イントロスペクション管理者
- NI Adm - ネットワーク イントロスペクション管理者
- FA - フル アクセス
- E - 実行

■ R - 読み取り

表 21-5. ロールと権限

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[ネットワ ーク] > [Tier-0 ゲートウ エイ]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [ネットワ ーク イン ターフェ イス]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [ネットワ ーク スタ ティック ルート]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [ロケール サービス]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [静的 ARP の 設定]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [セグメン ト]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [セグメン ト] > [セ グメント プロファ イル]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[ネットワ ーク] > [IP アド レス ブー ル]	FA	R	FA	FA	R	R	FA	R	R	R	なし	なし	なし

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[ネットワーク転送ポリシー]	FA	R	FA	R	FA	R	FA	R	なし	なし	なし	なし	なし
[ネットワーク] > [DNS]	FA	R	FA	FA	R	R	FA	R	R	R	なし	なし	なし
[ネットワーク] > [ロードバランシング]	FA	R	なし	なし	R	なし	FA	R	FA	R	なし	なし	なし
[ネットワーク] > [NAT]	FA	R	FA	R	FA	R	FA	R	R	R	なし	なし	なし
[ネットワーク] > [VPN]	FA	R	FA	R	FA	R	FA	R	なし	なし	FA	なし	なし
[ネットワーク] > [IPv6 プロファイル]													
[セキュリティ] > [分散ファイアウォール]	FA	R	R	R	FA	R	FA	R	R	R	R	R	R
[セキュリティ] > [ゲートウェイ ファイアウォール]	FA	R	R	R	FA	R	FA	R	なし	なし	なし	なし	FA
[セキュリティ] > [ネットワーク イントロスペクション]	FA	R	R	R	R	R	FA	R	なし	なし	なし	なし	FA
[セキュリティ] > [エンドポイント保護ルール]	FA	R	R	R	R	R	FA	R	なし	なし	なし	FA	なし

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[インベ ントリ] > [コンテキ スト プロ ファイル]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
[インベ ントリ] > [仮想マシ ン]	R	R	R	R	R	R	R	R	R	R	R	R	R
[プランと トラブル シューテ ィング] > [ポート ミラーリ ング]	FA	R	FA	R	R	R	FA	R	なし	なし	なし	なし	なし
[プランと トラブル シューテ ィング] > [ポート ミラーリ ングの割 り当て]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[プランと トラブル シューテ ィング] > [モニタリ ング プロ ファイル の割り当 て]	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
[プランと トラブル シューテ ィング] > [ファイア ウォール の IPFIX プロファ イル]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[プランと トラブル シューテ ィング] > [スイッチ の IPFIX プロファ イル]	FA	R	FA	R	R	R	FA	R	R	R	R	R	R
[システ ム] > [フ アプリッ ク] > [ノ ード] > [ホスト]	FA	R	R	R	R	R	R	R	なし	なし	なし	なし	なし
[システ ム] > [フ アプリッ ク] > [ノ ード] > [ノード]	FA	R	FA	R	FA	R	R	R	R	R	なし	なし	なし
[システ ム] > [フ アプリッ ク] > [ノ ード] > [Edge]	FA	R	FA	R	R	R	R	R	なし	なし	なし	なし	なし
[システ ム] > [フ アプリッ ク] > [ノ ード] > [Edge ク ラスタ]	FA	R	FA	R	R	R	R	R	なし	なし	なし	なし	なし
[システ ム] > [フ アプリッ ク] > [ノ ード] > [割り当 て]	FA	R	FA	R	R	R	なし	なし	R	R	なし	なし	なし

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[システム] > [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	なし	なし	なし
[システム] > [フ ァブリッ ク] > [ノ ード] > [トンネ ル]	R	R	R	R	R	R	R	R	R	R	なし	なし	なし
[システム] > [フ ァブリッ ク] > [ブ ロファイ ル] > [ア ップリン ク プロフ ァイル]	FA	R	R	R	R	R	R	R	R	R	なし	なし	なし
[システム] > [フ ァブリッ ク] > [ブ ロファイ ル] > [Edge ク ラスタ ブ ロファイ ル]	FA	R	FA	R	R	R	R	R	R	R	なし	なし	なし
[システム] > [フ ァブリッ ク] > [ブ ロファイ ル] > [設 定]	FA	R	なし	なし	なし	なし	R	R	なし	なし	なし	なし	なし

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[システム] > [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	なし	なし	なし
[システム] > [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	なし	なし	なし	なし	なし
[システム] > [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	なし	R	R
[システム] > [証 明書]	FA	R	なし	なし	FA	R	なし	なし	FA	R	FA	なし	なし
[システム] > [サ ービス展 開] > [サ ービスイ ンスタ ンス]	FA	R	R	R	FA	R	FA	R	なし	なし	なし	FA	FA
[システム] > [ユ ーティリ ティ] > [サポート バンドル]	FA	R	なし	なし	なし	なし	なし	なし	なし	なし	なし	なし	なし

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[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	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	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	なし	なし	なし
[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	なし	なし	なし
[システム] > [Active Directory]	FA	R	FA	R	FA	FA	R	R	R	R	R	R	R
[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	なし	なし	なし
[システム] > [ライセンス]	FA	R	R	R	R	R	なし	なし	なし	なし	なし	なし	なし
[システム] > [システム管理]	FA	R	R	R	R	R	R	R	なし	なし	なし	なし	なし

表 21-5. ロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[カスタム ダッシュ ボードの 設定]	FA	R	R	R	R	R	FA	R	R	R	R	R	R
[システ ム] > [ラ イフサイ クル管理] > [移行]	FA	なし	なし	なし	なし	なし	なし	なし	なし	なし	なし	なし	なし

表 21-6. [ネットワークとセキュリティの詳細設定] のロールと権限

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[ツール] > [ポート 接続ツ ール]	E	R	E	E	E	E	E	R	E	E	なし	なし	なし
[ツール] > [トレ スフロ ー]	E	R	E	E	E	E	E	R	E	E	なし	なし	なし
[ツール] > [ポート ミラーリ ング]	FA	R	FA	R	R	R	FA	R	なし	なし	なし	なし	なし
[ツール] > [IPFIX]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
[ファイア ウォール] > [分散フ ァイアウ ォール] > [全般]	FA	R	R	R	FA	R	FA	R	なし	なし	なし	なし	R
[ファイア ウォール] > [分散フ ァイアウ ォール] > [設定]	FA	R	R	R	FA	R	FA	R	なし	なし	なし	なし	なし

表 21-6. [ネットワークとセキュリティの詳細設定] のロールと権限 (続き)

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[ファイアウォール] > [Edge ファイア ウォール]	FA	R	R	R	FA	R	FA	R	なし	なし	なし	なし	FA
[ルーティング] > [ルーター]	FA	R	FA	FA	R	R	FA	R	R	R	R	なし	R
[ルーティング] > [NAT]	FA	R	FA	R	FA	R	FA	R	R	R	なし	なし	なし
[DHCP サーバ] > [サーバ プロファ イル]	FA	R	FA	R	なし	なし	FA	R	なし	なし	なし	なし	なし
[DHCP] > [サー バ]	FA	R	FA	R	なし	なし	FA	R	なし	なし	なし	なし	なし
[DHCP] > [リレー プロファ イル]	FA	R	FA	R	なし	なし	FA	R	なし	なし	なし	なし	なし
[DHCP] > [リレー サービス]	FA	R	FA	R	なし	なし	FA	R	なし	なし	なし	なし	なし
[DHCP] > [メタデ ータ プロ キシ]	FA	R	FA	R	なし	なし	なし	なし	なし	なし	なし	なし	なし
IP アドレ ス管理	FA	R	FA	FA	R	R	なし	なし	R	R	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	R	なし	R
[スイッチ ング] > [ポート]	FA	R	FA	FA	R	R	FA	R	R	R	R	なし	R

表 21-6. [ネットワークとセキュリティの詳細設定] のロールと権限 (続き)

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[スイッチ ング] > [スイッチ ング プロ ファイル]	FA	R	FA	FA	R	R	FA	R	R	R	なし	なし	なし
[ネットワ ーク] > [ロード バランサ]	FA	R	なし	なし	R	なし	FA	R	FA	R	なし	なし	なし
[ロード バランシ ング] > [プロファ イル] > [SSL プ ロファイ ル]	FA	R	なし	なし	FA	R	FA	R	FA	R	なし	なし	なし
[インベン トリ] > [グルー プ]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
[インベン トリ] > [IP セッ ト]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
[インベン トリ] > [IP アド レス プー ル]	FA	R	FA	R	なし	なし	なし	なし	R	R	R	R	R
[インベン トリ] > [MAC セ ット]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
[インベン トリ] > [サービ ス]	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R

表 21-6. [ネットワークとセキュリティの詳細設定] のロールと権限（続き）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
[インベ ントリ] > [仮想マシ ン]	R	R	R	R	R	R	R	R	R	R	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	なし	なし	なし	なし	なし	なし	なし	なし	なし

ロールの割り当てまたはプリンシパル ID の追加

VMware Identity Manager が NSX-T Data Center と統合されている場合は、ユーザーまたはユーザー グループにロールを割り当てることができます。プリンシパル ID にロールを割り当てすることもできます。

プリンシパルは、NSX-T Data Center 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。プリンシパル ID がある場合、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できます。プリンシパル ID には、次のプロパティがあります。

- 名前
- ノード ID：プリンシパル ID に割り当てられた任意の英数字です。
- 証明書
- このプリンシパルのアクセス権を示す RBAC ロール

エンタープライズ管理者ロールが割り当てられているユーザー（ローカル、リモート、またはプリンシパル ID）は、プリンシパル ID が所有するオブジェクトを変更または削除できます。エンタープライズ管理者ロールが割り当てられていないユーザー（ローカル、リモート、またはプリンシパル ID）は、プリンシパル ID が所有する保護されたオブジェクトを変更および削除することができません。ただし、保護されていないオブジェクトを変更または削除することはできます。

プリンシパル ID などのユーザー証明書が期限切れになった場合、新しい証明書をインポートし、API 呼び出しを行ってプリンシパル ID ユーザーの証明書を更新する必要があります（以下の手順を参照）。NSX-T Data Center API の詳細については、<https://docs.vmware.com/jp/VMware-NSX-T-Data-Center> で API リソースへのリンクを取得できます。

プリンシパル ID ユーザーの証明書は、次の要件を満たす必要があります。

- SHA 256 ベース。
- 2,048 ビット以上のキーサイズを持つ RSA/DSA メッセージ アルゴリズム。
- ルート証明書にすることはできません。

API を使用して、プリンシパル ID を削除できます。ただし、プリンシパル ID を削除しても、対応する証明書は自動的に削除されません。証明書を手動で削除する必要があります。

プリンシパル ID と証明書の削除手順：

- 1 削除するプリンシパル ID の詳細を取得し、応答の `certificate_id` 値をメモします。

```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 2 プリンシパル ID を削除します。

```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 3 手順 1 で取得した `certificate_id` 値を使用して証明書を削除します。

```
DELETE /api/v1/trust-management/certificates/<certificate_id>
```

前提条件

- ユーザーにロールを割り当てる場合は、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、[VMware Identity Manager Integration 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>>) に管理者権限でログインします。

- 2 [システム] - [ユーザー] の順に選択します。

- 3 ユーザーにロールを割り当てるには、[追加] - [ロールの割り当て] の順に選択します。

- a ユーザーまたはユーザー グループを選択します。
- b ロールを選択します。
- c [保存] をクリックします。

- 4 プリンシパル ID を追加するには、[追加] - [ロールを持つプリンシパル ID] の順に選択します。

- a プリンシパル ID の名前を入力します。
- b ロールを選択します。
- c ノード ID を入力します。
- d 証明書を PEM 形式で入力します。
- e [保存] をクリックします。

- 5 (オプション) NSX Cloud を使用している場合は、NSX Manager の代わりに CSM アプライアンスにログインし、手順 1 ～ 4 を繰り返します。

6 プリンシパル ID の証明書が期限切れで失効した場合は、次の操作を行います。

- a 新しい証明書をインポートして、証明書の ID をメモしておきます。[証明書のインポート](#) を参照してください。
- b 次の API を呼び出して、プリンシパル ID を取得します。

```
GET https://<nsx-mgr>/api/v1/trust-management/principal-identities
```

- c 次の API を呼び出して、プリンシパル ID の証明書を更新します。インポートされた証明書の ID を指定します。また、プリンシパル ID ユーザーの ID も指定する必要があります。

次はその例です。

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?
action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

NSX Manager のバックアップとリストア

NSX Manager クラスタが動作不能になった場合や、使用環境を前の状態にリストアする場合は、バックアップからリストアできます。NSX Manager が運用できない場合、データ プレーンに影響はありませんが、設定を変更できなくなります。

バックアップには 2 つのタイプがあります。

クラスタのバックアップ

このバックアップには、最適な状態の仮想ネットワークが含まれます。

ノードのバックアップ

これは、NSX Manager ノードのバックアップです。

バックアップ方法には次の 2 種類があります。

手動

バックアップはいつでも、手動で実行できます。

自動化

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。最新のバックアップが確保されるように、自動バックアップを使用することを強くお勧めします。

NSX-T Data Center の設定をリストアして、いずれかのバックアップにキャプチャされた状態に戻すことができます。バックアップをリストアする際は、バックアップしたアプライアンスと同じバージョンの NSX Manager 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。

バックアップの構成

バックアップが発生する前に、バックアップ ファイル サーバを構成する必要があります。バックアップ ファイル サーバを構成すると、任意の時刻にバックアップを開始できます。また、自動バックアップのスケジュールを設定することもできます。

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。SHA256 のハッシュ化された ECDSA (256 ビット) キーのみがフィンガープリントとして受け入れられます。[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。

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 [システム] - [バックアップとリストア] の順に選択します。
- 3 画面右上の [編集] をクリックして、バックアップを構成します。
- 4 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。
- 5 必要に応じてデフォルト ポートを変更します。

- 6 プロトコル フィールドはすでに入力されています。この値は変更しないでください。

サポートされているプロトコルは SFTP のみです。

- 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。

初めてファイル サーバを構成する場合は、パスワードを指定する必要があります。その後にファイル サーバを再構成する場合、サーバの IP アドレス（またはホスト名）、ポート、およびユーザー名が同じであれば、パスワードを再入力する必要はありません。

- 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。

ディレクトリがすでに存在している必要があります。/ は使用できません。NSX-T Data Center 展開が複数ある場合は、展開ごとに別のディレクトリを使用する必要があります。バックアップ ファイル サーバが Windows マシンの場合、宛先ディレクトリを指定するときにスラッシュを使用します。たとえば、Windows マシンのバックアップ ディレクトリが c:\SFTP_Root\backup の場合、宛先ディレクトリとして / SFTP_Root/backup を指定します。

注： バックアップ プロセスでは、バックアップ ファイルに非常に長い名前が生成される場合があります。Windows サーバでは、バックアップ ファイルのフルパス名の長さが Windows に設定されている制限を超えていると、バックアップに失敗します。この問題を回避するには、ナレッジベースの記事 <https://kb.vmware.com/s/article/76528> を参照してください。

- 9 バックアップを暗号化するには、[暗号化パスフレーズの変更] 切り替えボタンをクリックして、暗号化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。パスフレーズを忘れた場合は、バックアップをリストアできません。

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。

これを空白のままにして、サーバから提供されたフィンガープリントを受け入れるか、拒否することができます。

11 [スケジュール] タブをクリックします。**12** 自動バックアップを有効にするには、[自動バックアップ] 切り替えボタンをクリックします。**13** [毎週] をクリックしてバックアップの日時を設定するか、[間隔] をクリックしてバックアップの間隔を設定します。**14** [NSX の設定の変更を検出] を有効にすると、ランタイム関連の変更、構成以外の変更またはユーザー設定の変更を検出したときに、予定にない完全な構成バックアップがトリガされます。

設定変更によってトリガされたバックアップの間隔を設定できます。デフォルトは 5 分です。

注： このオプションを使用すると、多くのバックアップが生成される可能性があります。これは慎重に使用してください。

15 [保存] をクリックします。**結果**

バックアップ ファイル サーバを構成した後に [今すぐバックアップ] をクリックすると、いつでもバックアップを開始できます。

古いバックアップの削除

バックアップ ファイル サーバ上では、バックアップが蓄積して、大量のストレージを使用してしまうことがあります。NSX-T Data Center に含まれたスクリプトを実行して、古いバックアップを自動的に削除することができます。

Python スクリプト `nsx_backup_cleaner.py` は NSX Manager の `/var/vmware/nsx/file-store` ディレクトリ内にあります。このファイルにアクセスするには `root` としてログインする必要があります。通常、バックアップ ファイル サーバ上でジョブをスケジュールし、このスクリプトを定期的に行うことで古いバックアップをクリーンアップします。使用に関する次の情報は、スクリプトの実行方法を示します。

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]

Required parameters:
  -d/--dir: Backup root directory
  -k/--retention-period: Number of days need to retain a backup file

Optional parameters:
  -l/--min-count: Minimum number of backup files to be kept, default value is 100
  -h/--help: Display help message
```

バックアップの有効期間は、バックアップのタイムスタンプとスクリプトの実行時間の差として計算されます。この値が保持期間よりも大きく、バックアップの最小値よりもディスク上のバックアップ数の方が多ければ、バックアップが削除されます。

Linux または Windows サーバ上で定期的に行うスクリプトの設定方法については、スクリプトの先頭に記述されたコメントを参照してください。

利用可能なバックアップのリスト

バックアップ ファイル サーバには、NSX Manager のすべてのバックアップが保存されます。リストアップするバックアップを見つけられるようにバックアップのリストを取得するには、`get_backup_timestamps.sh` スクリプトを実行する必要があります。

このスクリプトは NSX Manager に格納されています。フルパス名は `/var/vmware/nsx/file-store/get_backup_timestamps.sh` です。このスクリプトは、Linux マシンまたは NSX-T Data Center アプライアンスでも実行できます。ベスト プラクティスでは、すべての NSX Manager にアクセスできなくなってもこのスクリプトを実行できるように、NSX-T Data Center をインストールした後、NSX Manager ではないマシンにこのスクリプトをコピーする必要があります。バックアップをリストアップする必要があるのに、このスクリプトにアクセスできない場合は、新しい NSX Manager をインストールして、そこでこのスクリプトを実行できます。

スクリプトを別のマシンまたはバックアップ ファイル サーバにコピーするには、管理者として NSX Manager にログインして、CLI コマンドを実行します。次はその例です。

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

スクリプトはインタラクティブ形式で、バックアップ ファイル サーバの設定時に指定した情報の入力を求められます。表示するバックアップ数を指定することができます。各バックアップは、タイムスタンプ、NSX Manager ノードの IP アドレス、または FQDN（NSX Manager ノードが自身の FQDN を公開するように設定されている場合）、およびノード ID とともに表示されます。次はその例です。

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

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、バックアップ時にネットワークの状態がリストアされます。また、NSX Manager によって維持されていた設定もリストアされ、バックアップの作成後にファブリックに行われた変更（ノードの追加や削除など）もすべて調整されます。

バックアップを新しい NSX Manager アプライアンスにリストアする必要があります。

バックアップを作成したときに NSX Manager クラスタを使用していた場合は、同様に NSX Manager クラスタにリストアしてください。リストア プロセスでは、まず 1 台の NSX Manager ノードをリストアします。その後、他の NSX Manager ノードを追加するように求められます。

重要： NSX Manager クラスタ内のノードがまだ利用できる場合は、リストアを開始する前にパワーオフする必要があります。

前提条件

- バックアップ ファイル サーバのログイン認証情報を入手していることを確認します。
- 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。SHA256 のハッシュ化された ECDSA（256 ビット）キーのみがフィンガープリントとして受け入れられます。[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 ファイルのパスフレーズを保持していることを確認します。
- [利用可能なバックアップのリスト](#) の手順に従って、リストアするバックアップを特定します。バックアップを取得した NSX Manager ノードの IP アドレスまたは FQDN をメモします。
- FQDN を公開するように NSX Manager ノードを設定する場合は、DNS サーバで NSX Manager ノードに正引き参照と逆引き参照のエントリを設定する必要があります。

手順

- 1 リストアする NSX Manager クラスタのすべてのノードをパワーオフします。
- 2 バックアップをリストアする新しい NSX Manager ノードを 1 つインストールします。
 - リストアするバックアップのバックアップ リストに IP アドレスが含まれている場合は、同じ IP アドレスを使用して新しい NSX Manager ノードを展開する必要があります。FQDN を公開するように NSX Manager ノードを構成しないでください。

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- リストアするバックアップのバックアップ リストに FQDN が含まれている場合は、その FQDN を新しい NSX Manager ノードに設定する必要があります（詳細については、『NSX-T Data Center インストール ガイド』のトピック「NSX Manager のインストール」で「NSX Manager の FQDN の公開」セクションを参照してください）。また、新しい NSX Manager ノードに元のノードと異なる IP アドレスが設定されている場合は、DNS サーバで NSX Manager ノードの正引き参照と逆引き参照のエントリを新しい IP アドレスで更新する必要があります。

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

新しい NSX Manager ノードが実行され、オンラインになったら、リストアを続行できます。

- 3 ブラウザから、新しい NSX Manager に管理者権限でログインします。
- 4 [システム] - [バックアップとリストア] の順に選択します。
- 5 [リストア] タブをクリックします。
- 6 バックアップ ファイル サーバを構成するには、[編集] をクリックします。
- 7 IP アドレスまたはホスト名を入力します。
- 8 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。
- 9 サーバにログインするには、ユーザー名とパスワードを入力します。
- 10 [宛先ディレクトリ] テキスト ボックスに、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。
- 11 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。
- 12 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。
- 13 [保存] をクリックします。
- 14 バックアップを選択します。
- 15 [リストア] をクリックします。

リストア操作の状態が表示されます。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、特定のアクションを実行するように指示されます。

バックアップに NSX Manager クラスタに関する情報が含まれている場合は、NSX Manager ノードを追加するよう求められます。NSX Manager ノードを追加する選択をしなかった場合でも、リストアは続行できます。

リストア操作の完了後、[リストアの完了] 画面にリストアの結果、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] 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。

また、ログ ファイルを選択して、クラスタのリストアまたはノードのリストアに失敗したかどうかを確認することもできます。get log-file syslog 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。

マネージャを再起動するには、restart service manager コマンドを実行します。

マネージャを再起動するには、reboot コマンドを実行します。

- 16 1台のノードのみが展開されている場合、リストアされた NSX Manager ノードが起動して稼動した後に、追加のノードを展開して NSX Manager クラスタを形成できます。

手順については、『NSX-T Data Center インストール ガイド』を参照してください。

- 17 新しい NSX Manager クラスタが展開されたら、手順 1 でパワーオフした元の NSX Manager クラスタ仮想マシンを削除します。

クラスタの 2 番目と 3 番目のノードの証明書も置き換える必要があります。

結果

バックアップ後にコンピュート マネージャを追加し、リストア後にコンピュート マネージャを再度追加しようとすると、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。[解決] ボタンをクリックすると、エラーを解決して、コンピュート 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 4 を参照してください。vCenter Server に保存されている NSX-T Data Center に関する情報を削除する場合は、[vCenter Server からの NSX-T Data Center の拡張機能の削除](#) の手順を実行します。

アップグレード中のバックアップとリストア

アップグレードの実行中に管理プレーンが応答不能になった場合は、アップグレードの実行中に作成したバックアップをリストアする必要があります。

問題

Upgrade Coordinator がアップグレードされましたが、管理プレーンが応答不能になりました。アップグレードの実行中にバックアップを作成しています。

解決方法

- 1 バックアップを作成した IP アドレスを使用して、管理プレーン ノードを展開します。
- 2 アップグレード プロセスの開始時に使用したアップグレード バンドルをアップロードします。
- 3 Upgrade Coordinator をアップグレードします。
- 4 アップグレード プロセスで作成したバックアップをリストアします。
- 5 必要に応じて、新しいアップグレード バンドルをアップロードします。
- 6 アップグレード プロセスを続行します。

vCenter Server からの NSX-T Data Center 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。コンピュート マネージャを削除すると、vCenter Server の拡張機能が自動的に削除されます。何らかの理由で拡張機能が削除されない場合は、次の手順で拡張機能を手動で削除できます。

前提条件

<https://kb.vmware.com/s/article/2042554> の手順に従って、vCenter Server 管理対象オブジェクト ブラウザ (MOB) へのアクセスを有効にします。

手順

- 1 `https://<vCenter Server hostname or IP address>/mob` で MOB にログインします。
- 2 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。
- 3 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。
- 4 メソッド テーブルの [UnregisterExtension] リンクをクリックします。
- 5 [値] テキスト フィールドに `com.vmware.nsx.management.nsxt` と入力します。
- 6 パラメータ テーブルの下ページの右側にある [メソッドの起動] 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。
- 7 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

NSX Manager クラスタの管理

NSX Manager が動作不能になった場合は、再起動できます。NSX Manager の IP アドレスを変更することもできます。

本番環境で高可用性を実現するには、NSX Manager クラスタに 3 つのメンバーを含めることを強くお勧めします。NSX Manager を削除して新規に展開する場合は、新しい NSX Manager に同じ IP アドレスを設定することも、異なる IP アドレスを設定することもできます。

注： プライマリ NSX Manager ノードは、マネージャ クラスタを作成する前に最初に作成するノードです。このノードは削除できません。プライマリ マネージャ ノードの UI でさらに 2 つのマネージャ ノードを展開してクラスタを作成すると、2 番目と 3 番目のマネージャ ノードにのみ削除オプションが表示されます（歯車アイコンから選択できます）。マネージャ ノードの削除と追加の詳細については、[NSX Manager の IP アドレスの変更](#)を参照してください。

NSX Manager クラスタの構成および状態の表示

NSX Manager ユーザー インターフェイスから NSX Manager クラスタの構成と状態を表示することができます。CLI を使用すると追加の情報を取得できます。

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 [システム] - [概要] の順に選択します。
NSX Manager クラスタの状態が表示されます。
- 3 構成に関する追加情報を表示するには、次の CLI コマンドを実行します。

```
manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
```

Cluster Configuration Version: 3
 Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9

Node Status: JOINED

ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			5c8d01f1-f3ee-4f94-b517-a093d8fbfad3	
10.160.71.225	443	ychin-nsxmanager-ob-12065118-1-F5		
CONTROLLER			06fd0574-69c0-432e-a8af-53d140dbef8f	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
CLUSTER_BOOT_MANAGER			da8d535e-7a0c-4dd8-8919-d88bddde006b8	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
DATASTORE			3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4	
10.160.71.225	9000	ychin-nsxmanager-ob-12065118-1-F5		
MANAGER			eb5e8922-23bd-4c3a-ae22-d13d9195a6bc	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
POLICY			f9da1039-08ad-4a20-bacc-5b91c5d67730	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		

Node UUID: 8ebb0642-201e-6a5f-dd47-a1e38542e672

Node Status: JOINED

ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			3757f155-8a5d-4b53-828f-d67041d5a210	
10.160.93.240	443	ychin-nsxmanager-ob-12065118-2-F5		
CONTROLLER			7b1c9952-8738-4900-b68b-ca862aa4f6a9	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
CLUSTER_BOOT_MANAGER			b5e12db1-5e0d-4e33-a571-6ba258dceb2e	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
DATASTORE			bee1f629-4e23-4ab8-8083-9e0f0bb83178	
10.160.93.240	9000	ychin-nsxmanager-ob-12065118-2-F5		
MANAGER			45ccd6e3-1497-4334-944c-e6bbcd5c723e	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
POLICY			d5ba5803-b059-4fbc-897c-3aace8cf1219	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		

Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea

Node Status: JOINED

ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			bce3cc4c-7d60-45e2-aa7b-cdc75e445a14	
10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5		
CONTROLLER			ced46f5c-9e52-4b31-a1cb-b3dead991c71	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
CLUSTER_BOOT_MANAGER			88b70d31-3428-4ccc-ab57-55859f45030c	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
DATASTORE			fb4aec3c-cae3-4386-b5b9-c0b99b7d9048	
10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5		
MANAGER			82b07440-3ff6-4f67-a1c9-e9327d1686ad	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
POLICY			61f21a78-a56c-4af1-867b-3f24132d53c7	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		

4 状態に関する追加情報を表示するには、次の CLI コマンドを実行します。

```

manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
Group Status: STABLE

Members:
      UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

Group Type: CLUSTER_BOOT_MANAGER
Group Status: STABLE

Members:
      UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

Group Type: CONTROLLER
Group Status: STABLE

Members:
      UUID                                FQDN
IP      STATUS
7b1c9952-8738-4900-b68b-ca862aa4f6a9    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
ced46f5c-9e52-4b31-a1cb-b3dead991c71    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP
06fd0574-69c0-432e-a8af-53d140dbef8f    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP

Group Type: MANAGER
Group Status: STABLE

Members:
      UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

```

```
Group Type: POLICY
Group Status: STABLE
```

```
Members:
```

UUID	FQDN
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225	UP
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240	UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33	UP

```
Group Type: HTTPS
Group Status: STABLE
```

```
Members:
```

UUID	FQDN
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225	UP
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240	UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33	UP

NSX Manager クラスタのシャットダウンとパワーオン

NSX Manager クラスタをシャットダウンする必要がある場合は、次の手順を行います。

手順

- 1 NSX Manager クラスタをシャットダウンするには、一度に1台のマネージャ ノードをシャットダウンします。マネージャ ノードのコマンドライン インターフェイス (CLI) に `admin` としてログインし、`shutdown` コマンドを実行するか vCenter Server からマネージャ ノード仮想マシンをシャットダウンできます。

次の仮想マシンに進む前に、vCenter Server で現在の仮想マシンがパワーオフされていることを確認します。

- 2 NSX Manager クラスタをパワーオンするには、vCenter Server で一度に1台のマネージャ ノード仮想マシンをパワーオンします。

次のノードに進む前に、現在のノードが稼動していることを確認します。

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。

複数の NSX Manager を再起動する必要がある場合は、一度に1つずつ再起動する必要があります。再起動した NSX Manager がオンラインになるまで待機してから、別の再起動を行います。

手順

- 1 NSX Manager の CLI にログインします。

2 次のコマンドを実行します。

```
nsx-manager> reboot  
Are you sure you want to reboot (yes/no): y
```

NSX Manager の IP アドレスの変更

NSX Manager クラスタ内の NSX Manager の IP アドレスを変更できます。このセクションでは、いくつかの方法について説明します。

たとえば、Manager A、Manager B、Manager C から構成されるクラスタがある場合は、次の方法で 1 つ以上のマネージャの IP アドレスを変更できます。

■ シナリオ A :

- Manager A の IP アドレスは 172.16.1.11 です。
- Manager B の IP アドレスは 172.16.1.12 です。
- Manager C の IP アドレスは 172.16.1.13 です。
- 新しい IP アドレス（たとえば、192.168.55.11）を持つ Manager D を追加します。
- Manager A を削除します。
- 新しい IP アドレス（たとえば、192.168.55.12）を持つ Manager E を追加します。
- Manager B を削除します。
- 新しい IP アドレス（たとえば、192.168.55.13）を持つ Manager F を追加します。
- Manager C を削除します。

■ シナリオ B :

- Manager A の IP アドレスは 172.16.1.11 です。
- Manager B の IP アドレスは 172.16.1.12 です。
- Manager C の IP アドレスは 172.16.1.13 です。
- 新しい IP アドレス（たとえば、192.168.55.11）を持つ Manager D を追加します。
- 新しい IP アドレス（たとえば、192.168.55.12）を持つ Manager E を追加します。
- 新しい IP アドレス（たとえば、192.168.55.13）を持つ Manager F を追加します。
- Manager A、Manager B、Manager C を削除します。

■ シナリオ C :

- Manager A の IP アドレスは 172.16.1.11 です。
- Manager B の IP アドレスは 172.16.1.12 です。
- Manager C の IP アドレスは 172.16.1.13 です。
- Manager A を削除します。
- 新しい IP アドレス（たとえば、192.168.55.11）を持つ Manager D を追加します。

- Manager B を削除します。
- 新しい IP アドレス（たとえば、192.168.55.12）を持つ Manager E を追加します。
- Manager C を削除します。
- 新しい IP アドレス（たとえば、192.168.55.13）を持つ Manager F を追加します。

最初の 2 つのシナリオでは、IP アドレスの変更中に、追加する NSX Manager に対して、仮想 RAM、CPU、ディスクの追加が必要になります。

シナリオ C の場合、NSX Manager の数を一時的に減らすため、IP アドレスの変更中に 2 つのアクティブなマネージャのいずれかが使用不能になると、NSX-T の操作に影響を及ぼします。このため、この方法はおすすめしません。このシナリオは、仮想 RAM、CPU、ディスクが追加できず、IP アドレスの変更が必要な状況を想定しています。

注： クラスタの仮想 IP アドレス機能を使用している場合は、新しい IP アドレスに同じサブネットを使用するか、IP アドレスの変更中にクラスタの仮想 IP アドレスを無効にする必要があります。クラスタの仮想 IP アドレスで、すべての NSX Manager が同じサブネットに属しているため、この操作が必要になります。

前提条件

クラスタに、NSX Manager を展開する方法について理解しておいてください。詳細については、『NSX-T Data Center インストール ガイド』を参照してください。

手順

- 1 削除する NSX Manager が手動で展開されている場合は、次の手順を行います。
 - a 次の CLI コマンドを実行して、クラスタから NSX Manager を接続解除します。


```
detach node <node-id>
```
 - b NSX Manager 仮想マシンを削除します。
- 2 削除する NSX Manager が NSX Manager ユーザー インターフェイスを使用して自動的に展開されている場合は、次の手順を実行します。
 - a 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。
この NSX Manager は、削除対象でない必要があります。
 - b [システム] タブで、[NSX 管理ノード] をクリックします。
NSX Manager クラスタの状態が表示されます。
 - c 削除する NSX Manager の歯車アイコンをクリックして、[削除] を選択します。
- 3 新しい NSX Manager を展開します。

NSX Manager ノードのサイズ変更

NSX Manager ノードの CPU コア数またはメモリの量はいつでも変更できます。

通常の動作条件では、3つのすべてのマネージャ ノードで CPU コア数とメモリの量を同じにする必要があります。1つのサイズの NSX Manager から別のサイズの NSX Manager に移行する場合に、NSX 管理クラスタ内の NSX Manager 間で CPU の数またはメモリの量に不一致が生じる可能性があります。

vCenter Server の NSX Manager 仮想マシンにリソース割り当ての予約を設定した場合は、予約の調整が必要になることがあります。詳細については、vSphere のドキュメントを参照してください。

前提条件

- 新しいサイズが、マネージャ ノードのシステム要件を満たしていることを確認します。詳細については、『NSX-T Data Center インストール ガイド』の「NSX Manager 仮想マシンのシステム要件」を参照してください。
- クラスタに、NSX Manager を展開する方法について理解しておいてください。詳細については、『NSX-T Data Center インストール ガイド』を参照してください。
- クラスタからマネージャ ノードを削除する方法については、[NSX Manager の IP アドレスの変更](#)を参照してください。

手順

- 1 新しいサイズの新しいマネージャ ノードを展開します。
- 2 新しいマネージャ ノードをクラスタに追加します。
- 3 古いマネージャ ノードを削除します。
- 4 手順 1～3 を繰り返して、他の 2 つの古いマネージャ ノードを置き換えます。

vCenter Server での ESXi ホスト トランスポート ノードの追加と削除

ESXi ホスト トランスポート ノードは、vCenter Server (VC) 間で移動することも、NSX Manager クラスタ間で移動することもできます。

シナリオ 1 : vCenter Server 1 が NSX Manager クラスタ 1 に接続し、vCenter Server 2 が NSX Manager クラスタ 2 に接続している

ESXi ホスト トランスポート ノードが vCenter Server 1 にある場合、次の手順で ESXi ホスト トランスポート ノードを vCenter Server 2 に移動できます。

- 1 ESXi から NSX をアンインストールします。
- 2 ESXi を vCenter Server 2 に移動します。
- 3 トランスポート ノード プロファイルを ESXi に適用します。

シナリオ 2 : vCenter Server 1 と vCenter Server 2 の両方が NSX Manager クラスタに接続している

ESXi ホスト トランスポート ノードが vCenter Server 1 にある場合、次の手順で ESXi ホスト トランスポート ノードを vCenter Server 2 に移動できます。

- 1 ESXi から NSX をアンインストールします。
- 2 ESXi を vCenter Server 2 に移動します。

- 3 トランスポート ノード プロファイルを ESX1 に適用します。

シナリオ 3 : vCenter Server 1 が NSX Manager クラスタ 1 に接続している

ESX1 ホスト トランスポート ノードが vCenter Server 1 にある場合、次の手順で ESXi ホスト トランスポート ノードをスタンドアローン ホストにして NSX Manager クラスタ 2 に移動できます。

- 1 ESX1 から NSX をアンインストールします。
- 2 NSX Manager クラスタ 2 に ESX1 を追加します。

NSX Edge クラスタでの NSX Edge トランスポート ノードの置き換え

NSX Manager ユーザー インターフェイスまたは API を使用して、NSX Edge クラスタ内の NSX Edge トランスポート ノードを置き換えることができます。

NSX Manager ユーザー インターフェイスを使用した NSX Edge トランスポート ノードの置き換え

次の手順では、NSX Manager ユーザー インターフェイスを使用して NSX Edge クラスタの NSX Edge トランスポート ノードを置き換える方法について説明します。Edge トランスポート ノードは、実行中かどうかに関係なく置き換えることができます。

置き換える Edge ノードが実行されていない場合、新しい Edge ノードには同じ管理 IP アドレスと TEP IP アドレスを設定することができます。置き換える Edge ノードが実行中の場合、新しい Edge ノードには異なる管理 IP アドレスと TEP IP アドレスを設定する必要があります。

前提条件

NSX Edge ノードをインストールし、Edge ノードを管理プレーンに追加し、NSX Edge トランスポート ノードを作成する手順について理解しておく必要があります。詳細については、『NSX-T Data Center インストール ガイド』を参照してください。

手順

- 1 新しい Edge トランスポート ノードに、置き換える Edge トランスポート ノードと同じ構成を設定する場合は、次の API 呼び出しを行って構成を見つけます。

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 『NSX-T Data Center インストール ガイド』の手順に従って、Edge トランスポート ノードをインストールして構成します。

この Edge トランスポート ノードの構成を、置き換える Edge トランスポート ノードと同じにするには、手順 1 で取得した構成を使用します。

- 3 NSX Manager で、[システム] - [ファブリック] - [ノード] - [Edge クラスタ] を選択します。
- 4 最初の列のチェックボックスをクリックして、Edge クラスタを選択します。

- 5 [アクション] - [Edge クラスタ メンバーの置き換え] をクリックします。

置き換えるトランスポート ノードをメンテナンス モードに切り替えることをお勧めします。トランスポート ノードが実行されていない場合は、この推奨を無視しても問題ありません。

- 6 ドロップダウンリストから、置き換えるノードを選択します。
- 7 ドロップダウン リストから、置き換え先のノードを選択します。
- 8 [保存] をクリックします。

API を使用した NSX Edge トランスポート ノードの置き換え

次の手順では、NSX-T API を使用して NSX Edge クラスタの NSX Edge トランスポート ノードを置き換える方法について説明します。Edge トランスポート ノードは、実行中かどうかに関係なく置き換えることができます。

置き換える Edge ノードが実行されていない場合、新しい Edge ノードには同じ管理 IP アドレスと TEP IP アドレスを設定することができます。置き換える Edge ノードが実行中の場合、新しい Edge ノードには異なる管理 IP アドレスと TEP IP アドレスを設定する必要があります。

前提条件

NSX Edge ノードをインストールし、Edge ノードを管理プレーンに追加し、NSX Edge トランスポート ノードを作成する手順について理解しておく必要があります。詳細については、『NSX-T Data Center インストール ガイド』を参照してください。

手順

- 1 新しい Edge トランスポート ノードに、置き換える Edge トランスポート ノードと同じ構成を設定する場合は、次の API 呼び出しを行って構成を見つけます。

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 『NSX-T Data Center インストール ガイド』の手順に従って、Edge トランスポート ノードをインストールして構成します。

この Edge トランスポート ノードの構成を、置き換える Edge トランスポート ノードと同じにするには、手順 1 で取得した構成を使用します。

- 3 API 呼び出しを行って、新しいトランスポート ノードと置き換えるトランスポート 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。次はその例です。

```
GET https://<nsx-manager-IP>/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",
```

- 4 API 呼び出しを行い、NSX Edge クラスタの ID を取得します。id フィールドには NSX Edge クラスタ ID が含まれています。members アレイから NSX Edge クラスタのメンバーを取得します。次はその例です。

```
GET https://<nsx-manager-IP>/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"
    }
  ],
```

- 5 API 呼び出しを行い、NSX Edge クラスタ内のトランスポート ノードを置き換えます。member_index は、置き換えるトランスポート ノードのインデックスと一致する必要があります。

たとえば、トランスポート ノード TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) が失敗し、NSX 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://<nsx-manager-IP>/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

vCenter Server が失われ、リカバリできない場合の NSX-T のリカバリ

vCenter Server (vCenter Server) が失われ、バックアップが存在しないか、バックアップが破損しているなどの理由でリカバリができない場合は、vCenter Server を再度展開した後、次の手順で NSX-T をリカバリします。

新しい vCenter Server には、元の vCenter Server と同じ FQDN と IP アドレスを設定する必要があります。また、同じホストを含む同じクラスタが必要です。vCenter Server に追加するホストにパワーオン状態の仮想マシンがある場合は注意してください。これらが vCenter Server データセンターではなく、正しいクラスタに追加されていることを確認してください。

コンピュータ マネージャ

NSX Manager で、古いコンピュータ マネージャを削除します。次に、新しい vCenter Server をコンピュータ マネージャとして追加します。

ホスト トランスポート ノード

NSX Manager で、ホストが正しい vCenter Server クラスタに表示されます。操作は必要ありません。

Edge ノード

NSX Manager UI から展開された Edge ノードを置き換える必要があります。

- 1 Edge ノードを置き換えるには、[NSX Manager ユーザー インターフェイスを使用した NSX Edge トランスポート ノードの置き換え](#)の手順に従ってください。
- 2 新しい Edge 仮想マシンでゲートウェイ（または論理ルーター）とトンネルが構成されていることを確認します。
- 3 [システム] - [ファブリック] - [Edge トランスポート ノード] の順に移動して、古い Edge ノードを削除します。Edge ノードを選択して、[アクション] - [削除] をクリックします。「パワーオフに失敗しました」などのエラーは無視できます。
- 4 vCenter Server で、古い Edge 仮想マシンをパワーオフし、削除します。
- 5 Edge ノードごとに上記の手順を繰り返します。

NSX Manager

NSX Manager UI から展開された NSX Manager は置き換える必要があります。通常、2 番目と 3 番目の NSX Manager はこの方法で展開されています。

- 1 最初の NSX Manager の UI にログインします。
- 2 [システム] - [アプライアンス] の順に移動し、3 番目の NSX Manager を選択します。[アクション] - [削除] の順にクリックします。Manager の仮想マシンはパワーオフできないため、この操作は失敗します。ここでは強制削除オプションを使用します。[アクション] - [強制的に削除] の順に選択します。
- 3 強制削除が機能しない場合は、次の手順を行います。
 - a 最初の NSX Manager の CLI にログインします。
 - b `get cluster status` コマンドを実行し、3 番目の NSX Manager の UID を取得します。
 - c `detach node <node-uid>` コマンドを実行して、クラスタから 3 番目の NSX Manager を接続解除します。

- d 次の API 呼び出しを実行して、3 番目の NSX Manager を強制的に削除します。

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
      action=delete&force_delete=true
```

- 4 vCenter Server で、3 番目の NSX Manager をパワーオフして削除します。
- 5 3 番目の NSX Manager と同じ構成で新しい NSX Manager を展開します。
- 6 上記の手順を繰り返して、2 番目の NSX Manager を削除します。
- 7 2 つの新しい NSX Manager を展開します。

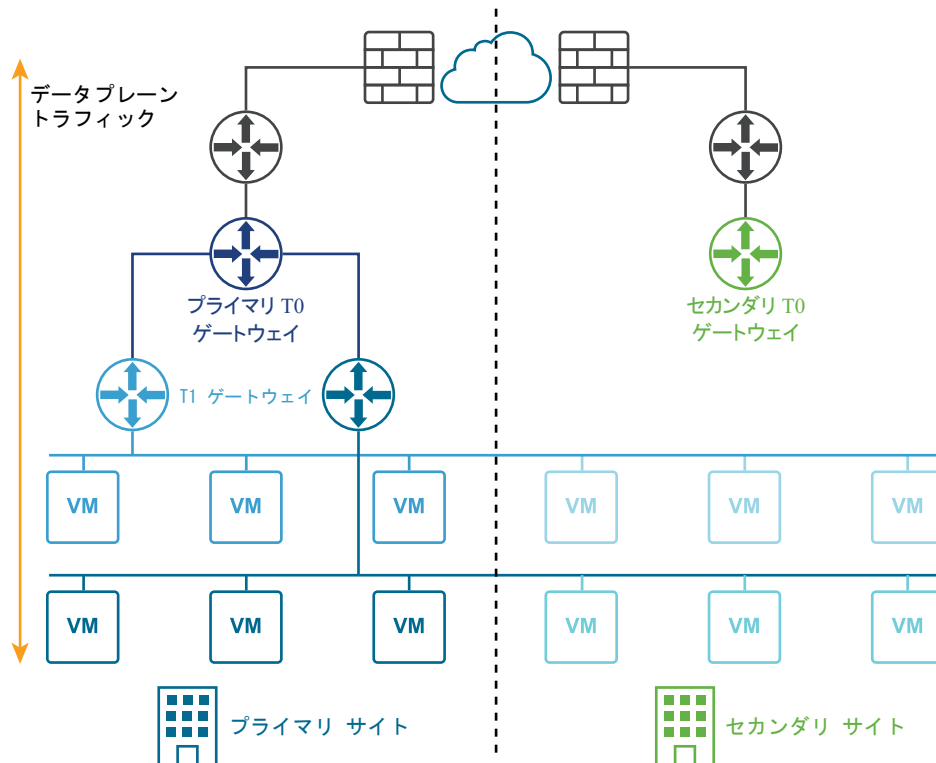
NSX-T Data Center の複数サイトの展開

NSX-T Data Center は複数サイトの展開をサポートしており、1 つの NSX Manager クラスタからすべてのサイトを管理できます。

複数サイトの展開では、2 つのタイプがサポートされています。

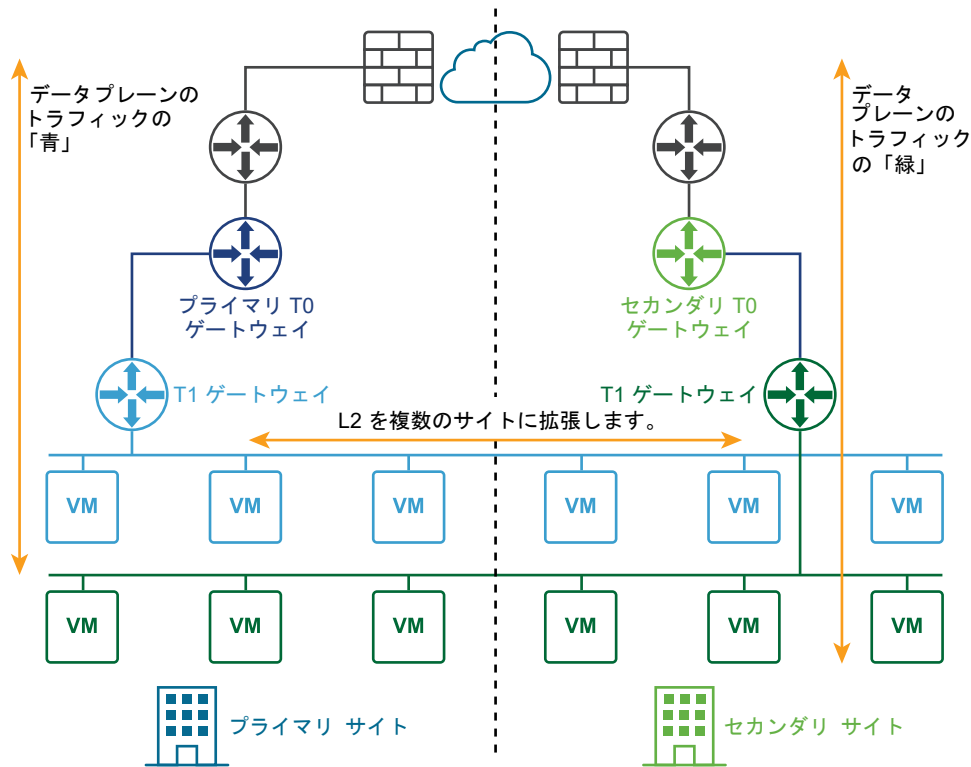
- ディザスタ リカバリ
- アクティブ/アクティブ

次の図に、ディザスタ リカバリの展開を示します。



アクティブ/アクティブ展開で、すべてのサイトがアクティブであり、レイヤー 2 トラフィックがサイトの境界を越えて広がります。ディザスタ リカバリの展開では、プライマリ サイトの NSX-T Data Center は企業のネットワークを処理します。セカンダリ サイトは、プライマリ サイトで致命的な障害が発生した場合に引き継ぐ準備をしています。

次の図に、アクティブ/アクティブ展開を示します。



管理プレーンとデータプレーンのリカバリを自動、手動またはスクリプトで行うため、2つのサイトを展開できます。

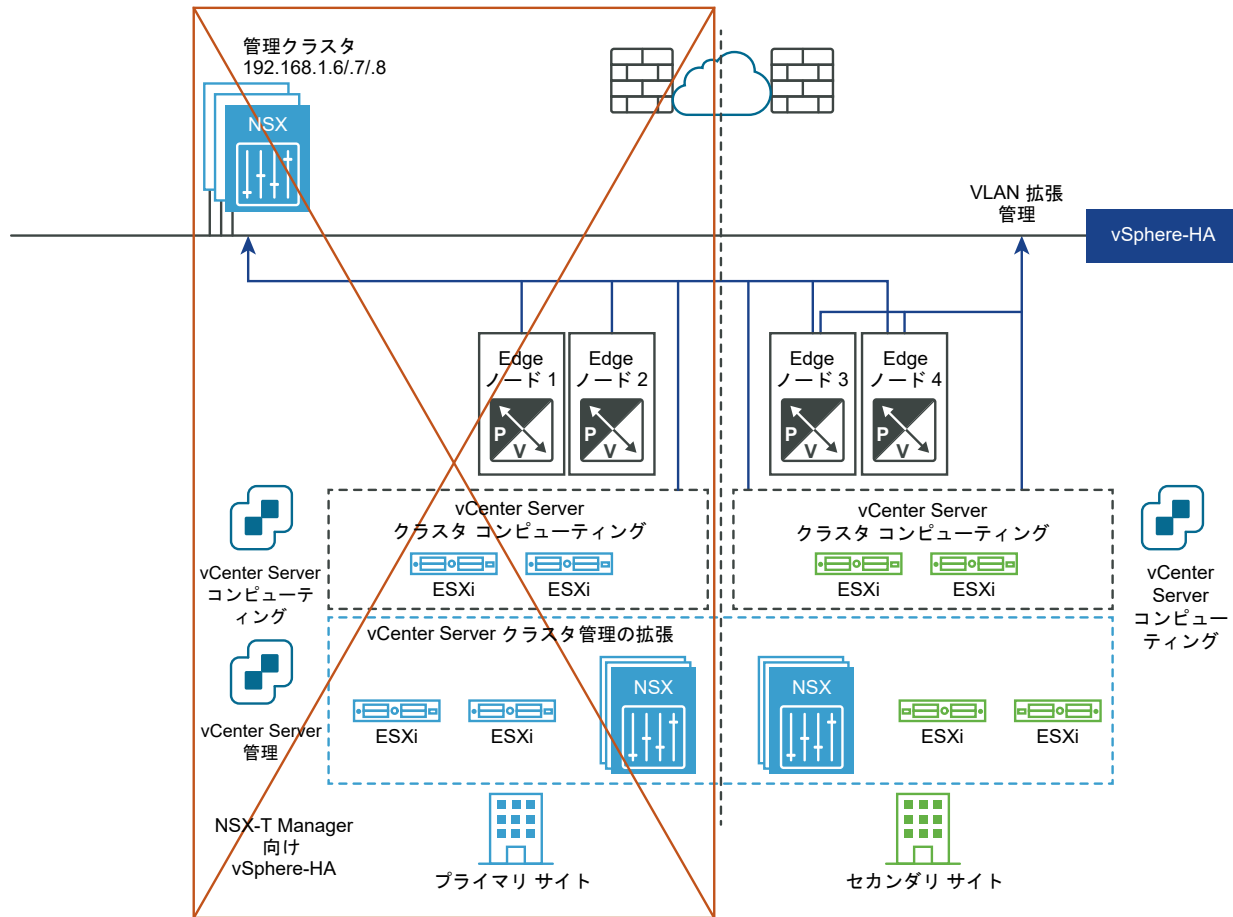
管理プレーンの自動リカバリ

要件：

- 拡張された vCenter Server クラスタでサイト間の HA が設定されている必要があります。
- 管理 VLAN が拡張されている必要があります。

NSX Manager クラスタは管理 VLAN に展開され、プライマリ サイトに物理的に配置されます。プライマリ サイトに障害が発生した場合、vSphere HA はセカンダリ サイトの NSX Manager を再起動します。すべてのトランスポート ノードが、再起動された NSX Manager に自動的に再接続します。このプロセスには約 10 分かかります。この間、管理プレーンは使用できませんが、データプレーンは影響を受けません。

次の図に、管理プレーンの自動リカバリを示します。



データ プレーンの自動リカバリ

要件：

- Edge ノード間の最大遅延が 10 ミリ秒でなければなりません。
- Tier-0 ゲートウェイの HA モードがアクティブ/スタンバイで、フェイルオーバー モードがプリエンプティブに設定されている必要があります。

注：Tier-1 ゲートウェイのフェイルオーバー モードは、プリエンプティブまたは非プリエンプティブに設定できません。

設定手順：

- API を使用して、2 つのサイト（たとえば、FD1A-Preferred_Site1 と FD2A-Preferred_Site1）に障害ドメインを作成します。プライマリ サイトの `preferred_active_edge_services` を `true` パラメータを設定し、セカンダリ サイトに `false` を設定します。

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Site1",
  "preferred_active_edge_services": "true"
}
```

```
POST /api/v1/failure-domains
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- API を使用して、2 つのサイト間で拡張された Edge クラスタを設定します。たとえば、クラスタのプライマリサイトに Edge ノード EdgeNode1A と EdgeNode1B があり、セカンダリサイトに Edge ノード EdgeNode2A と EdgeNode2B があるとします。アクティブな Tier-0 および Tier-1 ゲートウェイは EdgeNode1A と EdgeNode1B で実行されます。スタンバイの Tier-0 および Tier-1 ゲートウェイは EdgeNode2A と EdgeNode2B で実行されます。
- API を使用して、各 Edge ノードをサイトの障害ドメインと関連付けます。最初に GET /api/v1/transport-nodes/<transport-node-id> API を呼び出して、Edge ノードに関するデータを取得します。GET API の結果を PUT /api/v1/transport-nodes/<transport-node-id> API の入力として使用し、追加のプロパティ failure_domain_id を適切に設定します。次はその例です。

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- API を使用して、障害ドメインに基づいてノードを割り当てるように Edge クラスタを設定します。最初に GET /api/v1/edge-clusters/<edge-cluster-id> API を呼び出して、Edge クラスタに関するデータを取得します。GET API の結果を PUT /api/v1/edge-clusters/<edge-cluster-id> API の入力として使用し、追加のプロパティ allocation_rules を適切に設定します。次はその例です。

```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}

PUT /api/v1/edge-clusters/<edge-cluster-id>
{
  "_revision": 0,
```



```

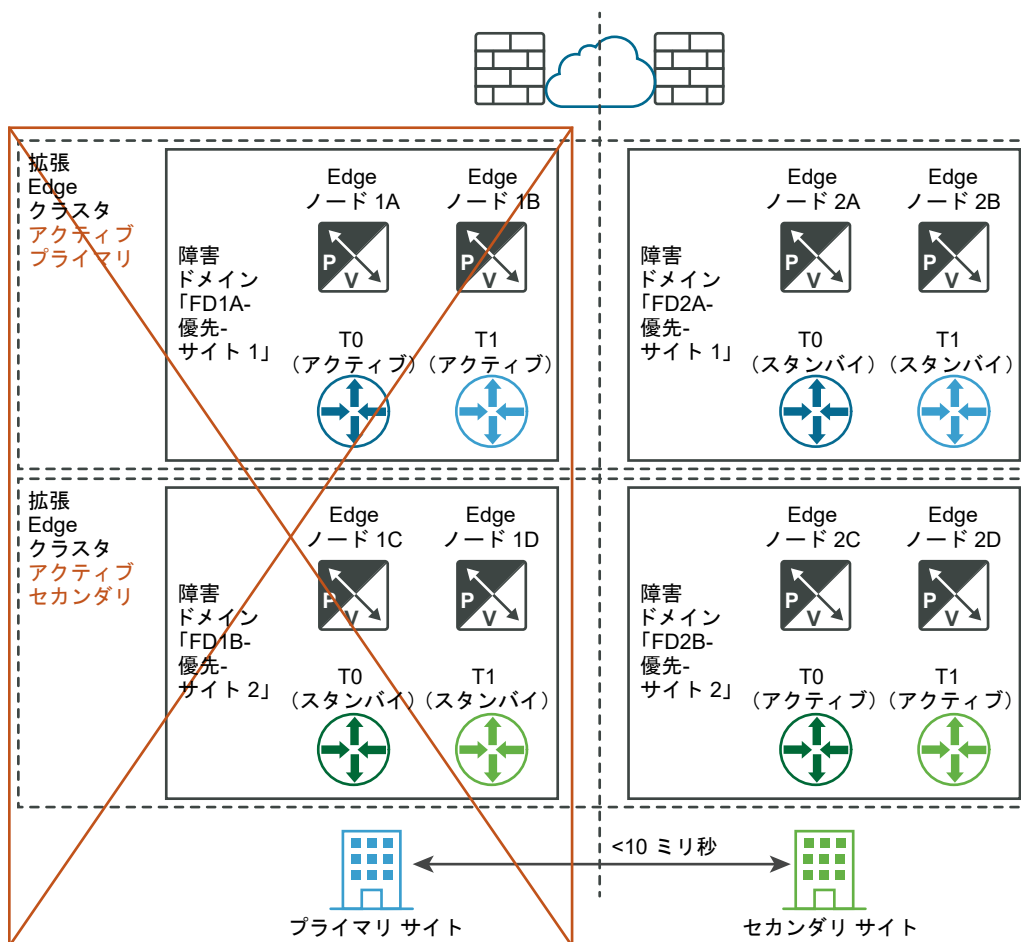
    "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
    "resource_type": "EdgeCluster",
    ...
    "allocation_rules": [
      {
        "action": {
          "enabled": true,
          "action_type": "AllocationBasedOnFailureDomain"
        }
      }
    ],
  },
}

```

- API または NSX Manager のユーザー インターフェイスを使用して、Tier-0 および Tier-1 ゲートウェイを作成します。

プライマリ サイトの Edge ノードで障害が発生すると、そのノードにホストされている Tier-0 および Tier-1 ゲートウェイはセカンダリ サイトの Edge ノードに移行されます。

次の図に、データ プレーンの自動リカバリを示します。



手動/スクリプトによる管理プレーンのリカバリ

要件：

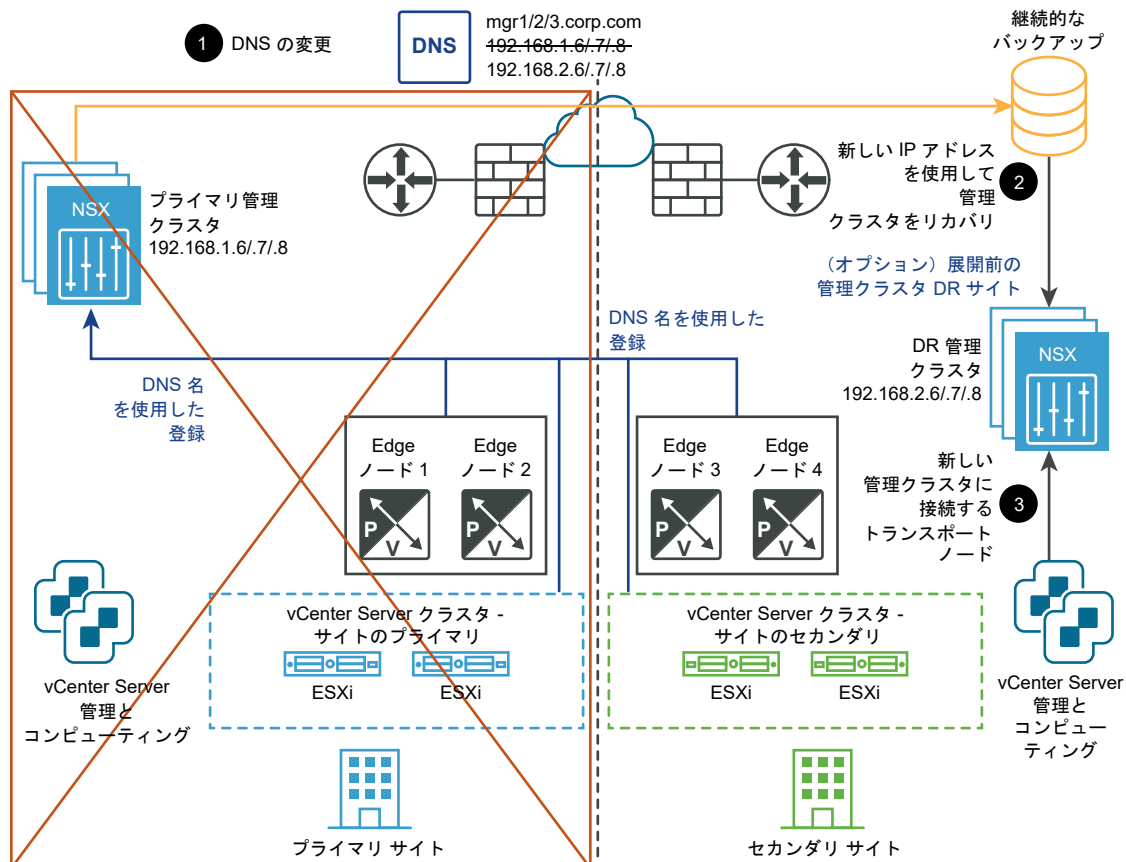
- NSX Manager の DNS に短い TTL（たとえば 5 分）が設定されている必要があります。
- バックアップが継続的に行われている必要があります。

vSphere HA または拡張された管理 VLAN は必要ありません。NSX-T Manager が、短い TTL の DNS 名に関連付けられている必要があります。すべてのトランスポート ノード（Edge ノードとハイパーバイザー）が、DNS 名を使用して NSX Manager に接続する必要があります。時間を節約するため、セカンダリ サイトに NSX Manager クラスタをプリインストールすることもできます。

リカバリ手順は次のとおりです。

- 1 NSX Manager クラスタで異なる IP アドレスを使用できるように DNS レコードを変更します。
- 2 NSX Manager クラスタをバックアップからリストアします。
- 3 新しい NSX Manager クラスタにトランスポート ノードを接続します。

次の図に、手動/スクリプトによる管理プレーンのリカバリを示します。



手動/スクリプトによるデータ プレーンのリカバリ

要件：

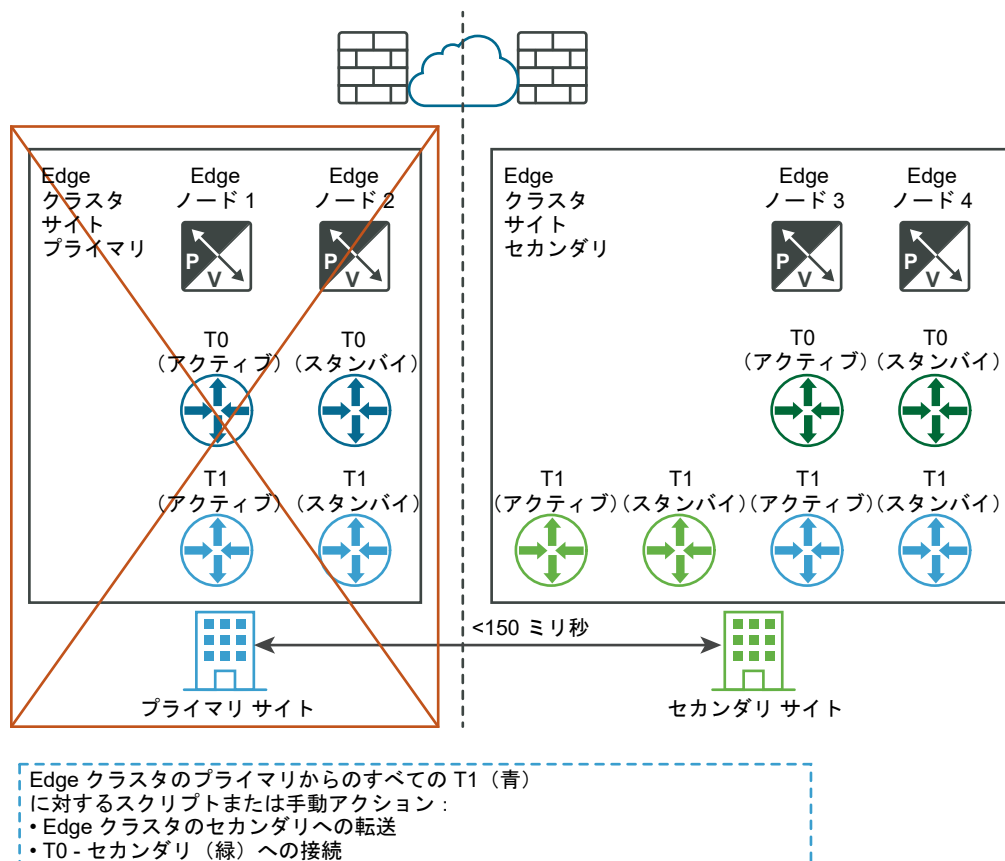
- Edge ノード間の最大遅延が 150 ミリ秒でなければなりません。

Edge ノードには仮想マシンまたはベアメタルを使用できます。Tier-0 ゲートウェイは、アクティブ/スタンバイまたはアクティブ/アクティブにできます。Edge ノードの仮想マシンは、別の vCenter Server にインストールできます。vSphere HA は必要ありません。

リカバリ手順は次のとおりです。

- 1 ディザスタ リカバリ (DR) サイトの既存の Edge クラスタに、スタンバイ Tier-0 ゲートウェイを作成します。
- 2 API を使用して、Tier-0 ゲートウェイに接続されている Tier-1 ゲートウェイを DR サイトの Tier-0 ゲートウェイに移動します。
- 3 API を使用して、スタンドアローン Tier-1 ゲートウェイを DR サイトに移動します。
- 4 API を使用して、レイヤー 2 ブリッジを DR サイトに移動します。

次の図に、手動/スクリプトによるデータ プレーンのリカバリを示します。



複数サイトの展開の要件

サイト間の通信

- 帯域幅は 1 Gbps 以上で、遅延 (RTT) は 150 ミリ秒未満である必要があります。

- MTU は 1,600 以上である必要があります。推奨は 9,000 です。

NSX Manager 設定

- NSX-T Data Center 設定の変更時の自動バックアップを有効にする必要があります。
- FQDN を使用できるように NSX Manager を設定する必要があります。

データ プレーン リカバリ

- NAT やロード バランサなどのサービスを介してパブリック IP アドレスを公開する場合は、同じインターネット プロバイダを使用する必要があります。
- Tier-0 ゲートウェイの HA モードがアクティブ/スタンバイで、フェイルオーバー モードがプリエンプティブに設定されている必要があります。

クラウド管理システム

- クラウド管理システム (CMS) は NSX-T Data Center プラグインをサポートする必要があります。このリリースでは、VMware Integrated OpenStack (VIO) および vRealize Automation (vRA) がこの要件を満たしています。

制限事項

- Local Egress 機能はありません。すべての North-South トラフィックは 1 つのサイト内で発生する必要があります。
- コンピューティング ディザスタリ カバリ ソフトウェアが VMware SRM 8.1.2 以降などの NSX-T Data Center をサポートしている必要があります。

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 Data Center 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 Data Center API ガイド』を参照してください。

表 21-7. 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 および NSX Edge)	API リクエスト (NSX Manager のみ)
システムのタイムゾーンを設定	<code>set timezone <timezone></code>	PUT <a href="https://<nsx-mgr>/api/v1/node">https://<nsx-mgr>/api/v1/node
NTP サーバを設定	<code>set ntp-server <ntp-server></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/services/ntp">https://<nsx-mgr>/api/v1/node/services/ntp
DNS サーバを設定	<code>set name-servers <dns-server></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/name-servers">https://<nsx-mgr>/api/v1/node/network/name-servers
DNS 検索ドメインを設定	<code>set search-domains <domain></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/search-domains">https://<nsx-mgr>/api/v1/node/network/search-domains

ライセンス キーの追加とライセンス使用レポートの生成

ライセンス キーを追加し、ライセンス使用レポートを生成することができます。使用レポートは、CSV 形式のファイルです。

次の非評価版の NSX-T Data Center ライセンス タイプを使用できます。

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office (ROBO)
- NSX Advanced (NSX-T Data Center 2.5.1 以降で利用可能)
- NSX Enterprise (NSX-T Data Center 2.5.1 以降で利用可能)

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。デフォルトの評価版ライセンスがある場合は、新しい評価版ライセンスを割り当てることができます。新しい評価版ライセンスは、デフォルトの評価版ライセンスをオーバーライドします。デフォルト以外の評価版ライセンスの割り当てを解除することもできます。その場合は、デフォルトの評価版ライセンスがリストアされます。

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。

ライセンスが 60 日以内に期限切れになる場合や、すでに期限切れになっている場合、NSX Manager にログインすると、状況を通知するウィンドウが表示されます。ウィンドウの右上隅にある通知アイコンをクリックして、通知を確認することもできます。

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 [システム] - [ライセンス] - [追加] を選択します。
- 3 ライセンス キーを入力します。
- 4 ライセンス使用レポートを生成するには、[エクスポート] - [ライセンス使用レポート] の順に選択します。

CSV レポートには、仮想マシン、CPU、一意の同時実行ユーザー、以下の機能の仮想 CPU とコアの使用数がリストされます。

- スイッチおよびルーティング

- NSX Edge ロード バランサ
- VPN
- 分散ファイアウォール (DFW)
- コンテキスト対応マイクロ セグメンテーション - アプリケーション ID
- コンテキスト対応マイクロ セグメンテーション - リモート デスクトップ セッション ホスト用の Identity Firewall
- サービス挿入
- Identity Firewall
- 拡張ゲスト イントロスペクション

注： Limited Export リリース バージョンでは、次の機能が無効になっています。

- IPsec VPN
 - HTTPS ベースのロード バランサ
-

証明書の設定

証明書をインポートして証明書署名リクエスト (CSR) を作成し、自己署名証明書を生成して、証明書失効リスト (CRL) をインポートできます。

NSX-T Data Center のインストール後、マネージャ ノードとクラスタに自己署名証明書が作成されます。セキュリティを向上させるため、自己署名証明書を CA 署名証明書に置き換えることを強くおすすめします。

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、有効化が完了した後で、デフォルトの自己署名証明書を置き換えることができます。

RSA ベースの証明書のみがサポートされます。

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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。

3 [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	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。証明書は暗号化できません。CA 署名証明書の場合、証明書 - 中間 ルートの順序でチェーン全体を含めるようにしてください。
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。
パスフレーズ	この証明書が暗号化されている場合は、パスフレーズを追加します。このリリースでは、暗号化された証明書がサポートされていないため、このフィールドは使用しません。
説明	この証明書の内容の説明を入力します。
サービス証明書	この証明書をロード バランサや VPN などのサービスで使用する場合は、[はい] に設定します。この証明書が NSX Manager ノード用の場合は、[いいえ] に設定します。

4 [インポート] をクリックします。

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、コモン ネーム、地域、国/地域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/地域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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。
- 3 [CSR] 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。

オプション	説明
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/地域	組織が存在する国/地域を入力します。 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 [生成] 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できます。インポートと有効化が完了すると、この CA によって署名された他の証明書は NSX-T Data Center によって信頼されます。

RSA ベースの証明書のみがサポートされます。

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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。
- 3 [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。
サービス証明書	この証明書をロード バランサや VPN などのサービスで使用する場合は、[はい] に設定します。この証明書が NSX Manager ノード用の場合は、[いいえ] に設定します。

- 4 [インポート] をクリックします。

自己署名証明書の作成

自己署名証明書を作成できます。ただし、自己署名証明書を使用する方法は、信頼されている証明書を使用する方法よりも安全性が低くなります。

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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。
- 3 [CSR] タブをクリックします。
- 4 CSR を選択します。
- 5 [アクション] - [CSR の自己署名証明書] の順に選択します。
- 6 自己署名証明書の有効期間を入力します。
デフォルトは 10 年です。
- 7 [追加] をクリックします。

結果

[証明書] タブに自己署名証明書が表示されます。

NSX Manager ノードまたは NSX Manager クラスタ仮想 IP の証明書の置き換え

API 呼び出しを使用すると、マネージャ ノードまたはマネージャ クラスタ仮想 IP (VIP) の証明書を置き換えることができます。

NSX-T Data Center のインストール後、マネージャ ノードとクラスタに自己署名証明書が作成されます。セキュリティを向上させるため、自己署名証明書を CA 署名証明書に置き換え、各ノードに異なる証明書を使用することを強くおすすめします。

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。[証明書のインポート](#) 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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。
- 3 [ID] 列で、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。
この証明書のインポート時に [サービス証明書] オプションが [いいえ] に設定されていたことを確認します。

- 4 マネージャ ノードの証明書を置き換えるには、POST `/api/v1/node/services/http?action=apply_certificate` API 呼び出しを使用します。次はその例です。

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

注：証明書チェーンは、業界標準である「証明書 - 中間 - ルート」の順序にする必要があります。

API の詳細については、『NSX-T Data Center API リファレンス』を参照してください。

- 5 マネージャ クラスタ VIP の証明書を置き換えるには、POST `/api/v1/cluster/api-certificate?action=set_cluster_certificate` API 呼び出しを使用します。次はその例です。

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

注：証明書チェーンは、業界標準である「証明書 - 中間 - ルート」の順序にする必要があります。

API の詳細については、『NSX-T Data Center API リファレンス』を参照してください。VIP を設定していない場合、この手順を行う必要はありません。

証明書失効リストのインポート

証明書失効リスト (CRL) は、サブスクライ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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。
- 3 [CRL] 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----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMaoGA1 UECBMD UUxEMRkwFwYDVQQKExBNaW5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbMBkG A1UEAxMSU1NMZW5IGRlbW8gc2VydmVyFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA OGCSqG S1b3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL-- </pre>
説明	CRL の内容について簡単な説明を入力します。

- 5 [インポート] 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。

証明書失効リストでの NSX Manager の設定

API を使用すると、証明書失効リスト (CRL) を取得するように NSX Manager を設定できます。その後、CRL の確認を行うには、認証局ではなく、NSX Manager への API 呼び出しを行います。

この機能には、次のメリットがあります。

- CRL はサーバ、つまり NSX Manager のキャッシュに保存しておくほうが効率的です。
- クライアント側で認証局との送信接続を確立する必要はありません。

次の API は証明書失効リストに関連するものです。

```
GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file
```

CRL の配布ポイントを管理し、NSX Manager に保存済みの CRL を取得できます。詳細については、『NSX-T Data Center API リファレンス』を参照してください。

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>>) に管理者権限でログインします。
- 2 [システム] - [証明書] の順に選択します。
- 3 [CSR] タブをクリックします。
- 4 CSR を選択します。
- 5 [アクション] - [CSR の証明書をインポート] の順に選択します。
- 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 [追加] をクリックします。

結果

[証明書] タブに自己署名証明書が表示されます。

パブリック証明書とプライベート キーの保存

パブリック証明書とプライベート キーは、NSX Manager に保存されます。プライベート キーを必要とするロード バランサまたは VPN サービスが作成されると、NSX Manager は、ロードバランサまたは VPN サービスが実行されている Edge ノードにプライベート キーのコピーを送信します。

コンプライアンス ベースの設定

FIPS 140-2 認証を受けている暗号化モジュールを使用して FIPS 準拠モードで実行するように、NSX-T Data Center を設定できます。これらのモジュールは、NIST の暗号モジュール認証プログラム (CMVP) による FIPS 140-2 標準で検証されています。

コンプライアンス レポートを使用すると、FIPS コンプライアンスに対する例外を確認できます。詳細については、[コンプライアンス状態レポートの表示](#)を参照してください。

NSX-T Data Center 2.5 では、次の認証済みモジュールが使用されています。

- VMware OpenSSL FIPS オブジェクト モジュール バージョン 2.0.9 : [Certificate #2839](#)
- VMware OpenSSL FIPS オブジェクト モジュール バージョン 2.0.20-vmw : [Certificate #3550](#)
- BC-FJA (Bouncy Castle FIPS Java API) バージョン 1.0.1 : [Certificate #3152](#)
- VMware IKE 暗号モジュール バージョン 1.1.0 : [Certificate #3435](#)
- VMware VPN 暗号モジュール バージョン 1.0 : [Certificate #3542](#)

VMware が FIPS 140-2 の認定を受けている暗号化モジュールの詳細については、<https://www.vmware.com/security/certifications/fips.html> を参照してください。

デフォルトでは、ロード バランサは FIPS モードがオフになっているモジュールを使用します。ロード バランサで使用されるモジュールの FIPS モードをオンに変更できます。詳細については、[ロード バランサのグローバル FIPS コンプライアンス モードの設定](#)を参照してください。

コンプライアンス状態レポートの表示

NSX-T Data Center 機能のコンプライアンス レポートを表示できます。このレポートを使用すると、IT ポリシーと業界標準に準拠するように NSX-T Data Center 環境を設定できます。

コンプライアンス レポートには、非遵守の構成に関する情報が含まれています。

表 21-8. コンプライアンス レポート情報

コンプライアンス レポートの列	説明	Example
[非遵守コード]	非遵守の種類を表すコード。	72301
[説明]	非遵守の種類の説明。	証明書に認証局 (CA) の署名がありません。
[リソース名]	影響を受けるリソースの名前または ID。	nsx-manager-1
[リソース タイプ]	影響を受けるリソースの種類。	CertificateComplianceReporter
[影響を受けるリソース]	影響を受けるリソースの数。非遵守の構成が存在し、機能が使用されていない場合は、この値が 0 になることもあります。	1

次の API でレポートを取得することもできます。 `GET/policy/api/v1/compliance/status`

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 [ホーム] 画面から、[モニタリング ダッシュボード] - [コンプライアンス レポート] の順にクリックします。

コンプライアンスの状態レポートのコード

コンプライアンスの状態レポートのコードの意味について詳しく説明します。

表 21-9. コンプライアンス レポートのコード

コード	説明	コンプライアンスの状態の送信元	修正方法
72001	暗号化が無効になっています。	この状態は、VPN IPsec プロファイルの設定に NO_ENCRYPTION、 NO_ENCRYPTION_AUTH_AES_G MAC_128、 NO_ENCRYPTION_AUTH_AES_G MAC_192 または NO_ENCRYPTION_AUTH_AES_G MAC_256 encryption_algorithms が含まれている場合に報告されます。 この状態は、報告された非遵守の構成を使用する IPsec VPN セッションの設定に影響します。	この状態を修正するには、準拠している暗号化アルゴリズムを含む VPN IPsec プロファイルを追加し、このプロファイルをすべての VPN 構成で使用します。 IPsec プロファイルの追加 を参照してください。
72011	ネイバーのバイパス整合性チェックの BGP メッセージ。メッセージ認証が定義されていません。	この状態は、BGP ネイバーにパスワードが設定されていない場合に報告されます。 この状態は、BGP ネイバーの設定に影響します。	この状態を修正するには、BGP ネイバーにパスワードを設定し、このパスワードを使用するよう Tier-0 ゲートウェイの設定を更新します。 BGP の設定 を参照してください。
72012	BGP ネイバーとの通信で、脆弱な整合性チェックが使用されています。メッセージ認証に MD5 が使用されています。	この状態は、BGP ネイバーのパスワードに MD5 認証が使用されている場合に報告されます。 この状態は、BGP ネイバーの設定に影響します。	NSX-T Data Center は BGP に MD5 認証のみをサポートしているため、この状態は修正できません。
72021	セキュアなソケット接続の確立に SSL バージョン 3 が使用されています。TLS バージョン 1.1 以降を実行し、プロトコルに脆弱性がある SSL バージョン 3 を完全に無効にすることをおすすめします。	この状態は、ロード バランサのクライアント SSL プロファイル、ロード バランサのサーバ SSL プロファイルまたはロード バランサの HTTPS モニターで SSL バージョン 3 が設定されている場合に報告されます。 この状態は、次の構成に影響します。 ■ ロード バランサ プールが HTTPS モニターに関連付けられている場合。 ■ ロード バランサの仮想サーバが、ロード バランサのクライアント SSL プロファイルまたはサーバ SSL プロファイルに関連付けられている場合。	この状態を修正するには、TLS 1.1 以降を使用するように SSL プロファイルを設定し、このプロファイルをすべてのロード バランサで使用します。 SSL プロファイルの追加 を参照してください。

表 21-9. コンプライアンス レポートのコード（続き）

コード	説明	コンプライアンスの状態の送信元	修正方法
72022	セキュアなソケット接続の確立に TLS バージョン 1.0 が使用されています。TLS バージョン 1.1 以降を実行し、プロトコルに脆弱性がある TLS バージョン 1.0 を完全に無効にすることをおすすめします。	この状態は、ロード バランサのクライアント SSL プロファイル、ロード バランサのサーバ SSL プロファイルまたはロード バランサの HTTPS モニターで TLS バージョン 1.0 が設定されている場合に報告されます。 この状態は、次の構成に影響します。 ■ ロード バランサ プールが HTTPS モニターに関連付けられている場合。 ■ ロード バランサの仮想サーバが、ロード バランサのクライアント SSL プロファイルまたはサーバ SSL プロファイルに関連付けられている場合。	この状態を修正するには、TLS 1.1 以降を使用するように SSL プロファイルを設定し、このプロファイルをすべてのロード バランサで使用します。 SSL プロファイルの追加 を参照してください。
72023	脆弱な Diffie-Hellman グループが使用されています。	このエラーは、VPN IPSec プロファイルまたは VPN IKE プロファイルの設定に Diffie-Hellman グループ（2、5、14、15、16）が含まれている場合に報告されます。グループ 2 と 5 は、脆弱な Diffie-Hellman グループです。グループ 14、15、16 は脆弱なグループではありませんが、FIPS に準拠していません。 この状態は、報告された非遵守の構成を使用する IPsec VPN セッションの設定に影響します。	この状態を修正するには、Diffie-Hellman グループ 19、20 または 21 を使用するよう VPN プロファイルを構成します。 プロファイルの追加 を参照してください。
72024	ロード バランサの FIPS グローバル設定が無効になっています。	このエラーは、ロード バランサの FIPS グローバル設定が無効になっている場合に報告されます。 この状態は、すべてのロード バランサ サービスに影響します。	この状態を修正するには、ロード バランサの FIPS を有効にします。 ロード バランサのグローバル FIPS コンプライアンス モードの設定 を参照してください。
72200	エントロピが十分ではありません。	この状態は、ハードウェアで生成されたエントロピではなく、擬似乱数ジェネレータで生成されたエントロピが使用されている場合に報告されます。 高度なエントロピの生成に必要なハードウェア アクセラレーションが NSX Manager ノードでサポートされていないため、ハードウェアによって生成されたエントロピが使用されていません。	この状態を修正するために、NSX Manager ノードを実行する新しいハードウェアが必要になる場合があります。最新のハードウェアでは、この機能がサポートされています。 注： 基盤となるインフラストラクチャが仮想の場合、真のエントロピは得られません。

表 21-9. コンプライアンス レポートのコード (続き)

コード	説明	コンプライアンスの状態の送信元	修正方法
72201	エントロピ源が不明です。	この状態は、指定されたノードでエントロピの状態が不明な場合に報告されます。	この状態を修正するには、指定されたノードが正常に機能していることを確認します。
72301	証明書に認証局 (CA) の署名がありません。	この状態は、NSX Manager 証明書のいずれかに CA の署名がない場合に報告されます。NSX Manager は次の証明書を使用します。 <ul style="list-style-type: none"> ■ Syslog 証明書。 ■ 個別の NSX Manager ノードの API 証明書。 ■ NSX Manager VIP に使用されるクラスタ証明書。 	この状態を修正するには、CA 署名証明書をインストールします。 証明書の設定 を参照してください。

ロード バランサのグローバル FIPS コンプライアンス モードの設定

ロード バランサには、FIPS コンプライアンス用のグローバル設定があります。デフォルトでは、パフォーマンスを向上させるため、この設定はオフになっています。

ロード バランサの FIPS コンプライアンス用のグローバル構成を変更した場合、新しいロード バランサ インスタンスに影響しますが、既存のロード バランサ インスタンスには影響しません。

ロード バランサ (lb_fips_enabled) の FIPS 用のグローバル設定が *true* に設定されている場合、新しいロード バランサ インスタンスは FIPS 140-2 準拠のモジュールを使用します。既存のロード バランサ インスタンスで、非準拠のモジュールが使用されている可能性があります。

既存のロード バランサに変更を適用するには、ロード バランサを Tier-1 ゲートウェイから接続解除し、再度接続する必要があります。

ロード バランサのグローバル FIPS コンプライアンス 状態を確認するには、GET /policy/api/v1/compliance/status を使用します。

```
...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
    "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_type": "FipsGlobalConfig",
    "is_valid": true
  },
  "affected_resources": [
    {
      "path": "/infra/lb-services/LB_Service",
      "target_id": "/infra/lb-services/LB_Service",
      "target_display_name": "LB_1",
      "target_type": "LBService",
      "is_valid": true
    }
  ]
}
```



```

    }
  ]
},
...

```

注： コンプライアンス レポートには、ロード バランサの FIPS コンプライアンスのグローバル設定が表示されます。特定のロード バランサ インスタンスの FIPS コンプライアンス 状態がグローバル設定と異なる場合があります。

手順

- 1 ロード バランサのグローバル FIPS 設定を取得します。

GET <https://nsx-mgr1/policy/api/v1/infra/global-config>

応答の本文の例：

```

{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937915337,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 2
}

```

- 2 ロード バランサのグローバル FIPS 設定を変更します。

グローバル設定は、新しいロード バランサ インスタンスの作成時に使用されます。設定を変更しても、既存のロード バランサ インスタンスには影響しません。

PUT <https://nsx-mgr1/policy/api/v1/infra/global-config>

要求の本文の例：

```

{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}

```

応答の本文の例：

```
{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}
```

- 3 このグローバル設定を既存のロード バランサ インスタンスで使用する場合は、ロード バランサを Tier-1 ゲートウェイから接続解除し、再度接続する必要があります。

注意： ロード バランサを Tier-1 から接続解除すると、ロード バランサ インスタンスのトラフィックが中断します。

- [ネットワーク] - [ロード バランシング] に移動します。
- 接続解除するロード バランサで、3 つのドット メニュー [...] をクリックし、[編集] をクリックします。
- ⊗ をクリックして [保存] をクリックし、ロード バランサを Tier-1 ゲートウェイから接続解除します。

名前	サイズ	Tier-1 ゲートウェイ
LB_1	Small	TLR1_LR

- 3 つのドット メニュー [...] をクリックして、[編集] をクリックします。
- [Tier-1 ゲートウェイ] ドロップダウン メニューから正しいゲートウェイを選択し、[保存] をクリックしてロード バランサを Tier-1 ゲートウェイに再度接続します。

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場合は、各ノードのマニフェスト ファイルおよびサポート バンドルが含まれる単一のアーカイブ ファイルを入手できます。バンドルをファイル サーバにアップロードする場合は、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。

NSX Cloud のメモ CSM のサポート バンドルを収集する場合、CSM にログインして、[システム] - [ユーティリティ] - [サポート バンドル] の順に移動し、[ダウンロード] をクリックします。PCG のサポート バンドルは、次の手順を実行して NSX Manager から入手できます。PCG のサポート バンドルには、すべてのワークロード仮想マシンのログも含まれています。

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 [システム] - [サポート バンドル] の順に選択します。
- 3 収集対象のノードを選択します。
指定可能なノードのタイプは、[管理ノード]、[Edge]、[ホスト]、[Public Cloud Gateway] です。
- 4 (オプション) ログの収集期間 (日) を指定し、指定した日数以前の古いログを除外します。
- 5 (オプション) スイッチを切り替えて、コア ファイルおよび監査ログを含めるか除外するかを指定します。

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。

- 6 (オプション) チェック ボックスをクリックして、バンドルをリモート ファイル サーバにアップロードするオプションを選択します。
- 7 [バンドル収集を開始] 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 ファイルの数によっては、各ノードの収集に数分ずつかかる場合があります。
- 8 収集プロセスの状態を監視します。
[ステータス] タブには、サポート バンドルの収集に関する進行状況が表示されます。
- 9 リモート ファイル サーバにバンドルを送信するオプションを指定していない場合は、[ダウンロード] をクリックしてバンドルをダウンロードします。

十分なディスク容量がない場合、マネージャ ノードのバンドル収集が失敗することがあります。エラーが発生した場合は、障害が発生したノードに古いサポート バンドルが存在するかどうかを確認します。障害が発生したマネージャ ノードの NSX Manager UI に IP アドレスを使用してログインし、そのノードからバンドル収集を開始します。NSX Manager によってプロンプトが表示されたら、古いバンドルをダウンロードするか、削除します。

ログ メッセージとエラー コード

NSX-T Data Center のコンポーネントは、`/var/log` ディレクトリのログファイルに書き込みます。NSX-T アプライアンスと KVM ホストの NSX Syslog メッセージは RFC 5424 に準拠しています。ESXi ホストの Syslog メッセージは RFC 3164 に準拠しています。

ログの表示

NSX-T アプライアンスの Syslog メッセージは /var/log/syslog にあります。KVM ホストの Syslog メッセージは /var/log/vmware/nsx-syslog に含まれています。

NSX-T アプライアンスでは、次の NSX-T CLI コマンドを実行してログを表示できます。

```
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log |
node-mgmt.log | policy.log | syslog> [follow]
```

ログ ファイルは次のとおりです。

名前	説明
auth.log	認証ログ
controller	コントローラ ログ
controller-error	コントローラ エラー ログ
http.log	HTTP サービス ログ
kern.log	カーネル ログ
manager.log	マネージャ サービス ログ
node-mgmt.log	ノード管理ログ
policy.log	ポリシー サービス ログ
Syslog	システム ログ

ハイパーバイザーでは、tac、tail、grep、more などの Linux コマンドを使用してログを表示できます。

各 Syslog メッセージには、メッセージの送信元を識別するためのコンポーネント (comp) 情報とサブコンポーネント (subcomp) 情報が含まれます。

NSX-T Data Center は、facility local6 のログ (数値 22) を生成します。

監査ログは Syslog の一部です。監査ログ メッセージは、structured-data フィールドの文字列 audit="true" で識別できます。次はその例です。

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy"
username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo",
Operation status="success"
```

各 API 呼び出しにより、1 つの監査ログ メッセージが生成されます。API 呼び出しに関連付けられた監査ログには、次の情報が含まれます。

- API のオブジェクトを識別するためのエンティティ ID パラメータ entId。
- 特定の API 呼び出しを識別するためのリクエスト ID パラメータ req-id。
- API 呼び出しにヘッダー X-NSX-EREQID:<string> が含まれている場合は、外部リクエスト ID パラメータ ereqId。

- API 呼び出しにヘッダー `X-NSX-EUSER:<string>` が含まれている場合は、外部ユーザー パラメータ `euser`。

RFC 5424 および RFC 3164 では、次の重要度が定義されています。

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：重大な問題がある状況
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に、一意のエラー コードが記載されます。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。

ログ メッセージの形式

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 3164 の詳細については、<https://tools.ietf.org/html/rfc3164> を参照してください。

RFC 5424 は、ログ メッセージのに次の形式を定義します。

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

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.
```

エラー コード

エラー コードの完全なリストについては、ナレッジベースの記事 [KB71077NSX-T Data Center 2.x Error Codes](#) を参照してください。

リモート ログの構成

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 Data Center アプライアンスとハイパーバイザーを設定できます。

リモート ログは NSX Manager、NSX Edge、およびハイパーバイザーでサポートされています。各ノードで個別にリモート ログを設定する必要があります。

KVM ホストでは、NSX-T Data Center インストール パッケージにより /etc/rsyslog.d ディレクトリ内に構成ファイルが配置され、rsyslog デーモンが自動的に構成されます。

前提条件

- CLI コマンド `set logging-server` について理解しておく必要があります。詳細については、『NSX-T CLI リファレンス』を参照してください。
- NSX CLI でプロトコルに TLS または LI-TLS を使用してログ サーバとのセキュアな接続を構成している場合、サーバとクライアントの証明書を各 NSX-T Data Center アプライアンスの /image/vmware/nsx/file-store に保存する必要があります。ファイル ストア内の証明書は、NSX CLI を使用してエクスポートが構成されている場合にのみ必要です。API を使用している場合、ファイル ストアを使用する必要はありません。Syslog エクスポートの構成が完了したら、潜在的なセキュリティの脆弱性を回避するため、この場所からすべての証明書とキーを削除する必要があります。
- ログ サーバとのセキュアな接続を構成するには、サーバが CA 署名付き証明書で構成されていることを確認します。たとえば、ログ サーバに Log Insight サーバ `vrli.prome.local` を使用している場合は、クライアントから次のコマンドを実行すると、サーバ上の証明書チェーンを確認できます。

```
root@cserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
 2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE
```

手順

- 1 NSX-T Data Center アプライアンスでリモート ログを構成するには、次のコマンドを実行して、ログ サーバとそのサーバに送信するメッセージのタイプを構成します。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>] [serverca <filename>] [clientca <filename>]
[certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

コマンドを複数回実行し、複数の設定を追加することができます。次はその例です。

```
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
```

リモート サーバに監査ログのみを転送するには、structured-data パラメータに audit="true" を指定します。次はその例です。

```
set logging-server <server-ip> proto udp level info structured-data audit="true"
```

- 2 プロトコルに LI-TLS を使用してセキュアなリモート ログを構成するには、proto li-tls パラメータを指定します。次はその例です。

```
set logging-server vrli.prome.local proto li-tls level info messageid
SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-
full-chain.crt
```

設定に成功すると、テキストのないプロンプトが表示されます。サーバの証明書チェーンの内容（ルートまでの中間認証局）を表示するには、root としてログインして次のコマンドを実行します。

```
root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-
chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
```

成功と失敗の両方のログが /var/log/loginsight-agent/liagent_2020-MM-DD-`<file-num>`.log に記録されます。設定に成功した場合は、次のコマンドを使用して Log Insight の設定を表示できます。

```
root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrli.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" )}

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog
extract_sd=yes

[update]
auto_update=no
```

- 3 プロトコルに TLS を使用してセキュアなリモート ログを構成するには、`proto tls` パラメータを指定します。次はその例です。

```
set logging-server vrli.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem
```

次の点に注意してください。

- `serverCA` パラメータには、完全なチェーンではなく、ルート証明書のみを指定します。
- `clientCA` が `serverCA` と異なる場合は、ルート証明書のみが必要です。
- 証明書には、NSX Manager の完全なチェーンが含まれ、NDcPP 準拠（EKU、BASIC、CDP）になっている必要があります（CDP の場合、このチェックは無視してかまいません）。

各証明書の内容を検査できます。例：

```
root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
```



```

Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1:  DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
  MD5:  36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
  SHA1:  D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
  SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5:  94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1:  42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1:  DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

/var/log/syslog の成功ログの例：

```
<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result:{'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514
```

/var/log/syslog の失敗ログの例：

```
<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"] Certificate trust
check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied
key', 'status': 'ERROR'}
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"] Failed to create
certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
```

```
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED
```

次のコマンドを使用して、証明書とプライベート キーが一致しているかどうか確認できます。一致する場合、出力は writing RSA key になります。それ以外の出力が表示された場合は、一致していません。次はその例です。

```
root@caserter:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key
```

破損したプライベート キーの例：

```
root@caserter:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYVvuUX8IRB48Li3/DufOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthUP8khCwd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Zl0Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf1lDZAHz
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjncQnHI+z6sQvpyJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZYlly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
```

```
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwjK2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----
```

有効なプライベート キーと証明書の例（ただし、それぞれ別のものです）：

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCWd2d2rZ09cUZV10P9
< kIYBb5RMFC7Z10Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDa3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy40iyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvaUzrIbsJh/xp2ShDa
< uKKEY0gUghLtCa3TpV918d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwjK2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX216u5J14/X/pUDI/YHmIf06bsZ1r/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KWVFe3gw3homHU39q4pQjsJsxTcTE3oDMLIY0nWJ0PRUst3DffYUH1L
> W0NUN9ydn+faL2Uf021iuDqVy9V8AH3ON6fu+QCA8nt71ZkzeTxSA0ldp12NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r300itnyAzEGLaRT3//PKfe0Oe
> HCdxGMLrUtMqxIItJahEsqvMufyqNYecVscyXLHPelizKCsQfy8c08LnznG8VAdc
> YILSn3uYGZap6aF1SgVxsvZicwv1YnssmgE13Af0nScmfM96k9h5joHVEkWK6O8v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektR8HdMHQit5uvmMRY3S5zow
> FtvfSDFwxxKyTy6GBRpp+8F+Jq91yGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hbvXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmMveinDhU35IqWEXHAwcCAwEAAQ==
```

- 4 ログの構成を表示するには、`get logging-server` コマンドを実行します。次はその例です。

```
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
```

- 5 リモート ログの構成をクリアするには、次のコマンドを実行します。

```
nsx> clear logging-servers
```

6 ESXi ホストでリモート ログを設定する方法：

- a Syslog を設定してテスト メッセージを送信するには、次のコマンドを実行します。

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b 設定を表示するには、次のコマンドを実行します。

```
esxcli system syslog config get
```

7 KVM ホストでリモート ログを構成するには、次の操作を行います。

- a お使いの環境の /etc/rsyslog.d/10-vmware-remote-logging.conf ファイルを編集します。

- b 次の行をファイルに追加します。

```
*.* @<ip>:514;RFC5424fmt
```

- c 次のコマンドを実行します。

```
service rsyslog restart
```

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 21-10. 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
SWITCHING	Edge クラスタ
	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

表 21-10. ログ メッセージ ID （続き）

メッセージ ID	例
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
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 アップグレード（NSX Manager、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

Syslog 問題のトラブルシューティング

ログがリモート ログ サーバに受信されない場合、次の手順を実行します。

- リモート ログ サーバの IP アドレスを確認します。
- level パラメータが適切に設定されていることを確認します。
- facility パラメータが適切に設定されていることを確認します。
- プロトコルが TLS の場合は、プロトコルを UDP に設定して証明書に不一致があるかどうかを確認します。

- プロトコルが TLS の場合は、ポート 6514 が両端で開いていることを確認します。
- メッセージ ID フィルタを解除して、ログがサーバで受信されているかどうかを確認します。
- `restart service rsyslogd` コマンドを使用して rsyslog サービスを再起動します。

アプライアンス仮想マシンでのシリアル ログの構成

アプライアンス仮想マシンのシリアル ログを構成して、仮想マシンがクラッシュしたときにログ メッセージをキャプチャできます。

手順

- 1 `root` として仮想マシンにログインします。
- 2 `/etc/default/grub` を編集します。
- 3 パラメータ `GRUB_CMDLINE_LINUX_DEFAULT` を見つけて `console=ttyS0 console=tty0` を追加します。
- 4 コマンド `update-grub2` を実行します。
- 5 `/boot/grub/grub.cfg` ファイルに手順 3 での変更が反映されていることを確認します。
- 6 仮想マシンをパワーオフします。
- 7 仮想マシンの構成ファイル (`.vmx`) を編集し、次の行を追加します。

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsRRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

- 8 仮想マシンをパワーオンします。

結果

仮想マシンでカーネル パニックが発生した場合、`.vmx` ファイルと同じ場所に、ログ メッセージを含む `serial.out` ファイルを見つけることができます。

カスタマー エクスペリエンス向上プログラム

NSX-T Data Center は、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加しています。

CEIP を通して収集されるデータおよび VMware のその使用目的に関する詳細は、Trust & Assurance センター (<https://www.vmware.com/solutions/trustvmware/ceip.html>) に記載されています。

NSX-T Data Center の CEIP への参加/参加中止、またはプログラム設定の編集については、[カスタマー エクスペリエンス向上プログラム構成の編集](#)を参照してください。

カスタマー エクスペリエンス向上プログラム構成の編集

NSX Manager のインストール時またはアップグレード時に、CEIP に参加するかどうかを決定し、データ収集について設定することができます。

また、既存の CEIP 設定を編集して、CEIP プログラムへの参加または脱退、情報を収集する頻度と日数の定義、およびプロキシ サーバ設定の定義を行うこともできます。

前提条件

- NSX Manager が接続され、ハイパーバイザーと同期できることを確認します。
- データのアップロードのために、NSX-T Data Center がパブリック ネットワークに接続され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>>) に管理者権限でログインします。
- 2 [システム] - [カスタマー プログラム] を選択します。
- 3 [カスタマー エクスペリエンス向上プログラム] セクションで、[編集] をクリックします。
- 4 [カスタマー エクスペリエンス向上プログラムの編集] ダイアログ ボックスで [VMware カスタマー エクスペリエンス向上プログラムに参加する] チェック ボックスを選択します。
- 5 [スケジュール] スイッチを切り替えて、データ収集を無効または有効にします。
スケジュールはデフォルトで有効になっています。
- 6 (オプション) データの収集とアップロードの繰り返し設定を編集します。
- 7 [保存] をクリックします。

オブジェクトへのタグの追加

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。

NSX Cloud の注 NSX Cloud を使用する場合は、[NSX Cloud でサポートされる NSX-T Data Center の機能](#)を参照して、自動生成される論理エンティティ、サポートされる機能、NSX Cloud に必要な設定を確認してください。

大半のオブジェクトには、最大で 30 個のタグを指定できます。次のオブジェクトの場合、内部で作成されたタグを使用するため、最大値が低くなります。

表 21-11. [ネットワークとセキュリティの詳細] タブで作成したオブジェクトのタグの最大数

オブジェクト	タグの最大数
仮想マシン	25
論理ポート	29

表 21-12. [ネットワーク]、[セキュリティ]、[インベントリ] タブで作成したオブジェクトのタグの最大数

オブジェクト	タグの最大数
グループ	29
セグメント	27
セグメント ポート	29
論理ルーター ポート	30 - ラベル数
NAT ルール	27
IPsec VPN セッション	29

表 21-13. Cloud Service Manager オブジェクトのタグの最大数

オブジェクト	タグの最大数
BFD 健全性モニタリング プロファイル、トランスポート ゾーン、アップリンク ホスト スイッチ プロファイル、トランスポート ノード、Edge クラスタ	23

表 21-14. パブリック クラウド マネージャ オブジェクトのタグの最大数

オブジェクト	タグの最大数
BFD 健全性モニタリング プロファイル、トランスポート ゾーン、論理スイッチ、ノード、トランスポート ノード、Edge クラスタ、論理ルーター、論理ルーター アップリンク ポート、スタティック ルート、DHCP プロファイル、NSGroup、ファイアウォール セクションのルール リスト	23
NAT ルール	20
IP セット、NSGroup	22

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 オブジェクトを編集します。

たとえば、[セグメント] タブに移動して、セグメントを編集します。

3 [タグ] フィールドに移動し、タグを追加します。

各タグには、必須のタグ値と、オプションの範囲値が含まれています。タグの最大長は 256 文字です。範囲の最大長は 128 文字です。

4 [保存] をクリックします。

リモート サーバの SSH フィンガープリントの検索

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

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

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

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 21-15. 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
```

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>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [グループ] 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。

外部ロード バランサの構成

外部ロード バランサを構成して、Manager クラスタ内の NSX Manager にトラフィックを分散させることができます。

NSX Manager クラスタに外部のロード バランサは必要ありません。NSX Manager 仮想 IP (VIP) は、マネージャ ノードで障害が発生した場合に回復性を提供しますが、次の制限があります。

- VIP は、NSX Manager 間でロード バランシングを行いません。
- VIP を使用するには、すべての NSX Manager が同じサブネットに属している必要があります。
- マネージャ ノードで障害が発生した場合、VIP のリカバリに 1 ～ 3 分ほどかかります。

外部ロード バランサには、次のようなメリットがあります。

- NSX Manager 間のロード バランシング。
- 複数の NSX Manager を異なるサブネットに配置できます。
- マネージャ ノードで障害が発生した場合の迅速なリカバリ。

NSX Manager VIP では外部ロード バランサは機能しません。外部ロード バランサを使用している場合は、NSX Manager VIP を設定しないでください。

外部ロード バランサを介してブラウザから NSX Manager にアクセスする場合は、ロード バランサでセッション パーシステンスを有効にする必要があります。

外部ロード バランサを介して API クライアントから NSX Manager にアクセスする場合は、4 つの認証方法を使用できます（詳細については、『NSX-T Data Center API ガイド』を参照してください）。

- HTTP 基本認証：ロード バランサ セッションのパーシステンスは必要ありません。
- クライアント証明書による認証：ロード バランサ セッションのパーシステンスは必要ありません。
- vIDM による認証：ロード バランサ セッションのパーシステンスは必要ありません。

- セッション ベース認証 : ロード バランサ セッションのパーシステンスは必要です。

推奨事項 :

- 外部ロード バランサで、ブラウザと API の両方のアクセスに単一の IP アドレスを構成します。ロード バランサではセッション パーシステンスが有効になっている必要があります。

NSX Cloud を使用すると、NSX-T Data Center を使用してパブリック クラウド インベントリを管理し、安全性を確保することができます。

NSX Cloud 展開ワークフローについては、『NSX-T Data Center インストール ガイド』の [NSX Cloud コンポーネントのインストール](#)を参照してください。

[パブリック クラウド](#)も参照してください。

この章には、次のトピックが含まれています。

- [Cloud Service Manager のクイック ツアー](#)
- [NSX Cloud 検疫ポリシーを使用した脅威の検出](#)
- [NSX 強制モード](#)
- [Native Cloud 強制モード](#)
- [NSX Cloud でサポートされる NSX-T Data Center の機能](#)
- [よくある質問 \(FAQ\)](#)

Cloud Service Manager のクイック ツアー

Cloud Service Manager (CSM) は、パブリック クラウド インベントリに、1つの画面で管理できる管理エンドポイントを提供します。

CSM インターフェイスは、次のように分類されます。

- **[検索]**：検索テキスト ボックスは、パブリック クラウド アカウントや関連する構造を検索するために使用できます。
- **[クラウド]**：パブリック クラウド インベントリは、このカテゴリにあるセクションを使用して管理されます。
- **[システム]**：このカテゴリから Cloud Service Manager の **[設定]**、**[ユーティリティ]**、および **[ユーザー]** の順にアクセスできます。

CSM の **[クラウド]** サブセクションに移動すると、パブリック クラウドのすべての操作を実行できます。

バックアップ、リストア、アップグレード、ユーザー管理などのシステム ベースの操作を実行するには、**[システム]** サブセクションに移動します。

クラウド

[クラウド] にあるセクションは次のとおりです。

クラウド > 概要

[クラウド] をクリックして、パブリック クラウド アカウントにアクセスします。

[概要]：この画面上の各タイルは、パブリック クラウド アカウントと、それに含まれるアカウント数、リージョン数、Virtual Private Cloud (VPC) または VNet、およびインスタンス（ワークロード仮想マシン）数を表します。

次の手順を実行します。

パブリック クラウド アカウント またはサブスクリプションの追加	1つ以上のパブリック クラウド アカウントまたはサブスクリプションを追加することができます。これにより、CSM でパブリック クラウド インベントリを参照することができ、NSX-T Data Center が管理する仮想マシンの数とその状態を表示できます。 詳細な手順については、『NSX-T Data Center インストール ガイド』の「[パブリック クラウド アカウントの追加]」を参照してください。
NSX Public Cloud Gateway の展開または展開解除	1つまたは2つ（High Availability の場合）の PCG を展開または展開解除することができます。CSM から PCG を展開解除することもできます。 詳細な手順については、『NSX-T Data Center インストール ガイド』の「[PCG の展開]」または「[PCG の展開解除]」を参照してください。
検疫ポリシーの有効化または無効化	検疫ポリシーを有効または無効にすることができます。詳細については、 NSX Cloud 検疫ポリシーを使用した脅威の検出 を参照してください。
グリッド表示およびカード表示の切り替え	カードにインベントリの概要が表示されます。グリッドには、詳細が表示されます。アイコンをクリックして、ビュー タイプを切り替えます。

CSM では、パブリック クラウド インベントリをさまざまな方法で表示することで、NSX Cloud に接続されているすべてのパブリック クラウド アカウントの全体像を参照できます。

- 使用中のリージョンの数を表示できます。
- リージョンごとの VPC/VNet の数を表示できます。
- VPC/VNet ごとのワークロード仮想マシンの数を表示できます。

[クラウド] には 4 つのタブがあります。

クラウド > {パブリック クラウド} > アカウント

CSM のアカウント セクションは、追加済みのパブリック クラウド アカウントについての情報を提供します。

各カードは、クラウドで選択したクラウド プロバイダのパブリック クラウド アカウントを表します。

このセクションから、次のアクションを実行することができます。

- アカウントの追加
- アカウントの編集
- アカウントの削除

- アカウントの再同期

クラウド > {パブリック クラウド} > リージョン

リージョン セクションには、選択したリージョンのインベントリが表示されます。

リージョンはパブリック クラウド アカウント別にフィルタリングできます。各リージョンには VPC/VNet とインスタンスがあります。PCG を展開している場合、PCG 健全性のインジケータとともに [ゲートウェイ] としてここに表示されます。

クラウド > {パブリック クラウド} > VPC または VNet

Virtual Private Cloud (VPC) または VNet セクションには、パブリック クラウド インベントリが表示されます。

インベントリはアカウントとリージョン別にフィルタリングすることができます。

- 各カードは、1 つの VPC/VNet を表します。
- トランジット VPC または VNet には 1 つまたは 2 つ（HA の場合）の PCG を展開できます。
- コンピュート VPC/VNet をトランジット VPC/VNet にリンクできます。
- グリッド表示に切り替えて、各 VPC または VNet の詳細を表示できます。

注： グリッド ビューには、[概要]、[インスタンス]、[セグメント] の 3 つのタブが表示されます。

- [概要] には、次の手順で説明するアクションのオプションが表示されます。
 - [インスタンス] には、VPC/VNet 内のインスタンスの一覧が表示されます。
 - [セグメント] には、NSX-T のオーバーレイ セグメントが表示されます。この機能は、NSX Cloud の現在のリリースではサポートされていません。この画面に表示されているタグを使用して、AWS または Microsoft Azure のワークロード仮想マシンにタグを付けないでください。
-
- [アクション] をクリックして、以下を実行できます。
 - [設定の編集]（トランジット VPC/VNet でのみ使用可能）：
 - NSX 強制モード の場合は、検疫ポリシーを有効または無効にします。
 - NSX 強制モード を使用している場合、VPC/VNet が NSX Cloud からオフボーディングされているときに必要なフォールバック セキュリティ グループを指定します。[検疫ポリシーが無効時の影響](#) を参照してください。
 - プロキシ サーバの選択を変更します。
 - [トランジット VPC/VNet へのリンク]：このオプションを使用できるのは、PCG が展開されていない VPC/VNet のみです。リンク先のトランジット VPC/VNet をクリックして選択します。
 - [NSX Cloud Gateway の展開]：このオプションを使用できるのは、PCG が展開されていない VPC/VNet のみです。このオプションをクリックすると、この VPC/VNet への PCG の展開が開始し、この VPC/VNet がトランジット VPC/VNet または自己管理 VPC/VNet になります。詳細手順については、NSX-T Data Center インストール ガイドの「[NSX Public Cloud Gateway の展開またはリンク]」を参照してください。

クラウド > {パブリック クラウド} > インスタンス

インスタンス セクションには、Virtual Private Cloud (VPC) または VNet のインスタンスの詳細が表示されます。

インスタンスのインベントリはアカウント、リージョン、VPC、または VNet でフィルタリングすることができます。

各カードはインスタンス（ワークロード仮想マシン）を示し、サマリが表示されます。

インスタンスの詳細については、カードをクリックするか、グリッド表示に切り替えます。

CSM ホワイトリストにインスタンスを追加したり、インスタンスを削除したりできます。詳細については、[ホワイトリストへの仮想マシンの登録](#)を参照してください。




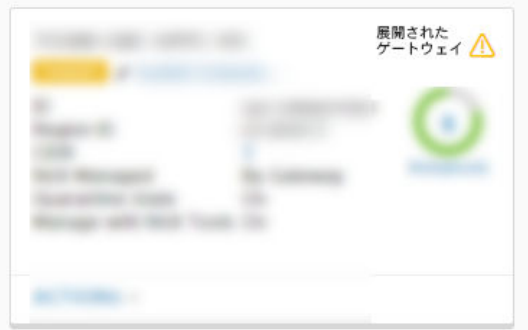
CSM のアイコン

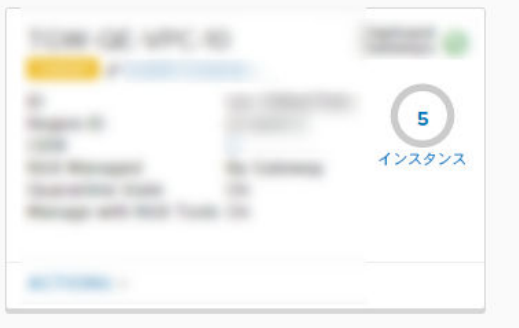
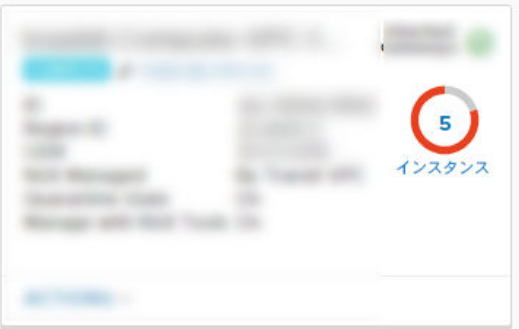
CSM では、わかりやすいアイコンを使用して、パブリック クラウド構造の状態と健全性が表示されます。


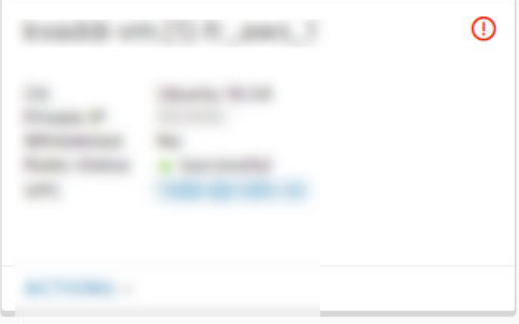
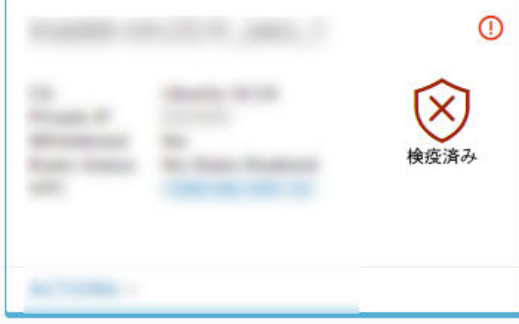
注： Native Cloud 強制モード では、検疫ポリシーが常に有効になり、すべての仮想マシンが常に NSX で管理されます。このモードには、NSX が管理する仮想マシンで検疫ポリシーが有効になっている状態のみが適用されます。

NSX 強制モード：検疫ポリシーが無効になり、VPC/VNet で仮想マシンが管理対象外になる可能性があります。このモードには、関連するすべての状態が適用されます。

CSM セクションとアイコン	説明
[VPC/VNet]	
	トランジット VPC/VNet
	コンピュート VPC/VNet

CSM セクションとアイコン	説明
	自己管理 VPC/VNet
	PCG が良好な状態の VPC/VNet
	PCG がエラー状態の VPC/VNet
	1つの PCG がエラー状態で、もう 1つが良好な状態の VPC/VNet

CSM セクションとアイコン	説明
	仮想マシンが NSX で管理されている VPC/VNet
	仮想マシンが管理対象外の VPC/VNet
	仮想マシンがエラー状態の VPC/VNet
	仮想マシンがパワーオフ状態の VPC/VNet
[インスタンス]	

CSM セクションとアイコン	説明
	エラーが発生していない NSX 管理対象仮想マシン
	エラーが発生し、検疫ポリシーが無効になっている NSX 管理対象仮想マシン
	エラーが発生し、検疫ポリシーが有効になっている NSX 管理対象仮想マシン

CSM セクションとアイコン	説明
	ホワイトリストに登録された管理対象外の仮想マシン
	隔離された管理対象外の仮想マシン

システム

[システム] にあるセクションは次のとおりです。

システム > 設定

これらの設定は、CSM をインストールするときに最初に構成されます。その後、編集することができます。

NSX Manager への CSM の追加

CSM アプライアンスと NSX Manager を接続して、これらのコンポーネントが相互通信できるようにする必要があります。

前提条件

- NSX Manager がインストールされていて、NSX Manager に管理者アカウントでログインするためのユーザー名とパスワードが必要です。
- CSM がインストール済みで、エンタープライズ管理者ロールが CSM に割り当てられている必要があります。

手順

- 1 ブラウザから CSM にログインします。
- 2 セットアップ ウィザードでプロンプトが表示されたら、[設定の開始] をクリックします。

3 [NSX Manager の認証情報] 画面で、次の詳細を入力します。

オプション	説明
NSX Manager のホスト名	NSX Manager の完全修飾ドメイン名 (FQDN) を入力します (分かっている場合)。NSX Manager の IP アドレスを入力することもできます。
管理者認証情報	NSX Manager のエンタープライズ管理者のユーザー名とパスワードを入力します。
NSX Manager のサムプリント	オプションで NSX Manager のサムプリント値を入力します。このフィールドを空白のままにすると、システムはサムプリントを識別し、次の画面に表示します。

- 4 (オプション) NSX Manager にサムプリント値を指定しなかった場合、または値が正しくない場合は、[サムプリントの確認] 画面が表示されます。チェック ボックスを選択し、システムによって検出されたサムプリントを受け入れます。

- 5 [接続] をクリックします。

注： セットアップ ウィザードでこの設定をしなかった場合、または関連付けられた NSX Manager を変更する場合は、CSM にログインし、[システム] - [設定] の順にクリックし、[関連付けられた NSX ノード] というパネルで [構成] をクリックします。

CSM は、NSX Manager のサムプリントを確認して、接続を確立します。

- 6 (オプション) プロキシ サーバを設定します。(オプション) プロキシ サーバの設定の手順を参照してください。

(オプション) プロキシ サーバの設定

信頼性の高い HTTP プロキシを介してインターネットに向かうすべての HTTP/HTTPS トラフィックをルーティングして監視する場合は、CSM で最大 5 台のプロキシ サーバを構成できます。

PCG および CSM からのすべてのパブリック クラウド通信は、選択したプロキシ サーバを介してルーティングされます。

PCG のプロキシ設定は CSM のプロキシ設定とは独立しています。PCG にプロキシ サーバを設定しないか、または異なるプロキシ サーバを設定することができます。

次のレベルの認証を選択できます。

- 認証情報ベースの認証。
- HTTPS インターセプトの証明書ベースの認証。
- 認証なし。

手順

- 1 [システム] - [設定] の順にクリックします。次に、[プロキシ サーバ] パネルの [設定] をクリックします。

注： これらの詳細は、CSM セットアップ ウィザードを使用する際にも指定できます。セットアップ ウィザードは CSM の初回インストール時に使用できます。

2 プロキシ サーバの設定画面で、次の詳細を入力します。

オプション	説明
デフォルト	このラジオ ボタンは、デフォルトのプロキシ サーバを指定する場合に使用します。
プロファイル名	プロキシ サーバ プロファイルの名前を指定します。このオプションは必須です。
プロキシ サーバ	プロキシ サーバの IP アドレスを入力します。このオプションは必須です。
ポート	プロキシ サーバのポートを入力します。このオプションは必須です。
認証	任意。追加認証を設定する場合は、このチェック ボックスを選択して、有効なユーザー名とパスワードを入力します。
ユーザー名	[認証] チェック ボックスを選択した場合は、必須です。
パスワード	[認証] チェック ボックスを選択した場合は、必須です。
証明書	任意。HTTPS インターセプトの認証証明書を指定する場合は、このチェックボックスを選択して、表示されたテキスト ボックスに証明書をコピーして貼り付けします。
プロキシなし	設定されているプロキシ サーバのいずれも使用しない場合は、このオプションを選択します。

システム > ユーティリティ

次のユーティリティを設定できます。

バックアップとリストア

CSM のバックアップとリストアを実行するときには、NSX Manager の場合と同じ手順を実行します。詳細については、[NSX Manager のバックアップとリストア](#)を参照してください。

サポート バンドル

[ダウンロード] をクリックして、CSM のサポート バンドルを取得します。これはトラブルシューティングに使用されます。詳細については、『NSX-T Data Center トラブルシューティング ガイド』を参照してください。

システム > ユーザー

ユーザーは、ロールベースのアクセス コントロール (RBAC) を使用して管理されます。

詳細については、[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](#)を参照してください。

NSX Cloud 検疫ポリシーを使用した脅威の検出

NSX Cloud の検疫ポリシー機能を使用すると、NSX が管理するワークロード仮想マシンに対する脅威を検出できます。

2 つの仮想マシン管理モードによって、検疫ポリシーの実装方法が異なります。

表 22-1. NSX 強制モード と Native Cloud 強制モード での検疫ポリシーの実装

検疫ポリシーに関連する設定	NSX 強制モード の場合	Native Cloud 強制モード の場合
デフォルトの状態	NSX Tools を使用して PCG を展開すると無効になります。これは、PCG の展開画面で有効にできます。 検疫ポリシーを有効または無効にする方法 を参照してください。	常に有効。無効にできません。
各モードに自動生成される固有のセキュリティ グループ	良好な状態の NSX 管理対象仮想マシンには vm-underlay-sg セキュリティ グループ が割り当てられます。	NSX Manager の分散ファイアウォール ポリシーと一致する NSX 管理対象ワークロード仮想マシンには、nsx-<NSX GUID> セキュリティ グループが作成され、適用されます
両方のモードに共通の自動生成されるパブリック クラウド セキュリティ グループ：	<p>[gw] セキュリティ グループは、AWS または Microsoft Azure のそれぞれの PCG インターフェイスに適用されます。</p> <ul style="list-style-type: none"> ■ gw-mgmt-sg ■ gw-uplink-sg ■ gw-vtep-sg <p>[vm] セキュリティ グループは、現在の状態と検疫ポリシーの設定（有効または無効）に応じて、NSX 管理対象の仮想マシンに適用されます。</p> <ul style="list-style-type: none"> ■ vm-quarantine-sg (Microsoft Azure)、default (AWS) <p>注： AWS で、default セキュリティ グループがすでに存在します。これは、NSX Cloud によって作成されません。</p>	

NSX 強制モード の一般的な推奨事項：

[既存環境]への展開を無効で開始する場合：検疫ポリシーは、デフォルトで無効です。パブリック クラウド環境に仮想マシンが設定済みの場合は、ワークロード仮想マシンのオンボーディングが完了するまで、検疫ポリシーを無効モードにします。これにより、既存の仮想マシンが自動的に隔離されないようにします。

[新規] 展開を有効で開始する場合：新規の展開では、検疫ポリシーを有効にして、仮想マシンの脅威の検出を NSX Cloud で管理することが推奨されます。

NSX 強制モード の検疫ポリシー

NSX 強制モード では、検疫ポリシーの有効化はオプションです。

検疫ポリシーを有効または無効にする方法

NSX 強制モード では、検疫ポリシーを 2 つの方法で有効にすることができます。

検疫ポリシーを最初に有効にするのは、トランジット VPC/VNet に PCG を展開する場合、またはコンピュータ VPC/VNet をトランジットにリンクする場合です。[関連付けられている VPC/VNet の検疫ポリシー] のスライダをデフォルトの [無効] から [有効] に移動します。『NSX-T Data Center インストール ガイド』の [PCG の展開] を参照してください。

この手順に従って、検疫ポリシーを後で有効にすることもできます。

前提条件

PCG への展開またはリンク後に検疫ポリシーを有効にする場合は、1つ以上のトランジットまたはコンピュータ VPC/VNet を NSX 強制モード でオンボーディングしておく必要があります。つまり、ワークロード仮想マシンの管理に NSX Tools を選択する必要があります。

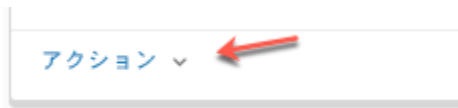
手順

1 CSM にログインし、パブリック クラウドに移動します。

- a AWS を使用している場合は、[クラウド] - [AWS] - [VPC] の順に移動します。中継 VPC またはコンピュータ VPC をクリックします。
- b Microsoft Azure を使用している場合は、[クラウド] - [Azure] - [VNet] の順に移動します。中継 VNet またはコンピュータ VNet をクリックします。

2 次のいずれかの方法を使用してオプションを有効にします。

- タイル ビューの場合は、[アクション] - [設定の編集] の順にクリックします。



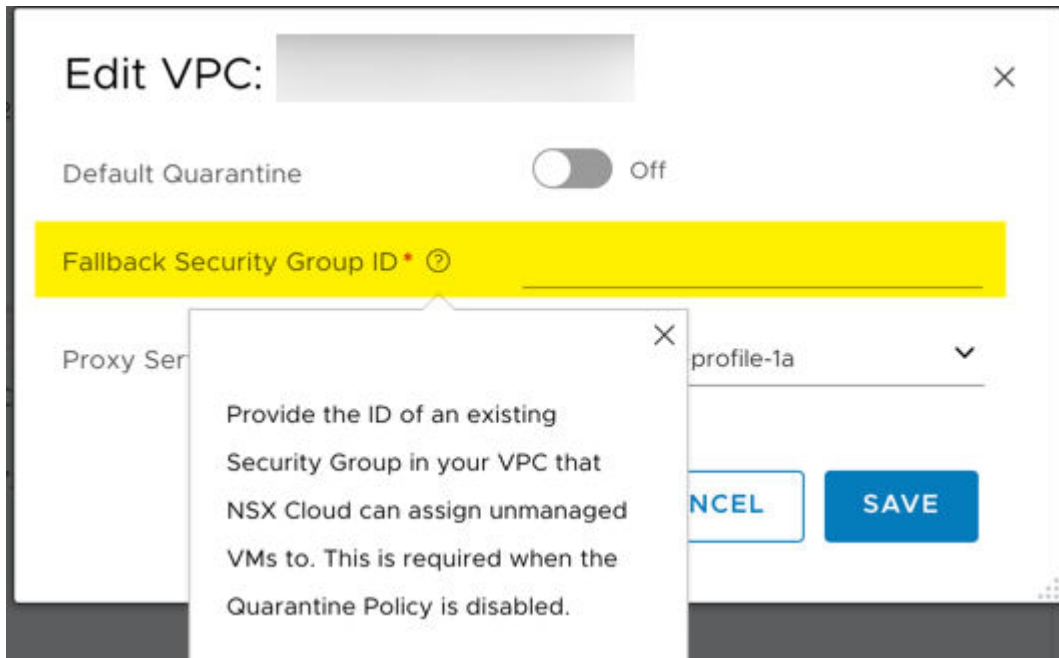
- グリッド ビューの場合は、VPC または VNet の横にあるチェック ボックスを選択し、[アクション] - [設定の編集] の順にクリックします。
- ◆ VPC または VNet のページの場合は、[アクション] アイコンをクリックして [設定の編集] に移動します。



3 [デフォルトの検疫] を有効または無効にします。

4 検疫ポリシーを無効にしている場合は、フォールバック セキュリティ グループを指定する必要があります。

注： フォールバック セキュリティ グループは、パブリック クラウド内の既存のユーザー定義セキュリティ グループである必要があります。NSX Cloud セキュリティ グループをフォールバック セキュリティ グループとして使用することはできません。



- この VPC または VNet 内のすべての管理対象外の仮想マシンは、検疫ポリシーを無効にすると、フォールバック セキュリティ グループが割り当てられます。
- すべての管理対象仮想マシンは、NSX Cloud によって割り当てられたセキュリティ グループを保持します。検疫ポリシーを無効にした後、初めてそれらの仮想マシンのタグ付けが解除され、管理対象外になったときに、それらにもフォールバック セキュリティ グループが割り当てられます。

5 [保存] をクリックします。

検疫ポリシーが無効時の影響

検疫ポリシーが無効になっている場合、NSX Cloud はタグ付けされていない仮想マシンのパブリック クラウド セキュリティ グループを管理しません。

ただし、パブリック クラウドで `nsx.network=default` とタグ付けされた仮想マシンの場合、NSX Cloud は仮想マシンの状態に応じて適切なセキュリティ グループを割り当てます。この動作は、検疫ポリシーが有効になっている場合と似ていますが、検疫セキュリティ グループ（Microsoft Azure の `vm-quarantine-sg` と AWS の `default`）のルールは制限が少なくなります。タグ付けされた仮想マシンのセキュリティ グループが手動で変更されても、NSX Cloud に割り当てられたセキュリティ グループに 2 分以内に戻されます。

注： NSX Cloud が NSX 管理の（タグ付けされた）仮想マシンにセキュリティ グループを割り当てないようにするには、CSM でこれらの仮想マシンをホワイトリストに登録します。[ホワイトリストへの仮想マシンの登録](#) を参照してください。

次の表は、検疫ポリシーが無効になっている場合に、NSX Cloud がワークロード仮想マシンのパブリック クラウド セキュリティ グループをどのように管理するのを示しています。

表 22-2. 検疫ポリシーが無効になっている場合の NSX Cloud によるパブリック クラウド セキュリティ グループの割り当て

パブリック クラウドで仮想マシンに <code>nsx.network=default</code> というタグが付いているか。	仮想マシンがホワイトリストに登録されているか。	検疫ポリシーが無効になっている場合の仮想マシンのパブリック クラウド セキュリティ グループと説明
タグ付き	ホワイトリストに登録されていない	<ul style="list-style-type: none"> ■ 仮想マシンに脅威がない場合：vm-underlay-sg ■ 仮想マシンに潜在的な脅威（注を参照）がある場合：Microsoft Azure では vm-quarantine-sg、AWS では default。 <p>注： ワークロード仮想マシンに <code>nsx.network=default</code> タグが適用されてから 90 秒以内に、パブリック クラウド セキュリティ グループの割り当てが開始します。NSX で管理する仮想マシンには、引き続き NSX Tools をインストールする必要があります。NSX Tools がインストールされるまで、タグ付けされたワークロード仮想マシンは隔離されます。</p>
タグ付けなし	ホワイトリストに登録されていない	NSX Cloud はタグ付けされていない仮想マシンにアクションを行わないため、既存のパブリック クラウド セキュリティ グループが維持されます。
タグ付き	ホワイトリスト登録済み	NSX Cloud は、ホワイトリストに登録された仮想マシンにアクションを実行しないため、既存のパブリック クラウド セキュリティ グループが保持されます。
タグ付けなし		

次の表は、この VPC/VNet のセキュリティ グループの割り当てを処理するために設定されたフォールバック セキュリティ グループにより、有効な検疫ポリシーが無効になった場合に、NSX Cloud が仮想マシンのパブリック クラウド セキュリティ グループをどのように管理するのかを示しています。

表 22-3. 検疫ポリシーが有効から無効になった場合の NSX Cloud によるパブリック クラウド セキュリティ グループの割り当て

パブリック クラウドで仮想マシンに <code>nsx.network=default</code> というタグが付いているか。	仮想マシンがホワイトリストに登録されているか。	検疫ポリシーが有効になっていたときの仮想マシンの既存のパブリック クラウド セキュリティ グループ	検疫ポリシーが無効になり、フォールバック セキュリティ グループが適用された後の仮想マシンのパブリック クラウド セキュリティ グループ
タグ付けなし	ホワイトリストに登録されていない	vm-quarantine-sg (Microsoft Azure)、default (AWS)	検疫ポリシーを無効にすると、タグ付けが解除され、NSX の管理対象外になるため、この仮想マシンにはフォールバック セキュリティ グループが割り当てられます。したがって、検疫ポリシーを無効にするときに、NSX Cloud はこの仮想マシンに割り当てられていたセキュリティ グループを取り消します。
タグ付き	ホワイトリストに登録されていない	vm-underlay-sg または vm-quarantine-sg (Microsoft Azure)、default (AWS)	隔離モードが有効か無効に関わらず、タグ付けされた仮想マシンのセキュリティ グループは維持されるため、NSX Cloud が割り当てたセキュリティ グループを維持します。
タグ付き	ホワイトリスト登録済み	既存のパブリック クラウド セキュリティ グループ	NSX Cloud は、ホワイトリストに登録された仮想マシンにアクションを実行しないため、既存のパブリック クラウド セキュリティ グループが保持されます。 注： NSX Cloud が割り当てたセキュリティ グループにホワイトリストの仮想マシンが存在する場合、指定したフォールバック セキュリティ グループに仮想マシンを手動で移動する必要があります。
タグ付けなし			

検疫ポリシーが有効時の影響

検疫ポリシーが有効になっている場合、NSX Cloud はこの VPC/VNet 内のすべてのワークロード仮想マシンのパブリック クラウド セキュリティ グループを管理します。

セキュリティ グループが手動で変更されても、NSX Cloud に割り当てられたセキュリティ グループに 2 分以内に戻されます。NSX Cloud が仮想マシンにセキュリティ グループを割り当てないようにするには、CSM でこれらの仮想マシンをホワイトリストに登録します。[ホワイトリストへの仮想マシンの登録](#) を参照してください。

注： 仮想マシンをホワイトリストから削除すると、仮想マシンは、NSX Cloud に割り当てられたセキュリティ グループに戻ります。

表 22-4. 検疫ポリシーが有効になっている場合の NSX Cloud によるパブリック クラウド セキュリティ グループの割り当て

パブリック クラウドで仮想マシンに <i>nsx.network=default</i> というタグが付いているか。	仮想マシンがホワイトリストに登録されているか。	検疫ポリシーが有効になっている場合の仮想マシンのパブリック クラウド セキュリティ グループと説明
タグ付き	ホワイトリストに登録されていない	<ul style="list-style-type: none"> ■ 仮想マシンに脅威がない場合：vm-underlay-sg ■ 仮想マシンに潜在的な脅威（注を参照）がある場合：Microsoft Azure では vm-quarantine-sg、AWS では default。 <p>注： ワークロード仮想マシンに <i>nsx.network=default</i> タグが適用されてから 90 秒以内に、パブリック クラウド セキュリティ グループの割り当てが開始します。NSX で管理する仮想マシンには、引き続き NSX Tools をインストールする必要があります。NSX Tools がインストールされるまで、タグ付けされたワークロード仮想マシンは隔離されます。</p>
タグ付けなし	ホワイトリストに登録されていない	vm-quarantine-sg (Microsoft Azure)、default (AWS)タグ付けの仮想マシンは管理対象外と見なされ、NSX Cloud によって隔離されます。
タグ付き	ホワイトリスト登録済み	NSX Cloud は、ホワイトリストに登録された仮想マシンにアクションを実行しないため、既存のパブリック クラウド セキュリティ グループが保持されます。
タグ付けなし		

次の表は、無効だった検疫ポリシーを有効にした場合にセキュリティ グループの割り当てが受ける影響を示したものです。

表 22-5. 検疫ポリシーが無効から有効になった場合の NSX Cloud によるパブリック クラウド セキュリティ グループの割り当て

パブリック クラウドで仮想マシンに <i>nsx.network=default</i> というタグが付いているか。	仮想マシンがホワイトリストに登録されているか。	検疫ポリシーが無効になっていたときの仮想マシンの既存のパブリック クラウド セキュリティ グループ	検疫ポリシーが有効になった後の仮想マシンのパブリック クラウド セキュリティ グループ
タグ付けなし	ホワイトリストに登録されていない	既存のパブリック クラウド セキュリティ グループ	vm-quarantine-sg (Microsoft Azure)、default (AWS)
タグ付き	ホワイトリストに登録されていない	vm-underlay-sg または vm-quarantine-sg (Microsoft Azure)、default (AWS)	隔離モードが有効か無効かに関わらず、タグ付けされた仮想マシンのセキュリティ グループは維持されるため、NSX Cloud が割り当てたセキュリティ グループを維持します。

表 22-5. 検疫ポリシーが無効から有効になった場合の NSX Cloud によるパブリック クラウド セキュリティ グループの割り当て（続き）

パブリック クラウドで仮想マシンに <i>nsx.network=default</i> というタグが付いているか。	仮想マシンがホワイトリストに登録されているか。	検疫ポリシーが無効になっていたときの仮想マシンの既存のパブリッククラウドセキュリティグループ	検疫ポリシーが有効になった後の仮想マシンのパブリッククラウドセキュリティグループ
タグ付き	ホワイトリスト登録済み	既存のパブリッククラウドセキュリティグループ。	NSX Cloud は、ホワイトリストに登録された仮想マシンにアクションを実行しないため、既存のパブリッククラウドセキュリティグループが保持されます。
タグ付けなし			

Native Cloud 強制モード の検疫ポリシー

Native Cloud 強制モード では、検疫ポリシーが常に有効になっています。

表 22-6. Native Cloud 強制モード でのパブリック クラウド セキュリティ グループの割り当て

仮想マシンは、有効な NSX-T セキュリティ ポリシーの一部になっているか。	仮想マシンがホワイトリストに登録されているか。	仮想マシンのパブリッククラウドセキュリティグループと説明
仮想マシンは有効な NSX-T セキュリティ ポリシーに一致している	ホワイトリストに登録されていない	NSX Cloud に作成されたパブリッククラウドセキュリティグループ (<code>nsx-{NSX-GUID}</code>)。これは、NSX-T セキュリティ ポリシーのパブリッククラウドセキュリティグループに対応しています。
仮想マシンに有効な NSX-T ファイアウォール ポリシーはない	ホワイトリストに登録されていない	vm-quarantine-sg (Microsoft Azure)、default (AWS)。これは、NSX Cloud の脅威検出動作です。Native Cloud 強制モード では、NSX Cloud が作成するセキュリティグループ (Microsoft Azure の vm-quarantine-sg または AWS の default) は、デフォルトのパブリッククラウドセキュリティポリシーに類似しています。 注： CSM では、仮想マシンがエラー状態になります。
仮想マシンには有効な NSX-T セキュリティ ポリシーがある	ホワイトリスト登録済み	NSX Cloud は、ホワイトリストに登録された仮想マシンにアクションを実行しないため、既存のパブリッククラウドセキュリティグループが保持されます。
仮想マシンに有効な NSX-T セキュリティ ポリシーはない		

ホワイトリストへの仮想マシンの登録

ホワイトリスト登録は、パブリッククラウド インベントリ内のすべてのワークロード仮想マシンで CSM から使用可能なオプションです。

ホワイトリスト登録は、両方の仮想マシン管理モード（NSX 強制モード と Native Cloud 強制モード）の両方で動作します。

仮想マシンをホワイトリストに登録する理由

- NSX 強制モード：検疫ポリシーを有効にしている、仮想マシン上の既存のアプリケーションで特定の DFW ポリシーを確認する必要がある場合、NSX Cloud でオンボーディングする前に、このような仮想マシンをホワイトリストに登録します。

■ NSX 強制モード または Native Cloud 強制モード：

- エラーが発生している仮想マシンにアクセスしてエラーを解決する場合は、仮想マシンを隔離状態から移動して必要に応じてデバッグ ツールを使用できるように、仮想マシンをホワイトリストに登録します。
- パブリック クラウド インベントリ内で、NSX-T で管理する必要のない仮想マシンをホワイトリストに登録します（DNS フォワーダー、プロキシ サーバなど）。

ホワイトリストへの仮想マシンの登録方法とホワイトリストからの削除方法

次の手順に従って、ホワイトリストで仮想マシンの追加または削除を行います。

前提条件

1 つ以上のパブリック クラウド アカウントが CSM に追加されている必要があります。

手順

- 1 エンタープライズの管理者アカウントを使用して CSM にログインし、パブリック クラウド アカウントに移動します。
 - a AWS を使用している場合は、[クラウド] - [AWS] - [VPC] - [インスタンス] の順に移動します。
 - b Microsoft Azure を使用している場合は、[クラウド] - [Azure] - [VNet] - [インスタンス] の順に移動します。
- 2 タイル モードの場合は、インスタンス ビューの右隅にあるモード セレクタをクリックして、グリッド モードに切り替えます。
- 3 ホワイトリストに追加またはホワイトリストから削除する仮想マシン（インスタンス）を選択します。
- 4 [アクション] をクリックし、[ホワイトリストに追加] または [ホワイトリストから削除] を選択します。
- 5 [アカウント] タブに戻り、アカウント タイルを選択して、[アクション] - [アカウントの再同期] の順にクリックします。

結果

ホワイトリストに追加された仮想マシンは、追加前に割り当てられたセキュリティ グループに残ります。必要に応じて、仮想マシンに別のセキュリティ グループを適用できるようになりました。NSX Cloud は、検疫ポリシーの状態に関係なく、ホワイトリストされた仮想マシンを無視します。

Native Cloud 強制モード でホワイトリストから仮想マシンを削除するか、NSX 強制モード で NSX 管理対象の仮想マシンをホワイトリストから削除すると、NSX Cloud は仮想マシンの状態に応じて、セキュリティ グループを割り当てます。

NSX 強制モード

NSX 強制モード では、NSX Tools を使用している場合、最初に仮想マシンをパブリック クラウドにタグ付けし、それらの仮想マシンに NSX Tools をインストールします。その後、NSX-T Data Center を使用して、これらの仮想マシンを管理する必要があります。

現在サポートされているワークロード仮想マシンのオペレーティング システム

これは、現在 NSX 強制モード のワークロード仮想マシンに対して NSX Cloud でサポートされているオペレーティング システムのリストです。

現在、次のオペレーティング システムがサポートされています。

注： 例外については、NSX-T Data Center リリース ノートの「NSX Cloud の既知の問題」セクションを参照してください。サポートされているオペレーティングシステムの場合、標準の Linux カーネル バージョンを使用していることを前提としています。ソースが変更されたアップストリームの Linux カーネルなど、カスタム カーネルを含むパブリック クラウド マーケットプレイス イメージはサポートされません。

- Red Hat Enterprise Linux (RHEL) 7.2、7.3、7.4、7.5、7.6
- CentOS 7.2、7.3、7.4、7.5、7.6

注： RHEL と CentOS の RHEL Extended Update Support (EUS) カーネルはサポートされていません。

注： NSX Cloud でサポートされる CentOS マーケットプレイス イメージは、想定されるマイナー カーネル バージョンと一致する配布バージョンのもののみです。たとえば、配布バージョンと対応するカーネル バージョンは次のように想定されます。

RHEL バージョン	カーネル バージョン
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

- Ubuntu 14.04、16.04、18.04
- Microsoft Windows Server 2016 - サービス ベースのリリース、デスクトップ エクスペリエンス (1709、1803、1809)
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 バージョン 1809、1803、1709 (現在の NSX Cloud リリースでは Microsoft Azure のみでサポートされます)

NSX 強制モード の仮想マシンのオンボーディング

NSX 強制モード で、パブリック クラウドからワークロード仮想マシンをオンボーディングおよび管理するのに必要な手順の概要については、このワークフローを参照してください。

表 22-7. NSX Cloud へのワークロード仮想マシンのオンボーディングの Day-N ワークフロー

タスク	方法
<input type="checkbox"/> キー値 <code>nsx.network=default</code> をワークロード仮想マシンにタグ付けします。	ワークロード仮想マシンのタグ付けについては、パブリック クラウドのドキュメントに記載された手順を実行してください。
<input type="checkbox"/> Windows および Linux のワークロード仮想マシンに NSX Tools をインストールします。 注： CSM で、Microsoft Azure VNet に [NSX Tools の自動インストール] が有効になっている場合、NSX Tools が自動的にインストールされます。	NSX Tools のインストール を参照してください。
<input type="checkbox"/> (オプション) CSM で、NSX で管理するすべての仮想マシンをホワイトリストから削除します。 注： ホワイトリスト登録は、CSM にパブリック クラウド インベントリを追加する際の最初のワークフローで推奨される手動プロセスです。ホワイトリストに追加しなかった場合は、ホワイトリストから仮想マシンを削除する必要はありません。	ホワイトリストへの仮想マシンの登録方法とホワイトリストからの削除方法 を参照してください。

パブリック クラウド内の仮想マシンへのタグの適用

NSX-T Data Center を使用して管理する仮想マシンに `[nsx.network=default]` タグを適用します。

手順

- 1 パブリック クラウド アカウントにログインして、NSX-T Data Center でワークロード仮想マシンを管理する VPC または VNet に移動します。
- 2 NSX-T Data Center を使用して管理する仮想マシンを選択します。
- 3 以下の仮想マシンのタグの詳細を追加し、変更内容を保存します。

```
Key: nsx.network
Value: default
```

注： このタグを仮想マシン レベルで適用します。

結果

`nsx.network=default` タグをワークロード仮想マシンに適用した VPC/VNet がすでにオンボーディングされている可能性があります。タグを適用した後に、これらの VPC/VNet をオンボーディングすることもできます。VPC/VNet のオンボーディングが成功すると、ワークロード仮想マシンが NSX の管理対象と見なされます。

次のステップ

これらの仮想マシンに NSX Tools をインストールします。[NSX Tools のインストール](#) を参照してください。

Microsoft Azure を使用している場合、タグ付けされた仮想マシンに NSX Tools を自動インストールするオプションがあります。詳細については、[NSX Tools の自動インストール](#)を参照してください。

NSX Tools のインストール

ワークロード仮想マシンへの NSX Tools のインストール

NSX Tools のインストールに使用できるオプションがいくつかあります。

- 個別のワークロード仮想マシンに NSX Tools をダウンロードしてインストールします。Linux と Windows の仮想マシンには、いくつかのバリエーションがあります。
- パブリック クラウドでサポートされる方法を使用して、NSX Tools がインストールされたレプリケート可能なイメージを使用します。たとえば、AWS の場合は AMI を作成し、Microsoft Azure の場合は管理対象イメージを作成します。
- AWS の場合：仮想マシンを起動するときに、[ユーザー データ] に NSX Tools のダウンロード場所とインストール コマンドを指定します。
- Microsoft Azure の場合：Microsoft Azure VNet に PCG を展開するとき、またはトランジット VNet にリンクするときに NSX Tools の自動インストールを有効にします。あるいは、トランジット/コンピューティング VNet の設定を編集して自動インストールを有効にします。

注： NSX Tools をインストールするワークロード仮想マシンがホワイトリストに追加されている場合は、その仮想マシンに割り当てたセキュリティ グループで次のポートが開いていることを確認します。

- 受信 UDP 6081：オーバーレイ データ パケット用。これは、(アクティブ/スタンバイ) PCG の VTEP IP アドレス (eth1 インターフェイス) に許可する必要があります。
- 送信 TCP 5555：制御パケット用。これは、(アクティブ/スタンバイ) PCG の管理 IP アドレス (eth0 インターフェイス) に許可する必要があります。
- TCP 8080：PCG の管理 IP アドレスでのインストール/アップグレード用。
- TCP 80：NSX Tools のインストール中にサードパーティの依存関係のダウンロードに使用。
- UDP 67、68：DHCP パケット用。
- UDP 53：DNS 解決用。

Linux 仮想マシンへの NSX Tools

Linux ワークロード仮想マシンに NSX Tools をインストールするには、次の手順に従います。

現在サポートされている Linux ディストリビューションについては、[現在サポートされているワークロード仮想マシンのオペレーティング システム](#) の一覧を参照してください。

注： このスクリプトのチェックサムを確認するには、[VMware ダウンロード] - [ドライバ & ツール] - [NSX Cloud スクリプト] の順に移動します。

前提条件

NSX Tools のインストール スクリプトを実行するには、次のコマンドが必要です。

- [wget]
- [nslookup]

■ [dmidecode]

手順

- 1 CSM にログインし、パブリック クラウドに移動します。

- a AWS を使用している場合は、[クラウド] - [AWS] - [VPC] の順に移動します。中継 VPC またはコンピュータ VPC をクリックします。
- b Microsoft Azure を使用している場合は、[クラウド] - [Azure] - [VNet] の順に移動します。1 つまたはペアの PCG が展開され、実行されている VNet をクリックします。

[注]: トランジット VPC/VNet では、1 つまたはペアの PCG が展開され、実行されます。コンピュータ VPC/VNet は中継 VPC/VNet にリンクされたもので、そこに展開されている PCG インスタンスを使用できます。

- 2 画面の [NSX Tools のダウンロードとインストール] セクションから、[Linux] の [ダウンロード場所] と [インストール コマンド] を書き留めます。

注: VNet の場合、インストール コマンドの DNS サフィックスは、PCG の展開時に選択した DNS 設定と一致するように動的に生成されます。トランジット VNet では、`-dnsServer <dns-server-ip>` パラメータはオプションです。コンピュータ VNet では、DNS フォワーダの IP アドレスを指定してこのコマンドを完了する必要があります。

- 3 スーパー ユーザー権限で Linux ワークロード仮想マシンにログインします。

- 4 `wget` または相当するコマンドを使用して、CSM で書き留めた [ダウンロードの場所] から Linux 仮想マシンにインストール スクリプトをダウンロードします。`wget` コマンドを実行したディレクトリに、インストール スクリプトがダウンロードされます。

注: このスクリプトのチェックサムを確認するには、[VMware ダウンロード] - [ドライバ & ツール] - [NSX Cloud スクリプト] の順に移動します。

- 5 必要に応じて、インストール スクリプトの権限を変更して実行可能にし、実行します。

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

[注]: Red Hat Enterprise Linux とその派生製品で、SELinux はサポートされません。NSX Tools をインストールするには、SELinux を無効にします。

- 6 NSX Tools のインストールが開始すると、Linux 仮想マシンとの接続が失われます。次のようなメッセージが画面に表示されます: `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` オンボーディング プロセスを完了するには、仮想マシンに再度ログインします。

結果

NSX Tools がワークロード仮想マシンにインストールされます。

注：

- NSX Tools が正常にインストールされた後、ポート 8888 はワークロード仮想マシンでは開いていると表示されますが、アンダーレイ モードの仮想マシンではブロックされていると表示されます。このポートは、高度なトラブルシューティングが必要な場合にのみ使用してください。 ジャンプホストがアクセスするワークロード仮想マシンと同じ VPC にある場合は、ジャンプホストを使用してポート 8888 経由でワークロード仮想マシンにアクセスできます。
 - スクリプトは、デフォルトのインターフェイスとして eth0 を使用します。
-

次のステップ**NSX 強制モード での仮想マシンの管理****Windows 仮想マシンへの NSX Tools**

次の手順に従って、Windows ワークロード仮想マシンに NSX Tools をインストールします。

現在サポートされている Microsoft Windows のバージョンについては、[現在サポートされているワークロード仮想マシンのオペレーティング システム](#) の一覧を参照してください。

注： このスクリプトのチェックサムを確認するには、[VMware ダウンロード] - [ドライバ & ツール] - [NSX Cloud スクリプト] の順に移動します。

手順

- 1 CSM にログインし、パブリック クラウドに移動します。
 - a AWS を使用している場合は、[クラウド] - [AWS] - [VPC] の順に移動します。トランジットまたはコンピュート VPC をクリックします。
 - b Microsoft Azure を使用している場合は、[クラウド] - [Azure] - [VNet] の順に移動します。1 つまたはペアの PCG が展開され、実行されている VNet をクリックします。

[注]: トランジット VPC/VNet では、1 つまたはペアの PCG が展開され、実行されます。コンピュート VPC/VNet では、トランジットにリンクされた VPC/VNet で、PCG を展開して使用できます。
- 2 画面の [NSX Tools のダウンロードとインストール] セクションから、[Windows] の [ダウンロード場所] と [インストール コマンド] を書き留めます。

注： VNet の場合、インストール コマンドの DNS サフィックスは、PCG の展開時に選択した DNS 設定と一致するように動的に生成されます。トランジット VNet では、-dnsServer <dns-server-ip> パラメータはオプションです。コンピュート VNet では、DNS フォワーダの IP アドレスを指定してこのコマンドを完了する必要があります。

- 3 管理者として Windows ワークロード仮想マシンに接続します。

- CSM で書き留めた [ダウンロードの場所] から Windows 仮想マシンにインストール スクリプトをダウンロードします。Internet Explorer などの任意のブラウザを使用して、スクリプトをダウンロードできます。C:\Downloads などのブラウザのデフォルトのダウンロード ディレクトリにダウンロードされます。

注： このスクリプトのチェックサムを確認するには、[VMware ダウンロード] - [ドライバ & ツール] - [NSX Cloud スクリプト] の順に移動します。

[注]：

- PowerShell プロンプトを開き、ダウンロードしたスクリプトが格納されたディレクトリに移動します。
- CSM で書き留めた [インストール コマンド] を使用してダウンロードしたスクリプトを実行します。

次はその例です。

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

注： ファイルの引数に指定するディレクトリと同じディレクトリにいる場合、または PowerShell スクリプトが指定するディレクトリにある場合を除いて、ファイルの引数にはフル パスを指定する必要があります。たとえば、スクリプトをダウンロードする場所が C:\Downloads で、そのディレクトリに移動していない場合は、スクリプトに含める場所を次のように指定する必要があります。powershell -file 'C:\Downloads\nsx_install.ps1' ...

- スクリプトを実行し、完了すると、NSX Tools が正常にインストールされたかどうかを示すメッセージが表示されます。

注： スクリプトは、プライマリ ネットワーク インターフェイスをデフォルトとして認識します。

次のステップ

NSX 強制モード での仮想マシンの管理

複製可能なイメージの生成

NSX Agent がインストールされた仮想マシンの AWS で AMI を生成するか、Microsoft Azure で管理対象イメージを生成することができます。

この機能を使用すると、エージェントが設定され、実行されている複数の仮想マシンを起動できます。

NSX Agent がインストールされている仮想マシンの AMI/管理対象イメージ（このトピックの残りのイメージ）を生成する方法は、2 つあります。

- [未設定の NSX Agent を使用してイメージを生成する]：-noStart オプションを使用して NSX Agent がインストールされながらも設定されていない仮想マシンから、イメージを生成できます。このオプションを使用すると、NSX Agent パッケージを取得してインストールできますが、NSX Services は起動されません。また、証明書の生成などの NSX の設定は行われません。
- [NSX Agent の既存の設定を削除した後にイメージを生成する]：NSX の管理対象仮想マシンから設定を削除して、その仮想マシンをイメージの生成に使用することができます。

未設定の NSX Agent を使用した AMI の生成

NSX Agent がインストールされていて、まだ設定されていない仮想マシンに対して、AMI を生成することができます。

-noStart オプションを使用して、NSX Agent がインストールされている仮想マシンからイメージを生成するには、以下の操作を実行します。

手順

- 1 CSM から NSX Agent のインストール コマンドをコピーして、貼り付けます。[NSX Tools のインストール](#)にある手順を参照してください。

- a 次のように Windows のコマンドを編集します。

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <> -noStart true
```

- b 次のように Linux のコマンドを編集します。

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 パブリック クラウド内のこの仮想マシンに移動して、イメージを作成します。

既存の NSX Agent の設定を削除した後のイメージの生成

NSX Agent が設定された仮想マシンのイメージを生成できます。

既存の NSX 管理対象仮想マシンから設定を削除して、イメージを生成するために使用するには、次の操作を実行します。

手順

- 1 Windows または Linux 仮想マシンから NSX Agent の設定を削除します。

- a ジャンプホストを使用して可能であれば、ワークロード仮想マシンにログインします。
- b NSX-T CLI を開きます。

```
sudo nsxcli
```

- c 次のコマンドを入力します。

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

- 2 パブリック クラウド内でこの仮想マシンを検索し、イメージを作成します。

NSX Tools の自動インストール

現在、Microsoft Azure でのみサポートされます。

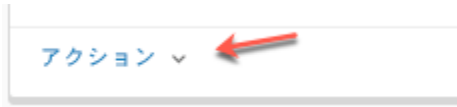
Microsoft Azure では、以下の条件が満たされている場合、NSX Tools が自動的にインストールされます。

- NSX Cloud に追加された VNet 上の仮想マシンに Azure 仮想マシンの拡張機能がインストールされている。
詳細については、[仮想マシンの拡張機能に関する Microsoft Azure のドキュメント](#)を参照してください。

- Microsoft Azure で仮想マシンに適用されるセキュリティ グループで、NSX Tools のインストールを許可する必要があります。検疫ポリシーが有効になっている場合、インストール前に CSM の仮想マシンをホワイトリストに追加し、インストール後にホワイトリストから削除することができます。
- 仮想マシンがキー `nsx.network` と値 `default` を使用してタグ付けされている。

この機能を有効にするには、次の手順を実行します。

- 1 [クラウド] - [Azure] - [VNet] の順に移動します。
- 2 CSM を自動的にインストールする仮想マシンを含む VNet を選択します。
- 3 次のいずれかの方法を使用してオプションを有効にします。
 - タイル ビューの場合は、[アクション] - [設定の編集] の順にクリックします。



- グリッド ビューの場合は、VNet の横にあるチェック ボックスを選択し、[アクション] - [設定の編集] の順にクリックします。



- [VNet] タブの場合は、[アクション] アイコンをクリックして [設定の編集] に移動します。



- 4 [NSX Tools の自動インストール] の横にあるスライダを ON の位置に移動します。

注： NSX Tools のインストールが失敗した場合は、次の操作を行います。

- 1 Microsoft Azure ポータルにログインし、NSX Tools のインストールが失敗した仮想マシンに移動します。
 - 2 仮想マシンの拡張機能に移動し、 `VMwareNsxAgentInstallCustomScriptExtension` という名前の拡張機能をアンインストールします。
 - 3 この仮想マシンから `nsx.network=default` タグを削除します。
 - 4 この仮想マシンに再度 `nsx.network=default` タグを追加します。
- 3 分以内に NSX Tools がこの仮想マシンにインストールされます。
-

AWS でのユーザー データを使用した NSX Tools のインストール

AWS VPC で新しいワークロード仮想マシンを起動するときに、[ユーザー データ] フィールドに NSX Tools のダウンロードとインストール手順を指定して、NSX Tools をインストールできます。

CSM から NSX Tools のダウンロードとインストールの手順をコピーし、新しいワークロード仮想マシンの起動時にユーザー データに貼り付けます。

手順

- 1 AWS コンソールにログインして、新しいワークロード仮想マシンを起動するプロセスを開始します。

2 別のブラウザ ウィンドウで、CSM にログインします。

- a [クラウド] - [AWS] - [VPC] の順に移動します。

注： トランジット VPC/VNet では、1 つまたはペアの PCG が展開され、実行されます。コンピュート VPC/VNet では、トランジットにリンクされた VPC/VNet で、PCG を展開して使用できます。

- b トランジットまたはコンピュート VPC をクリックします。
- c ワークロード仮想マシンで使用している OS に応じて、画面の [NSX Tools のダウンロードとインストール] のセクションから、[Linux] または [Windows] の下にある [ダウンロード場所] と [インストール コマンド] を情報をコピーします。

3 AWS で新しいワークロード仮想マシン インスタンスを起動する手順で、ダウンロード場所とインストール コマンドを [詳細詳細] セクションの [ユーザー データ] に [テキスト] として貼り付けます。

結果

ワークロード仮想マシンが起動し、NSX Tools が自動的にインストールされます。

NSX Tools のアンインストール

これらの OS 固有のコマンドを使用して、NSX Tools をアンインストールします。

Windows 仮想マシンからの NSX Tools のアンインストール

注： インストール スクリプトで利用可能なその他のオプションを確認するには、-help を使用します。

- 1 RDP を使用して仮想マシンにリモート ログインします。
- 2 インストール スクリプトを実行し、アンインストール オプションを選択します。

```
\nsx_install.ps1 -operation uninstall
```

Linux 仮想マシンからの NSX Tools のアンインストール

注： インストール スクリプトで利用可能なその他のオプションを確認するには、--help を使用します。

- 1 SSH を使用して仮想マシンにリモート ログインします。
- 2 インストール スクリプトを実行し、アンインストール オプションを選択します。

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

オンボーディング後の NSX 強制モード でのセキュリティ グループ

次のセキュリティ グループの設定は自動的行われます。

検疫ポリシーが有効な場合：

- 良好な状態の NSX 管理対象仮想マシンは、パブリック クラウドの vm-underlay-sg に移動します。

- 管理対象外の仮想マシンまたはエラーのある NSX 管理対象仮想マシンは、default セキュリティ グループ（AWS の場合）または vm-quarantine-sg ネットワーク セキュリティ グループ（Microsoft Azure の場合）に移動します。
- ホワイトリストに登録された仮想マシンは影響を受けません。

検疫ポリシーが無効な場合：

- 良好な状態の NSX 管理対象仮想マシンは、パブリック クラウドの vm-underlay-sg に移動します。
- エラーのある NSX 管理対象仮想マシンは、default セキュリティ グループ（AWS の場合）または vm-quarantine-sg ネットワーク セキュリティ グループ（Microsoft Azure の場合）に移動します。
- 管理対象外の仮想マシンとホワイトリストに登録された仮想マシンは影響を受けません。

NSX 強制モード での仮想マシンの管理

次の手順に従って、正常にオンボーディングされた NSX 強制モード の仮想マシンの管理を開始します。

表 22-8. NSX 強制モード で NSX 管理のワークロード仮想マシンのマイクロセグメンテーション ワークフロー

タスク	方法
 ワークロード仮想マシンに受信アクセスを許可するには、必要に応じて分散ファイアウォール (DFW) ルールを作成します。	NSX で管理されたワークロード仮想マシンの NSX 強制モード でのデフォルトの接続方法 を参照してください。
 パブリック クラウド タグまたは NSX-T Data Center タグを使用してワークロード仮想マシンをグループ化し、マイクロセグメンテーションを設定します。	NSX 強制モード でのワークロード仮想マシンのマイクロセグメンテーションの設定 を参照してください。 詳細については、 NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化 も参照してください。

NSX で管理されたワークロード仮想マシンの NSX 強制モード でのデフォルトの接続方法

トランジット VPC/VNet に PCG を展開するか、コンピュート VPC/VNet をトランジットにリンクすると、NSX Cloud は NSX で管理されたワークロード仮想マシンにデフォルトのセキュリティ ポリシーと DFW ルールを作成します。

2 つのステートレス ルールは DHCP アクセス用です。ワークロード仮想マシンへのアクセスには影響しません。

2 つのステートフル ルールは、次のとおりです。

ポリシー cloud-stateful-cloud-<VPC/VNet ID> に基づいて NSX Cloud によって作成される DFW ルール	プロパティ
[cloud-<VPC/VNet ID>-managed]	同じ VPC/VNet 内の仮想マシンへのアクセスを許可します。
[cloud-<VPC/VNet ID>-inbound]	VPC/VNet 外の任意の場所から NSX の管理対象仮想マシンへのアクセスをブロックします。

注： デフォルト ルールは編集しないでください。

既存の受信ルールのコピーを作成し、送信元と宛先を調整して、[許可] に設定します。デフォルトの [却下] ルールの上に [許可] ルールを配置します。新しいポリシーとルールを追加することもできます。手順については、[分散ファイアウォールの追加](#) を参照してください。

NSX 強制モード でのワークロード仮想マシンのマイクロセグメンテーションの設定

管理対象のワークロード仮想マシンに、マイクロセグメンテーションを設定できます。

NSX 管理対象のワークロード仮想マシンに分散ファイアウォール ルールを適用するには、次の手順を実行します。

- 1 仮想マシン名、タグ、またはその他のメンバーシップ基準（[web]、[app]、[DB] 階層など）を使用してグループを作成します。手順については、[グループの追加](#)を参照してください。

注： 次のタグのいずれかをメンバーシップ基準に使用できます。詳細については、[NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化](#)を参照してください。

- システム定義のタグ
- NSX Cloud によって検出された、Virtual Private Cloud (VPC) または VNet のタグ
- 独自のカスタム タグ

注： 分散ファイアウォール ルールは、仮想マシンに割り当てられたタグによって異なります。これらのタグは、適切なパブリック クラウド権限を持つユーザーであれば、誰でも変更することができます。このため、NSX-T Data Center では、このようなユーザーが信頼でき、仮想マシンに常に正しいタグが設定されていることをパブリック クラウドのネットワーク管理者が確認していることを前提としています。

- 2 East-West 分散ファイアウォール ポリシーとルールを作成し、作成したグループに適用します。[分散ファイアウォールの追加](#)を参照してください。

このマイクロセグメンテーションが有効になるのは、CSM でインベントリが手動で再同期されたとき、または、CSM がパブリック クラウドから変更内容を取得してから約 3 分以内です。

Native Cloud 強制モード

Native Cloud 強制モード では、すべてのワークロード仮想マシンが自動的に NSX で管理されます。ここで説明するワークフローに従い、NSX-T Data Center を使用してこれらの仮想マシンを管理してください。

注： Native Cloud 強制モード のワークロード仮想マシンでは、すべてのオペレーティング システムがサポートされています。

Native Cloud 強制モード での仮想マシンの管理

Native Cloud 強制モード では、NSX Cloud は NSX-T Data Center グループと分散ファイアウォール ルールを使用して、Microsoft Azure および AWS のセキュリティ グループに対応するアプリケーション セキュリティ グループとネットワーク セキュリティ グループを作成します。

Native Cloud 強制モード で VPC/VNet にオンボーディングされたワークロード仮想マシンは、すべて NSX で管理されます。

次のワークフローに従います。

表 22-9. Native Cloud 強制モード のワークロード仮想マシンのマイクロセグメンテーション ワークフロー

タスク	方法
<input type="checkbox"/> パブリック クラウドからワークロード仮想マシンを含めるには、NSX Manager に 1 つ以上のグループを作成します。	<p>詳細については、Native Cloud 強制モード でのワークロード仮想マシンのマイクロセグメンテーションの設定</p> <p>NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化 も参照してください。</p>
<input type="checkbox"/> NSX Manager で、パブリック クラウド ワークロード仮想マシン用に作成したグループに適用される 1 つ以上のセキュリティ ポリシーを作成します。	
<input type="checkbox"/> NSX-T セキュリティ ポリシーで管理する場合は、ワークロード仮想マシンを CSM のホワイトリストから削除します。	
<input type="checkbox"/> CSM で、パブリック クラウド アカウントを再同期します。	
<input type="checkbox"/> エラーが発生した場合は、VPC/VNet から CSM の詳細ビューに切り替え、セキュリティ ポリシーのトラブルシューティングを行います。	<p>詳細については、現在の制限事項と一般的なエラー</p>

Native Cloud 強制モード でのワークロード仮想マシンのマイクロセグメンテーションの設定

このワークフローでは、NSX Manager で Native Cloud 強制モード のワークロード仮想マシンにセキュリティポリシーを設定します。ワークロード仮想マシンには NSX Tools をインストールしません。

前提条件

Native Cloud 強制モード にトランジットまたはコンピュート VPC/VNet が必要です。

手順

- 1 NSX Manager で、ワークロード仮想マシンのグループを編集または作成します。たとえば、web、app、db で始まる仮想マシンを使用して 3 つのグループを作成します。手順については、[グループの追加](#)を参照してください。また、パブリック クラウド タグを使用してワークロード仮想マシンのグループを作成する方法については、[NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化](#) を参照してください。

基準に一致するワークロード仮想マシンがグループに追加されます。グループ基準に一致しない仮想マシンは、default セキュリティ グループ（AWS の場合）または vm-quarantine-sg ネットワーク セキュリティグループ（Microsoft Azure の場合）に配置されます。

注： NSX Cloud によって自動作成されたグループは使用できません。

注： 分散ファイアウォール ルールは、仮想マシンに割り当てられたタグによって異なります。これらのタグは、適切なパブリック クラウド権限を持つユーザーであれば、誰でも変更することができます。このため、NSX-T Data Center では、このようなユーザーが信頼でき、仮想マシンに常に正しいタグが設定されていることをパブリック クラウドのネットワーク管理者が確認していることを前提としています。

- 2 NSX Manager で、[送信元]、[宛先] または [適用先] フィールドを使用して、グループを含む分散ファイアウォール (DFW) ルールを作成します。手順については、[分散ファイアウォールの追加](#) を参照してください。

注： パブリック クラウド ワークロード仮想マシンでは、ステートフル ポリシーのみがサポートされます。NSX Manager でステートレス ポリシーを作成できますが、パブリック クラウド ワークロード仮想マシンが含まれているグループとは一致しません。

- 3 CSM で、NSX で管理する仮想マシンをホワイトリストから削除します。手順については、[ホワイトリストへの仮想マシンの登録方法とホワイトリストからの削除方法](#)を参照してください。

注： ホワイトリスト登録は、CSM にパブリック クラウド インベントリを追加する際の最初のワークフローで強く推奨される手動プロセスです。仮想マシンがホワイトリストに登録されていない場合は、ホワイトリストから削除する必要はありません。

- 4 パブリック クラウドで一致を検出するグループと DFW ルールの場合、次の処理が自動的に行われます。
 - a AWS で、NSX Cloud が `nsx-<NSX GUID>` という名前の新しいセキュリティ グループを作成します。
 - b Microsoft Azure で、NSX Cloud が NSX Manager で作成されたグループに対応するアプリケーション セキュリティ グループ (ASG) と、グループ化されたワークロード仮想マシンと一致する DFW ルールに対応するネットワーク セキュリティ グループ (NSG) を作成します。

注： NSX Cloud は、NSX Manager およびパブリック クラウド グループと DFW ルールを 30 秒ごとに同期します。

- 5 CSM で、パブリック クラウド アカウントを再同期します。
 - a CSM にログインし、パブリック クラウド アカウントに移動します。
 - b パブリック クラウド アカウントから、[アクション] - [アカウントの再同期] の順にクリックします。再同期が完了するまで待ちます。
 - c VPC/VNet に移動し、赤色のエラー インジケータをクリックします。インスタンス ビューに移動します。
 - d グリッド表示の場合はビューを詳細に切り替え、ルールの認識列で [失敗] をクリックすると、エラーが表示されます（存在する場合）。

次のステップ

[現在の制限事項と一般的なエラー](#) を参照してください。

現在の制限事項と一般的なエラー

これらの既知の制限事項と一般的なエラーを参照して、Native Cloud 強制モード のパブリック クラウド ワークロード仮想マシンの管理に関するトラブルシューティングを行ってください。

注： パブリック クラウドにより、次の制限が設定されます。

- ワークロード仮想マシンに適用できるセキュリティ グループの数。
- ワークロード仮想マシンで認識できるルールの数。
- セキュリティ グループごとに認識できるルールの数。
- セキュリティ グループの割り当て範囲。たとえば、Microsoft Azure のネットワーク セキュリティ グループ (NSG) の場合はそのリージョンに限定されますが、AWS のセキュリティ グループ (SG) の場合は VPC に限定されます。

これらの制限の詳細については、パブリック クラウドのドキュメントを参照してください。

現在の制限事項

現在のリリースでは、ワークロード仮想マシンの DFW ルールに次の制限があります。

- ネストされたグループはサポートされせん。
- メンバーとして仮想マシンや IP アドレスを持たないグループはサポートされません（たとえば、セグメントや論理ポートベースの基準はサポートされません）。
- 送信元と宛先の両方に IP アドレスまたは CIDR ベースのグループを設定できません。
- 送信元と宛先の両方に「任意」を設定できません。
- [Applied_To] グループには、送信元または宛先、あるいは送信元 + 宛先グループのみを指定できます。他のオプションは使用できません。
- ローカルの VPC/VNet ルールの適用のみがサポートされます。複数の VPC/VNet にまたがるグループを NSX Manager に作成できます。ただし、このようなルールの認識は VPC/VNet 内でのみ有効です。VPC/VNet 間の DFW ルールは認識されません。

- TCP および UDP のみがサポートされます。

注： AWS のみ：

AWS VPC 内のワークロード仮想マシンに作成された拒否ルールは AWS で認識されません。AWS のデフォルトでは、すべてがブラックリストに登録されます。これにより、NSX-T Data Center で次のような結果になります。

- VM1 と VM2 の間に拒否ルールがある場合、拒否ルールではなく、デフォルトの AWS 動作が原因で、VM1 と VM2 間のトラフィックは許可されません。拒否ルールが AWS で認識されません。
- NSX Manager で、同じ仮想マシンに次の 2 つのルールを作成し、ルール 1 がルール 2 より優先順位が高いとします。
 - a VM1 から VM2 への SSH 拒否
 - b VM1 から VM2 への SSH 許可

拒否ルールは、AWS で認識されないため無視されます。SSH 許可ルールが認識されます。これは想定に反した結果ですが、AWS のデフォルトの動作による制限です。

一般的なエラーとその解決方法

[エラー：NSX ポリシーが仮想マシンに適用されていません。]

このエラーが表示された場合、特定の仮想マシンに DFW ルールが適用されていません。この仮想マシンが対象になるように、NSX Manager でルールまたはグループを編集します。

[エラー：ステートレス NSX ルールはサポートされていません。]

このエラーが表示された場合は、ステートレス セキュリティ ポリシーのパブリック クラウド ワークロード仮想マシンに DFW ルールを追加しています。これはサポートされません。新しいセキュリティ ポリシーを作成するか、ステートフル モードで既存のセキュリティ ポリシーを使用します。

NSX Cloud でサポートされる NSX-T Data Center の機能

NSX Cloud は、NSX-T Data Center に論理ネットワーク エンティティを生成することにより、パブリック クラウド VPC または VNet のネットワーク トポロジを作成します。

このリストは、自動生成されたエンティティについて調べる際や、それらのエンティティをパブリック クラウドに適用するときに NSX-T Data Center 機能を使用する方法を調べるリファレンスとして使用してください。

NSX Manager の構成

PCG が正常に展開されたら、作成した論理エンティティの詳細について、『NSX-T Data Center インストール ガイド』の「自動作成された NSX-T の論理エンティティ」[]を参照してください。

重要： これらの自動作成されたエンティティは編集または削除しないでください。

注： Windows ワークロード仮想マシンで一部の機能を利用できない場合は、Windows ファイアウォールが正しく設定されていることを確認します。

表 22-10.

NSX-T Data Center の機能	詳細	NSX Cloud に関する注
セグメントまたは論理スイッチ	4 章 セグメント を参照してください。	管理対象仮想マシンの接続先となるすべてのパブリック クラウド サブネットにセグメントが作成されます。これは、ハイブリッド セグメントです。
ゲートウェイまたは論理ルーター	2 章 Tier-0 ゲートウェイ および 3 章 Tier-1 ゲートウェイ を参照してください。	PCG がトランジット VPC または VNet で展開されると、NSX Cloud によって Tier-0 論理ルーターが自動作成されます。トランジット VPC/VNet にリンクされると、コンピュータ VPC/VNet ごとに Tier-1 ルーターが作成されます。
IPFIX	IPFIX の設定 を参照してください。	<ul style="list-style-type: none"> ■ NSX Cloud では、UDP ポート 4739 でのみ IPFIX をサポートします。 ■ [スイッチと分散ファイアウォールからの IPFIX 設定]: IPFIX プロファイルを適用した Windows 仮想マシンと同じサブネットにコレクタが配置されている場合、Windows では、ARP エントリが見つからないと UDP パケットが暗黙的に破棄されてしまうため、Windows 仮想マシン上のコレクタの静的 ARP エントリが必要になります。
ポート ミラーリング	[ポート ミラーリング セッションの開始] を参照してください。	<p>ポート ミラーリングは、現在のリリースでは AWS でのみサポートされています。</p> <ul style="list-style-type: none"> ■ NSX Cloud の場合、ポート ミラーリングは [ツール] > [ポート ミラーリング セッション] で設定してください。 ■ L3SPAN ポート ミラーリングのみがサポートされています。 ■ コレクタは、送信元のワークロード仮想マシンと同じ VPC に配置する必要があります。
ゲートウェイ ファイアウォール	ゲートウェイ ファイアウォールの設定 を参照してください。	Tier-0 ゲートウェイでのみサポートされます。

NSX-T Data Center とパブリック クラウド タグを使用した仮想マシンのグループ化

NSX Cloud では、ワークロード仮想マシンに割り当てたパブリック クラウド タグを使用することができます。

NSX Manager は、パブリック クラウドと同様に、タグを使用して仮想マシンをグループ化します。つまり、仮想マシンのグループ化を容易にするには、ワークロード仮想マシンに適用されたパブリック クラウド タグが事前定義済みのサイズと予約語の要件を満たしている場合、NSX Cloud はそのタグを使用して NSX Manager に取り込みます。

注： 分散ファイアウォール ルールは、仮想マシンに割り当てられたタグによって異なります。これらのタグは、適切なパブリック クラウド権限を持つユーザーであれば、誰でも変更することができます。このため、NSX-T Data Center では、このようなユーザーが信頼でき、仮想マシンに常に正しいタグが設定されていることをパブリック クラウドのネットワーク管理者が確認していることを前提としています。

タグの用語

NSX Manager の [タグ] は、パブリック クラウドのコンテキストで [値] と呼ばれるものを指します。パブリック クラウド タグの [キー] は、NSX Manager では [スコープ] と呼ばれます。

タグのコンポーネント	
NSX Manager 内	パブリック クラウド内のタグの同等のコンポーネント
スコープ	キー
タグ	値

タグのタイプと制限事項

NSX Cloud では、NSX の管理対象パブリック クラウドの仮想マシンに対して 3 つのタイプのタグを使用できます。

- [システム タグ]：これらはシステムが定義するタグであるため、追加、編集、または削除することはできません。NSX Cloud は、次のシステム タグを使用します。
 - azure:subscription_id
 - azure:region
 - azure:vm_rg
 - azure:vnet_name
 - azure:vnet_rg
 - azure:transit_vnet_name
 - azure:transit_vnet_rg
 - aws:account
 - aws:availabilityzone
 - aws:region
 - aws:vpc
 - aws:subnet
 - aws:transit_vpc

- [検出タグ]：パブリック クラウド内の仮想マシンに追加したタグが NSX Cloud によって自動的に検出され、NSX Manager インベントリのワークロード仮想マシンに表示されます。これらのタグを NSX Manager 内から編集することはできません。検出タグの数に制限はありません。これらのタグには、Microsoft Azure から検出されたことを示す `dis:azure:`、および AWS から検出されたことを示す `dis:aws` がプレフィックスとして付いています。

パブリック クラウド内のタグに変更を加えた場合、変更は 3 分以内に NSX Manager に反映されます。

この機能はデフォルトで有効です。Microsoft Azure サブスクリプションまたは AWS アカウントを追加するときに、Microsoft Azure タグまたは AWS タグの検出を有効または無効にすることができます。

- [ユーザー タグ]：ユーザー タグは最大 25 個まで作成できます。作成者は、ユーザー タグに対して追加、編集、削除の権限を持ちます。ユーザー タグの管理については、[仮想マシンのタグの管理](#) を参照してください。

表 22-11. タグのタイプと制限事項の概要

タグのタイプ	タグのスコープまたは 事前定義済みプレフィックス	制限事項	エンタープライズ管理者 権限	監査者 権限
システム定義	すべてのシステム タグ <ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availability zone 	スコープ（キー）：20 文字 タグ（値）：65 文字 設定の上限：5	読み取り専用	読み取り専用
検出	VNet からインポートされた Microsoft Azure タグには以下のプレフィックスが付きます。 [dis:azure:] Virtual Private Cloud (VPC) からインポートされた AWS タグには以下のプレフィックスが付きます。 [dis:aws:]	スコープ（キー）：20 文字 タグ（値）：65 文字 設定の上限：制限なし 注： 文字数の制限に、プレフィックス [dis:<public cloud name>] は含まれません。これらの制限を超えるタグは、NSX Manager に反映されません。 プレフィックス [nsx] が付いたタグは無視されます。	読み取り専用	読み取り専用
ユーザー	ユーザー タグは、以下の値を除き、許可された文字数内であれば任意のスコープ（キー）と値を指定できます。 <ul style="list-style-type: none"> ■ スコープ（キー）のプレフィックス [dis:azure:] または [dis:aws:] ■ システム タグと同じスコープ（キー） 	スコープ（キー）：30 文字 タグ（値）：65 文字 設定の上限：25	追加/編集/削除	読み取り専用

検出タグの例

注： タグの形式は、パブリック クラウドでは **key=value** で、NSX Manager では **scope=tag** です。

表 22-12.

ワークロード仮想マシンの [パブリック クラウド] タグ	NSX Cloud による検出	ワークロード仮想マシンの同等の NSX Manager タグ
Name=Developer	○	dis:azure:Name=Developer
ValidDisTagKeyLength=ValidDisTagValue	○	dis:azure:ValidDisTagKeyLength=ValidDisTagValue
Abcdefghijklmnopqrstuvwxyz=value2	× (キーが 20 文字を超過)	なし
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgjgjuytreswqacvbcdefghijklmnopqrstuvwxyz	× (値が 65 文字を超過)	なし
nsx.name=Tester	× (キーのプレフィックスが [nsx])	なし

NSX Manager でのタグの使用方法

- [仮想マシンのタグの管理](#) を参照してください。
- [オブジェクトの検索](#) を参照してください。
- [グループの追加](#) を参照してください。
- [NSX 強制モード でのワークロード仮想マシンのマイクロセグメンテーションの設定](#) を参照してください。

ネイティブ クラウド サービスの使用

NSX Manager からパブリック クラウド ワークロード仮想マシンでは、次のネイティブ クラウド サービスがサポートされています。

PCG を展開すると、サポートされているネイティブ クラウド サービスごとに、NSX Manager にグループが作成されます。

現在サポートされているパブリック クラウド サービスに次のグループが作成されます。

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

これらのネイティブ クラウド サービスを使用する場合は、必要に応じて、ルールのソース フィールドまたは宛先フィールドにネイティブ クラウド サービス グループを含む DFW ポリシーを作成します。

DFW ルールは、ネイティブ クラウド サービスではなく、仮想マシンに適用されます。

注： NSX 強制モード、つまり NSX Tools を使用してワークロードを管理している場合、Microsoft Azure のネイティブ クラウド サービスはサポートされません。

現在の制限事項

エンドポイント			サービスを宛先として使用する DFW ルール		サービスをソースとして使用する DFW ルール	
[パブリック クラウド]	[サービス]	[スコープ]	[仮想マシンに適用済みか]	[サービスに適用済みか]	[サービスに適用済みか]	[仮想マシンに適用済みか]
Microsoft Azure	BLOB ストレージ	グローバル	○	×	×	○
	Cosmos DB					
	SQL					
	ロード バランサ					
AWS	S3	VPC ローカル	○	×	×	○
	Dynamo DB					
	RDS					
	ELB					

パブリック クラウドのサービス挿入

NSX Cloud では、NSX の管理対象ワークロード仮想マシンに対してパブリック クラウド内のサード パーティ サービスの使用をサポートします。

パブリック クラウドのワークロード仮想マシンでサービス挿入を利用するには、NSX-T Data Center ではなく、パブリック クラウドにサービス アプライアンスをホストする必要があります。サービス アプライアンスは中継 VPC/VNet にホストすることをお勧めします。

サービス挿入を有効にする前に、PCG を中継 VPC または VNet に展開する必要があります。

次に、NSX の管理対象ワークロード仮想マシンでサービス挿入を許可する 1 回限りの設定の概要を示します。

表 22-13. パブリック クラウド内の NSX の管理対象ワークロード仮想マシンでサービス挿入を行う場合に必要な設定の概要

頻度	タスク	方法
初期設定中に 1 回	パブリック クラウド内、可能であれば PCG が展開されている中継 VPC または VNet 内に、サービス アプライアンスを設定します。	サードパーティのサービス アプライアンスおよびパブリック クラウドに固有の手順を参照してください。
	NSX-T Data Center にサードパーティ サービスを登録します。	サービス定義と対応する仮想エンドポイントの作成 を参照してください。

表 22-13. パブリック クラウド内の NSX の管理対象ワークロード仮想マシンでサービス挿入を行う場合に必要な設定の概要（続き）

頻度	タスク	方法
	サービス アプライアンスでサービス挿入にのみ使用される /32 仮想サービス IP アドレス (VSIP) を使用して、サービスの仮想インスタンス エンドポイントを作成します。VSIP が VPC または VNet の CIDR 範囲と競合しないようにしてください。この VSIP は BGP 経由で PCG にアドバタイズされます。	サービス定義と対応する仮想エンドポイントの作成 を参照してください。
	サービス アプライアンスと PCG の間に IPsec VPN トンネルを作成します。	IPsec VPN セッションの設定 を参照してください。
	PCG とサービス アプライアンス間に BGP を構成し、サービス アプライアンスから VSIP をアドバタイズし、PCG からデフォルト ルート (0.0.0.0/0) をアドバタイズします。	BGP とルート再配分の設定 を参照してください。
	注： 現在のリリースでは、サービス挿入は North-South トラフィックに対してのみサポートされます。	
必要に応じて	1 回限りの設定が完了したら、NSX の管理対象ワークロード仮想マシンから VSIP にサービス トラフィックを再ルーティングするリダイレクト ルールを設定します。これらのルールは、PCG のアップリンク ポートに適用されます。	リダイレクト ルールの設定 を参照してください。

手順

1 サービス定義と対応する仮想エンドポイントの作成

パブリック クラウド内のサービス アプライアンスのサービス定義および仮想エンドポイントを作成するには、NSX Manager API を使用する必要があります。

2 IPsec VPN セッションの設定

PCG とサービス アプライアンス間の IPsec VPN セッションを設定します。

3 BGP とルート再配分の設定

IPsec VPN トンネルを介して PCG とサービス アプライアンス間に BGP を構成します。

4 リダイレクト ルールの設定

要件に応じて、リダイレクト ルールを調整できます。

サービス定義と対応する仮想エンドポイントの作成

パブリック クラウド内のサービス アプライアンスのサービス定義および仮想エンドポイントを作成するには、NSX Manager API を使用する必要があります。

前提条件

パブリック クラウド内のサービス アプライアンスの仮想エンドポイントとして提供する、予約済みの /32 IP アドレスを選択します (100.100.100.100/32 など)。このアドレスは、仮想サービス IP アドレス (VSIP) といいます。

注： 高可用性ペアにサービス アプライアンスを展開した場合、BGP の構成中、PCG にアドバタイズする際に、別のサービス定義は作成せず、同じ VSIP を使用します。

手順

- 1 サービス アプライアンスのサービス定義を作成するには、認証に NSX Manager 認証情報を使用して、次の API 呼び出しを実行します。

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

要求の例：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  [ "display_name": "Service_Appliance1", ]
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

応答の例：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  [ "display_name": "Service_Appliance1", ]
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
}
```

```

    "_protection": "REQUIRE_OVERRIDE",
    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 サービス アプライアンスの仮想エンドポイントを作成するには、認証に NSX Manager 認証情報を使用して、次の API 呼び出しを実行します。

```

PATCH https://{NSX Manager-IP}/policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-
services/cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

要求の例：

```

{
  "resource_type": "VirtualEndpoint",
  ["display_name": "Service_Appliance1_Endpoint",]
  "target_ips": [
    {
      [ "ip_addresses": [
        "100.100.100.100"
      ],
      "prefix_length": 32
    }
  ],
  [ "service_names": [
    "Service_Appliance1"
  ]
}

```

応答の例：

```

200 OK

```

注： 手順 1 の display_name は、手順 2 の service_names と一致する必要があります。

次のステップ

IPsec VPN セッションの設定

IPsec VPN セッションの設定

PCG とサービス アプライアンス間の IPsec VPN セッションを設定します。

前提条件

- 中継 VPC/VNet に PCG を単体で、または HA ペアで展開する必要があります。
- サービス アプライアンスは、パブリック クラウド内、可能であれば中継 VPC/VNet 内に設定する必要があります。

手順

- 1 [ネットワーク] - [VPN] の順に移動します。

- 2 IPsec タイプの [VPN サービス] を追加し、NSX Cloud に固有の次の構成オプションをメモしておきます。詳細については、[IPsec VPN サービスの追加](#)を参照してください。

オプション	説明
名前	ローカル エンドポイントおよび IPsec VPN セッションの設定には、この VPN サービスの名前が使用されます。設定をメモしておきます。
サービス タイプ	この値が IPsec に設定されていることを確認します。
Tier-0 ゲートウェイ	中継 VPC/VNet 用に自動作成された Tier-0 ゲートウェイを選択します。この名前には、cloud-t0-vpc-6bcd2c13 のような VPC/VNet ID が含まれています。

- 3 PCG の [ローカル エンドポイント] を追加します。ローカル エンドポイントの IP アドレスは、中継 VPC/VNet 内に展開された PCG の nsx:local_endpoint_ip タグの値です。この値の中継 VPC/VNet にログインします。NSX Cloud に固有の次の設定をメモします。詳細については、[ローカル エンドポイントの追加](#)を参照してください。

オプション	説明
名前	IPsec VPN セッションの設定には、ローカル エンドポイントの名前が使用されます。設定をメモしておきます。
VPN サービス	手順 2 で追加した VPN サービスを選択します。
IP アドレス	AWS コンソールまたは Microsoft Azure ポータルにログインして、この値を検索します。この値は、PCG のアップリンク インターフェイスに適用された nsx:local_endpoint_ip タグの値です。

- 4 PCG とパブリック クラウド内の（可能であれば中継 VPC/VNet 内にホストされている）サービス アプライアンスの間に [ルートベースの IPsec セッション] を作成します。

オプション	説明
タイプ	この値が [ルート ベース] に設定されていることを確認します。
VPN サービス	手順 2 で追加した VPN サービスを選択します。
ローカル エンドポイント	手順 3 で作成したローカル エンドポイントを選択します。
リモート IP アドレス	サービス アプライアンスのプライベート IP アドレスを入力します。 注： パブリック IP アドレスを使用してサービス アプライアンスにアクセスできる場合は、パブリック IP アドレスを PCG のアップリンク インターフェイスのローカル エンドポイント IP アドレス（別名、セカンダリ IP アドレス）に割り当てます。
トンネル インターフェイス	このサブネットは、VPN トンネルのサービス アプライアンスのサブネットと一致する必要があります。サービス アプライアンスで VPN トンネル用に設定したサブネットの値を入力するか、ここに入力した値をメモして、サービス アプライアンスで VPN を設定するときに同じサブネットが使用されるようにします。 注： このトンネル インターフェイスで BGP を構成します。 BGP とルート再配分の設定 を参照してください。

オプション	説明
リモート ID	パブリック クラウド内のサービス アプライアンスのプライベート IP アドレスを入力します。
IKE プロファイル	IPsec VPN セッションは IKE プロファイルに関連付けられている必要があります。プロファイルを作成する場合は、ドロップダウン メニューから選択します。デフォルトのプロファイルも使用できます。

次のステップ

BGP とルート再配分の設定

BGP とルート再配分の設定

IPsec VPN トンネルを介して PCG とサービス アプライアンス間に BGP を構成します。

PCG とサービス アプライアンス間に確立した IPsec VPN トンネル インターフェイス上に BGP ネイバーを設定します。詳細については、[BGP の設定](#)を参照してください。

同様に、サービス アプライアンスで BGP を設定する必要があります。詳細については、パブリック クラウド内の特定のサービスのドキュメントを参照してください。

次に、ルート再配分を次のように設定します。

- PCG はサービス アプライアンスにデフォルト ルート (0.0.0.0/0) をアドバタイズします。
- サービス アプライアンスは PCG に仮想サービス IP アドレス (VSIP) をアドバタイズします。これは、サービスを登録するときに使用される IP アドレスと同じです。[サービス定義と対応する仮想エンドポイントの作成](#)を参照してください。

注： サービス アプライアンスを高可用性ペアで展開する場合は、両方のサービス アプライアンスから同じ VSIP をアドバタイズします。

手順

- 1 [ネットワーク] - [Tier-0 ゲートウェイ] の順に移動します。
- 2 中継 VPC/VNet に自動作成された、cloud-t0-vpc-6bcd2c13 のような名前の Tier-0 ゲートウェイを選択して、[編集] をクリックします。
- 3 [BGP] セクションの [BGP ネイバー] の横にある番号またはアイコンをクリックします。
- 4 これらの設定をメモしておきます。

オプション	説明
IP アドレス	PCG とサービス アプライアンス間の VPN に、サービス アプライアンス トンネル インターフェイス上に設定された IP アドレスを使用します。
リモート AS の番号	この数は、パブリック クラウド内のサービス アプライアンスの AS 番号と一致する必要があります。
ルート フィルタ	出力フィルタを設定して、PCG からサービス アプライアンスにデフォルト ルート (0.0.0.0/0) をアドバタイズします。

- 5 [ルート再配分] セクションから、Tier-0 ゲートウェイでスタティック ルートを有効にします。

ルート再配分の設定

Tier-0 ゲートウェイ cloud-t0-415... #ルート再配分 ①

ルート再配分の追加

検索

名前	ルート再配分	ルート マップ
名前の入力	設定*	ルート マップの選択

ルート再配分の設定

Tier-0 ゲートウェイ cloud-t0-415... #選択した送信元 ①

送信元を以下で選択

Tier-0 サブネット

☒ スタティック ルート
 ☐ NAT IP

☐ IPsec のローカル IP
 ☐ DNS フォワーダの IP

☐ EVPN TEP IP
 ☐ 外部インターフェイスのサブネット

☐ 接続されたインターフェイスおよびセグメント
 ☐ 接続されたセグメント

☐ サービス インターフェイスのサブネット

☐ ループバック インターフェイスのサブネット

次のステップ

リダイレクト ルールの設定

リダイレクト ルールの設定

要件に応じて、リダイレクト ルールを調整できます。

初期設定が完了したら、NSX の管理対象ワークロード仮想マシンのさまざまなタイプのトラフィックをサービス アプライアンス経由で再ルーティングする際に必要となるリダイレクト ルールを作成し、編集することができます。

前提条件

リダイレクト ルールを作成する前に、すべてのサービス挿入の設定が完了している必要があります。

手順

- 1 [セキュリティ] - [North-South のファイアウォール] - [ネットワーク イントロスペクション (N-S)] の順に移動します。
- 2 [ポリシーの追加] をクリックします。

オプション	説明
名前:	ポリシーにわかりやすい名前を入力します。例： North-South サービス挿入(Azure 仮想マシン)。
リダイレクト先:	サービスを登録するときにこのサービス アプライアンス用に作成した仮想エンドポイントの名前を選択します。 サービス定義と対応する仮想エンドポイントの作成 を参照してください。
適用先:	PCG の Tier-0 ゲートウェイを選択します。

- 3 新しいポリシーを選択して、[ルールの追加] をクリックします。サービス挿入に固有の次の値をメモします。

オプション	説明
送信元	トラフィックをリダイレクトする必要があるサブネットのグループを選択します (NSX の管理対象ワークロード仮想マシンのグループなど)。
宛先	サービス アプライアンス経由でルーティングする、宛先 IP アドレスまたはサービス (Google など) のリストを選択します。
適用先	アクティブおよびスタンバイ PCG のアップリンク ポートを選択します。
アクション	[リダイレクト] を選択します。

NSX 管理対象仮想マシンでの NAT の有効化

NSX Cloud を使用すると、NSX の管理対象仮想マシンで NAT を有効にできます。

NSX の管理対象仮想マシンで North-South トラフィックを有効にするには、パブリック クラウド タグを使用します。

NAT を有効にする NSX の管理対象仮想マシンで、次のタグを適用します。

表 22-14.

キー	値
<code>nsx.publicip</code>	パブリック クラウドのパブリック IP アドレス (50.1.2.3 など)

注： ここで指定したパブリック IP アドレスは、開いておく必要があります。NAT を有効にするワークロード仮想マシンを含め、すべての仮想マシンに対してこのパブリック IP アドレスを割り当てないでください。他のインスタンスに以前関連付けられていたパブリック IP アドレス、またはプライベート IP アドレスを割り当てた場合、NAT は動作しません。この場合は、パブリック IP アドレスの割り当てを解除します。

このタグを適用すると、ワークロード仮想マシンはインターネット トラフィックにアクセスできるようになります。

Syslog 転送の有効化

NSX Cloud は、Syslog 転送をサポートします。

管理対象の仮想マシンで、分散ファイアウォール (DFW) パケットの Syslog 転送を有効にできます。詳細については、『NSX-T Data Center トラブルシューティング ガイド』の「[リモート ログの構成]」を参照してください。

次の手順を実行します。

手順

- 1 ジャンプ ホストを使用して PCG にログインします。
- 2 `nsxcli` と入力して、NSX-T Data Center CLI を開きます。

- 3 次のコマンドを入力して、分散ファイアウォール ログの転送を有効にします。

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <server-IP-address> proto udp level info
messageid FIREWALL-PKTLOG
```

このように設定すると、NSX Agent の DFW パケット ログが PCG 上の `/var/logs/syslog` で利用できるようになります。

- 4 仮想マシンごとにログ転送を有効にするには、次のコマンドを入力します。

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

NSX 強制モードでの VPN の設定

オンプレミスの NSX-T Data Center 環境で、自動作成された Tier-0 ゲートウェイとして表示される PCG を使用して VPN を設定できます。この手順は、NSX 強制モードで管理されているワークロード仮想マシンに固有のものであります。

ここで説明する追加の手順に従い、NSX Manager で Tier-0 ゲートウェイを使用して VPN を設定する場合と同じ方法で PCG を使用します。同じパブリック クラウドまたは異なるパブリック クラウドに展開されている PCG 間、またはオンプレミスのゲートウェイやルーターとの間で VPN トンネルを作成できます。NSX-T Data Center での VPN サポートの詳細については、[5 章 Virtual Private Network \(VPN\)](#)を参照してください。

前提条件

- VPC/VNet に PCG または PCG の HA ペアが展開されていることを確認します。
- リモート ピアがルートベースの VPN と BGP をサポートしていることを確認します。

手順

- 1 パブリック クラウドで、NSX が PCG に割り当てたローカル エンドポイントを検索します。必要に応じてパブリック IP アドレスを割り当てます。
 - a パブリック クラウドの PCG インスタンスに移動し、タグに移動します。
 - b `nsx.local_endpoint_ip` タグの値フィールドにある IP アドレスをメモします。
 - c (オプション) VPN トンネルでパブリック IP アドレスが必要な場合 (たとえば、別のパブリック クラウドやオンプレミスの NSX-T Data Center 環境に VPN を設定する場合) は、次の操作を行います。
 - 1 PCG インスタンスのアップリンク インターフェイスに移動します。
 - 2 手順 [b] でメモした `nsx.local_endpoint_ip` の IP アドレスにパブリック IP アドレスを割り当てます。
 - d (オプション) PCG インスタンスの HA ペアがある場合は、手順 [a] と [b] を繰り返します。必要であれば、手順 [c] の説明に従ってパブリック IP アドレスを割り当てます。

- 2 NSX Manager で、cloud-t0-vpc/vnet-<vpc/vnet-id> のような前の Tier-0 ゲートウェイとして表示される PCG で IPsec VPN を有効にします。この Tier-0 ゲートウェイのエンドポイントと目的の VPN ピアのリモート IP アドレスの間にルートベースの IPsec セッションを作成します。詳細については、[IPsec VPN サービスの追加](#)を参照してください。

- a [ネットワーク] - [VPN] - [VPN サービス] - [サービスの追加] - [IPsec] の順に移動します。次のように詳細を指定します。

オプション	説明
名前	VPN サービスにわかりやすい名前を付けます。たとえば <VPC-ID> AWS_VPN、<VNet-ID>-AZURE_VPN などを入力します。
Tier-0/Tier-1 ゲートウェイ	パブリック クラウド内の PCG に Tier-0 ゲートウェイを選択します。

- b [ネットワーク] - [VPN] - [ローカル エンドポイント] - [ローカル エンドポイントの追加] の順に移動します。次の情報を入力します。その他の詳細については、[ローカル エンドポイントの追加](#)を参照してください。

注： PCG インスタンスの HA ペアがある場合は、パブリック クラウドに接続している対応のローカル エンドポイント IP アドレスを使用して、各インスタンスにローカル エンドポイントを作成します。

オプション	説明
名前	ローカル エンドポイントにわかりやすい名前を付けます。たとえば、<VPC-ID>-PCG-preferred-LE や <VNET-ID>-PCG-preferred-LE などを入力します。
VPN サービス	手順 [2a] で PCG に作成した Tier-0 ゲートウェイに VPN サービスを選択します。
IP アドレス	手順 [1b] でメモした PCG のローカル エンドポイントの IP アドレスの値を入力します。

- c [ネットワーク] - [VPN] - [IPsec セッション] - [IPsec セッションの追加] - [ルート ベース] の順に移動します。次の情報を入力します。その他の詳細については、[ルートベース IPsec セッションの追加](#)を参照してください。

注： VPC に展開されている PCG と VNet に展開されている PCG の間に VPN トンネルを作成する場合は、VPC にある各 PCG のローカル エンドポイントから VNet にある PCG のリモート IP アドレスにトンネルを作成する必要があります。逆に、VNet の PCG から VPC にある PCG のリモート IP アドレスへのトンネルも作成する必要があります。アクティブ PCG とスタンバイ PCG に別のトンネルを作成する必要があります。これにより、2 つのパブリック クラウド間の IPsec セッションで完全なメッシュが構築されます。

オプション	説明
名前	IPsec セッションにわかりやすい名前を付けます。たとえば、<VPC-ID>-PCG1-to-remote_edge のように入力します。
VPN サービス	手順 [2a] で作成した VPN サービスを選択します。
ローカル エンドポイント	手順 [2b] で作成したローカル エンドポイントを選択します。
リモート IP アドレス	VPN トンネルを作成するリモート ピアのパブリック IP アドレスを入力します。

オプション	説明
	<p>注: DirectConnect や ExpressRoute などプライベート IP アドレスにアクセスできる場合は、リモート IP にプライベート IP アドレスを設定できます。</p>
トンネル インターフェイス	トンネル インターフェイスを CIDR 形式で入力します。IPsec セッションを確立するには、リモート ピアで同じサブネットを使用する必要があります。

vm NSX-T

ホーム ネットワーク セキュリティ インベントリ プランとトラブルシューティング システム

ポリシー マネージャ

ステップ 2a.

VPN サービス IPSEC セッション L2 VPN セッション ローカル エンドポイント プロファイル

サービスの追加

すべてを表示 名前、パスなどでフィルタリング

名前	サービス タイプ	Tier-0/Tier-1 ゲートウェイ	セッション	状態
<VPC-ID>-AWS_VPN	IPsec	cloud-to-vpc-073617880a9622d93	1	成功
説明	VPN service on AWS Transit VPC ID vpc-073617880a9622d93	管理状態	有効	
IKE ログ レベル	情報	タグ	0	
セッションの同期	有効			

vm NSX-T

vm NSX-T

ホーム ネットワーク セキュリティ インベントリ プランとトラブルシューティング システム

ポリシー マネージャ

ステップ 2b.

VPN サービス IPSEC セッション L2 VPN セッション ローカル エンドポイント プロファイル

ローカル エンドポイントの追加

すべてを表示 名前、パスなどでフィルタリング

名前	VPN サービス	IP アドレス	サイトの証明書	セッション	状態
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	未設定	1	成功
説明	未設定	ローカル ID	10.99.3.35		
信頼されている CA (証明書)	未設定	証明書失効リスト	未設定		
タグ	0				

vm NSX-T

vm NSX-T

ホーム ネットワーク セキュリティ インベントリ プランとトラブルシューティング システム

ポリシー マネージャ

ステップ 2c.

VPN サービス IPSEC セッション L2 VPN セッション ローカル エンドポイント プロファイル

IPSEC セッションの追加

すべてを表示 admin

名前	タイプ	VPN サービス	ローカル エンドポイント	リモート IP	状態	アラーム
<VPC-ID>-PCG1-to-remote_edge	ルート ベース	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	停止	0
説明	未設定	管理状態	有効			
コンプライアンス スイッチ	なし	トンネル インターフェイス	192.168.50.10/24			
認証モード	PSK	リモート ID	172.0.3.145			
プリシェアード キー	*****					
詳細なプロパティ						
IKE プロファイル	nsx-default-l3vpn-ike-profile	接続開始モード	イニシエータ			
IPsec プロファイル	nsx-default-l3vpn-	TCP MSS クランプ	無効			

更新

IPsec セッション: 1 個中 1 ~ 1 個

- 3 手順 [2] で設定した IPsec VPN トンネル インターフェイスで BGP ネイバーを設定します。詳細については、[BGP の設定](#)を参照してください。
- [ネットワーク] - [Tier-0 ゲートウェイ] の順に移動します。
 - IPsec セッションを作成した場所に、自動的に作成された Tier-0 ゲートウェイを選択して、[編集] をクリックします。
 - [BGP] セクションの [BGP ネイバー] の横にある番号またはアイコンをクリックして、次の詳細情報を入力します。

オプション	説明
IP アドレス	VPN ピアの IPsec セッションのトンネル インターフェイスで設定されたリモート VTI の IP アドレスを使用します。
リモート AS の番号	この番号は、リモート ピアの AS 番号と一致する必要があります。

 Tier-0 ゲートウェイ

[ゲートウェイの追加](#) [すべてを表示](#) [名前、パ](#)

	Tier-0 ゲートウェイの名前	HA モード	リンクされた Tier-1 ゲートウェイ	リンクされたセグメント
>	マルチキャスト			
>	BGP			
	ローカル AS	1000	サービス ルーター間の iBGP	● 有効
	BGP	● 有効	ECMP	● 有効
	グレースフル リスタート	ヘルパーのみ	Multipath Relax	● 有効
	グレースフル リスタート タイマー	180 秒間	グレースフル リスタート失効タイマー	600 秒間
	ルートの集約	0	BGP ネイバー	

ステップ 3.

BGP ネイバー

Tier-0 ゲートウェイ cloud-t0-415... [# ネイバー](#)

	IP アドレス	BFD	リモート AS の番号
⋮	192.168.50.11	無効	1000
	送信元アドレス	未設定	
	ホップの上限	1	

- 4 再配分プロファイルを使用して、VPN で使用するプリフィックスをアドバタイズします。NSX 強制モード で、再配分プロファイルの Tier-1 対応ルートを接続します。

Tier-0 ゲートウェイ

ゲートウェイの追加 ▼ すべてを表示 名前、パスなどでフィ

	Tier-0 ゲートウェイの名前	HA モード	リンクされた Tier-1 ゲートウェイ	リンクされたセグメント	状態 ①
>	BGP				
▼	ルート再配分				
	ルート再配分				2 ステップ 4. ルート再配分の状態 ● 有効
⋮ >	VRF TORvf	アクティブ/アクティブ	0	0	● 成功

更新

ルート再配分

Tier-0 ゲートウェイ cloud-t0-vpc... #選択した送信元 ①

Tier-0 サブネット

アドバタイズされた Tier-1 サブネット

- 接続されたインターフェイスとセグメント
- サービス インターフェイスのサブネット
- 接続されたセグメント

よくある質問 (FAQ)

このトピックでは、よくある質問をいくつか紹介します。

NSX Cloud のコンポーネントがインストールされ実行されていることを確認するにはどうすればよいですか。

- ワークロード仮想マシン上の NSX Tools が PCG に接続されていることを確認するには、次の操作を行います。
 - nsxcli コマンドを入力して NSX CLI を開きます。
 - たとえば、次のコマンドを入力して、ゲートウェイの接続ステータスを取得します。

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

- ワークロード仮想マシンには、PCG に接続するために正しいタグが設定されている必要があります。
 - AWS コンソールまたは Microsoft Azure ポータルにログインします。
 - 仮想マシンの eth0 またはインターフェイス タグを確認します。

`nsx.network` キーには値 `default` が設定されている必要があります。

cloud-init を使用して起動された仮想マシンが検疫され、サードパーティ ツールをインストールできません。どうしたらいいでしょう。

検疫ポリシーが有効になっている場合、次の仕様の cloud-init スクリプトを使用して仮想マシンを起動すると、仮想マシンが起動時に隔離され、カスタム アプリケーションやツールをインストールできません。

- `nsx.network=default` でタグ付け
- 仮想マシンがパワーオンされたときに自動インストールまたはブート ストラップされたカスタム サービス

[解決策:]

カスタムまたはサードパーティ アプリケーションのインストールに必要な受信ポートと送信ポートを追加するように、`default` (AWS) または `default-vnet-<vnet-ID>-sg` (Microsoft Azure) のセキュリティ グループを更新します。

仮想マシンに正しくタグを付け、NSX Tools をインストールしましたが、仮想マシンが隔離されています。どうしたらいいでしょう。

この問題が発生する場合は、以下を試します。

- NSX Cloud タグ: `nsx.network` とその値: `default` が正しく入力されているかどうかを確認します。大文字と小文字は区別されます。
- 次のようにして、AWS または Microsoft Azure アカウントを CSM から再同期します。
 - CSM にログインします。
 - [クラウド] - [AWS/Azure] - [アカウント] の順に移動します。
 - パブリック クラウド アカウント タイルから [アクション] をクリックし、[アカウントの再同期] をクリックします。

ワークロード仮想マシンにアクセスできない場合はどうすればいいですか。

パブリック クラウド (AWS または Microsoft Azure) から:

- 1 トラフィックを許可するには、NSX Cloud によって管理されているポートを含む、仮想マシン上のすべてのポート、OS ファイアウォール (Microsoft Windows または IPTables)、および NSX-T Data Center が適切に構成されていることを確認します。

たとえば、仮想マシンに ping を許可するには、以下の設定が適切に行われている必要があります。

- AWS または Microsoft Azure のセキュリティ グループ。詳細については [NSX Cloud 検疫ポリシーを使用した脅威の検出](#) を参照してください。
- NSX-T Data Center 分散ファイアウォール (DFW) ルール。詳細については、[NSX で管理されたワークロード仮想マシンの NSX 強制モード でのデフォルトの接続方法を参照してください](#)。
- Linux 上の Windows ファイアウォールまたは IPTables。

- 2 SSH または他の方法（たとえば、Microsoft Azure のシリアル コンソール）を使用して仮想マシンにログインすることによって、問題を解決します。
- 3 ロックアウトされた仮想マシンを再起動することができます。
- 4 それでも仮想マシンにアクセスできない場合は、ワークロード仮想マシンにセカンダリ NIC を接続し、その NIC を介してワークロード仮想マシンにアクセスします。

Native Cloud 強制モード でも PCG が必要ですか。

はい

CSM でパブリック クラウド アカウントをオンボーディングした後、PCG の IAM ロールを変更できますか。

はい。パブリック クラウドに適用可能な NSX Cloud スクリプトを再実行して、PCG ロールを再生成できます。PCG ロールを再生成した後に、新しいロール名で CSM のパブリック クラウド アカウントを編集します。パブリック クラウド アカウントに展開された新しい PCG インスタンスは、新しいロールを使用します。

既存の PCG インスタンスは、引き続き古い PCG ロールを使用することに注意してください。既存の PCG インスタンスの IAM ロールを更新する場合は、パブリック クラウドに移動し、その PCG インスタンスのロールを手動で変更します。

NSX Cloud の NSX-T Data Center オンプレミス ライセンスを使用できますか。

はい、ELA で許可されていれば可能です。

NSX Intelligence の使用

23

VMware NSX® Intelligence™ は、オンプレミスの NSX-T Data Center 環境のセキュリティ状態を視覚的に表示します。この表示は、特定の期間内に収集されたネットワーク トラフィック フローに基づいて行われます。NSX Intelligence は、セキュリティ ポリシーの適用状況を分析し、その結果に基づいた推奨事項を提供します。これは、マイクロセグメンテーションの計画に役立ちます。

重要： NSX Intelligence のインストール、設定、使用権限が付与されているエンタープライズ管理者ロールが必要です。

NSX Intelligence 機能を使い始める前に、NSX Intelligence アプライアンスをインストールして設定する必要があります。『NSX-T Data Center インストール ガイド』の「NSX Intelligence アプライアンスのインストールと設定」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。

- [NSX Intelligence の使い方](#)
- [NSX Intelligence のビューとフローについて](#)
- [NSX Intelligence 推奨事項の操作](#)
- [NSX Intelligence のバックアップとリストア](#)
- [NSX Intelligence の問題のトラブルシューティング](#)

NSX Intelligence の使い方

NSX Intelligence 機能を使用する前に、NSX Intelligence グラフィカル ユーザー インターフェイスについて理解しておきましょう。

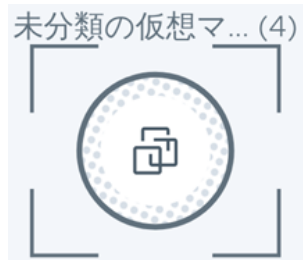
NSX Intelligence アプライアンスのインストールと構成が完了すると、NSX Manager UI の [プランとトラブルシューティング] タブで NSX Intelligence の機能が有効になります。[検出とプラン] セクションで、[検出とアクションの実行] を使用して NSX-T Data Center のエンティティを視覚的に表示します。また、[推奨] を使用すると、マイクロセグメンテーション プランに関する推奨事項を取得できます。

NSX Intelligence ホーム ページのツアー

NSX Intelligence ホーム ページにアクセスするには、NSX Manager ユーザー インターフェイスで [プランとトラブルシューティング] - [検出とアクションの実行] の順にクリックします。

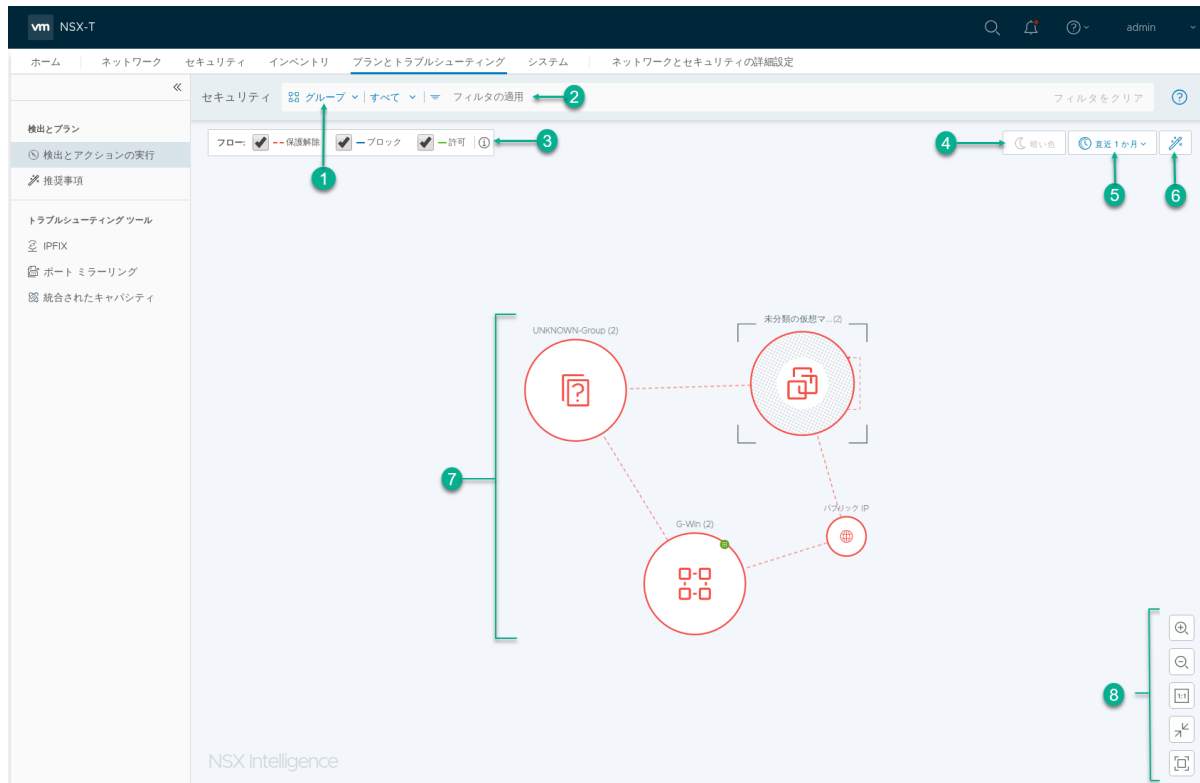
NSX Intelligence を初めてインストールして設定した後、[検出とアクションの実行] をクリックすると、「データがありません。上記のフィルタリングを変更してください。」というメッセージが表示されることがあります。表示に使用できるネットワーク トラフィック データが NSX Intelligence で収集されていないため、このメッセージが表示されます。NSX Manager からネットワーク トラフィック データを受信すると、NSX Intelligence で一部の表示を開始できます。


デフォルトでは、[検出とアクションの実行] をクリックすると、オンプレミスの NSX-T Data Center の仮想マシン メンバー間で直近 24 時間に保護解除のトラフィック フローが発生したすべてのグループのセキュリティ状態が表示されます。保護解除のネットワーク トラフィック フローは、マイクロセグメンテーションが実装されていない仮想マシン間のフローです。定義されているグループがない場合、グループは表示されません。どのグループにも属していない仮想マシンがある場合、未分類の仮想マシン グループのアイコンが表示されます。




グループが定義され、トラフィック データが収集されている場合は、次のスクリーンショットのように情報が視覚的に表示されます。次の表では、スクリーンショット内で番号の付いているセクションについて説明します。

注： NSX Intelligence は、192.168.0.0/16、172.16.0.0/12、10.0.0.0/8 のいずれかの CIDR 表記に属する IP アドレスをプライベート IP アドレスとして分類します。これらの CIDR 表記のいずれにも属していない IP アドレスは、パブリック IP アドレスとして分類されます。仮想マシンの IP アドレスがこれらの CIDR 表記のいずれにも該当しない場合は、NSX-T Data Center API ガイドの `PATCH /api/v1/intelligence/host-config` API を使用して CIDR 表記を追加することを検討してください。







セクション	説明
1	<p>セキュリティ ビューの選択領域では、表示するセキュリティのタイプを選択します。使用できるセキュリティ ビューは、[グループ] と [仮想マシン] の 2 つです。[検出とアクションの実行] をクリックすると、デフォルトでは、NSX-T Data Center 内で直近 24 時間に保護解除のフロー トラフィックが発生したグループ オブジェクトのグループ ビューが表示されます。</p> <ul style="list-style-type: none"> ■ 仮想マシン ビューを選択するには、[グループ] の横にある下矢印をクリックして、[仮想マシン] を選択します。 ■ ビューに表示する特定のグループまたは仮想マシンを選択するには、[すべて] の横にある下矢印をクリックして、リストから選択します。 ■ 選択したフィルタをクリアするには、画面の右上にある [フィルタをクリア] をクリックします。仮想マシン ビューで [フィルタをクリア] をクリックすると、フィルタがクリアされ、グループ ビューが表示されます。 <p>2 つのビュー タイプの使用方法については、グループ ビューの操作と仮想マシン ビューの操作を参照してください。</p>
2	<p>[フィルタの適用] を使用すると、表示に使用する基準を調整できます。表示に使用する基準をドロップダウン リストから選択できます。仮想マシンのメンバー、タグ、フロー タイプ、送信元 IP、宛先 IP、ルール ID または名前を選択できます。[フィルタの適用] を再度クリックして、複数のフィルタを定義できます。</p>
3	<p>[フロー] セクションでは、選択期間内で表示するトラフィック フロー タイプを選択できます。このセクションでは、フロー タイプに使用される色も表示されます。</p> <ul style="list-style-type: none"> ■ [保護解除] フローには、赤色の破線が使用されます。 ■ [ブロック] フローには青色の実線が使用されます。 ■ [許可] フローには緑色の実線が使用されます。 <p>デフォルトでは、現在の NSX Intelligence の表示に [保護解除] のトラフィック フロー タイプが選択されます。詳細については、トラフィック フローの操作を参照してください。</p>
4	<p>表示モード セクションでは、表示に使用するテーマを定義します。ライト テーマがデフォルトのモードです。</p> <ul style="list-style-type: none"> ■ ダーク テーマ モードを使用するには、[ダーク] アイコンをクリックします。ダーク テーマは、全画面表示モードの場合にのみ使用できます。 ■ 全画面表示モードに切り替えるには、表示コントロール セクションで  をクリックします。

セクション	説明
5	<p>このセクションで選択した期間に基づいて、表示と推奨事項を生成するために使用されるネットワーク フロー データが決まります。選択内容によって、グループ ビューまたは仮想マシン ビューで使用される履歴データが決まります。期間は、現在の時間と過去の一定の期間に対応しています。</p> <p>デフォルトの時間範囲は直近 24 時間です。選択した期間を変更するには、現在選択されている期間をクリックして、[直近 1 時間]、[直近 12 時間]、[直近 24 時間]、[直近 1 週間] または [直近 1 か月] を選択します。</p>
6	<p>このアイコン  をクリックすると、[推奨] ダイアログ ボックスに現在のビューのインベントリ サマリが表示されます。仮想マシン ビューで [新しい推奨の開始] をクリックすると、NSX Intelligence の推奨事項を生成できます。NSX Intelligence 推奨事項の操作 を参照してください。</p>
7	<p>このセクションでは、オンプレミスの NSX-T Data Center にある グループまたは仮想マシンのセキュリティ状態が表示されます。選択期間中に発生したネットワーク トラフィック フローも表示されます。このセクションで特定のノードまたはフローの矢印をポイントすると、そのエンティティの詳細が表示されます。</p> <p>詳細については、NSX Intelligence グラフィック要素についてと NSX Intelligence のビューとフローについてを参照してください。</p>
8	<p>このセクションには、ズームイン、ズームアウト、1:1 縦横比の適用、ビューのサイズ調整、全画面表示モードへの切り替えを行うコントロールが表示されます。表示コントロールはキーボード ホットキーで管理することもできます。キーボード ショートカットのヘルプ ウィンドウを表示するには、[Shift +/] を押します。</p> <p>以前に表示されていた内容に戻すには、Web ブラウザの [戻る] ボタンを使用します。全画面表示モードで同様の操作を行うには、画面左上にある [戻る] をクリックします。</p>

NSX Intelligence グラフィック要素について

NSX Intelligence ユーザー インターフェイスでは、データセンターのエンティティ、トラフィック フロー、NSX-T Data Center 環境内の特定のアクティビティを視覚的に表示するため、いくつかのグラフィック要素が使用されています。

次の表に、NSX Intelligence に表示される NSX-T Data Center グラフィック要素を示します。

グラフィック要素	説明
	<p>このアイコンはグループを表します。グループは、セキュリティ ポリシーを適用できる仮想マシンのコレクションを表します。このセキュリティ ポリシーには、East-West ファイアウォール ルールも含まれます。グループ ビューの操作 を参照してください。</p>
	<p>このアイコンは、NSX-T Data Center 環境に存在する 1 台の仮想マシン (VM) を表します。1 台の仮想マシンが複数のグループに属している場合もあります。仮想マシン ビューの操作 を参照してください。</p>
	<p>このアイコンは、インターネットのパブリック IP を表します。選択期間内に NSX-T Data Center 環境の少なくとも 1 台の仮想マシンがパブリック IP と通信した場合、そのトラフィック フローは現在の表示に含まれます。</p>
	<p>選択期間内にネットワーク トラフィック アクティビティに参加したユニキャスト、ブロードキャスト、マルチキャスト IP などの IP アドレス。</p>

グラフィック要素	説明
 <p>未分類の仮想マ... (4)</p>	<p>このアイコンは、グループに属していない仮想マシンのグループに使用されます。</p>
	<p>矢印は、選択した期間に 2 台の仮想マシン間で発生したネットワーク トラフィックのフローを表します。3 種類の矢印があります。保護解除のフローは赤い点線の矢印、ブロックされたフローは青い実線の矢印、許可されたフローは緑の実線の矢印で示されます。トラフィック フローの操作 を参照してください。</p>
	<p>フォーカスで現在のノードとして選択されているノードは、点線の円で囲まれています。これは、選択モードで固定されたノードで、現在のビューで表示されます。</p>
	<p>選択期間内にグループが NSX-T Data Center インベントリに追加されると、このアイコンがグループ ノードの境界に表示されます。選択期間内に NSX-T Data Center が仮想マシンを検出すると、その仮想マシン ノードの境界にこのアイコンが表示されます。</p>
	<p>選択期間内にグループが削除され、仮想マシン メンバーが削除されなかった場合、このアイコンがグループ ノードの境界に表示されます。このアイコンが仮想マシン ノードの境界に表示されている場合、この仮想マシンは選択期間内に削除されています。仮想マシンまたはグループは削除されていますが、選択期間内に仮想マシンまたはグループが削除されたことを示す履歴ビューを提供するため、このアイコンが表示されています。</p>
	<p>グループと仮想マシンを一緒に表示している場合、このアイコンが表示されます。たとえば、詳細なグループ ビューや、グループに関連する仮想マシンで表示されます。</p> <p>このアイコンは、次の場合に仮想マシン ノードの境界に表示されます。</p> <ul style="list-style-type: none"> ■ 選択期間内に、仮想マシンが現在表示されているグループから移動した場合 ■ 選択期間のある時点で、仮想マシンが現在表示しているグループの一部であったが、そのグループのメンバーでなくなった場合

NSX Intelligence のビューとフローについて

NSX Intelligence では、グループまたは仮想マシン、および選択した期間にこれらのグループや仮想マシンで発生したネットワーク フローが視覚的に表示されます。

重要： 特定の期間内に NSX-T データセンターで発生したすべてのネットワーク フローとアクティビティが表示されます。アクティビティには、仮想マシンやグループの追加、削除、移動などが含まれます。1 台の仮想マシンが複数回表示される場合もあります。たとえば、選択した期間内に管理対象外の ESXi ホストに仮想マシンが接続し、そのホストが VMware vCenter Server™ の管理対象になった場合、この仮想マシンは仮想マシン ビューに 2 回表示されます。同様に、選択した期間内に ESXi ホストが vCenter Server から切断され、再度追加された場合、このホストに接続している仮想マシンは削除と新規の両方として表示されます。選択期間内に未分類グループの仮想マシンがグループに追加されると、その仮想マシンはグループ ビューで未分類グループと新しいグループの両方に表示されます。

NSX Intelligence は、仮想マシンのメンバー タイプのみを持つグループをサポートします。グループに他のタイプのメンバーが含まれている場合、グループ ビューには、セキュリティ ルールの実際のグループではなく、仮想マシンのメンバー タイプを持つグループ間の関連フローが表示されることがあります。

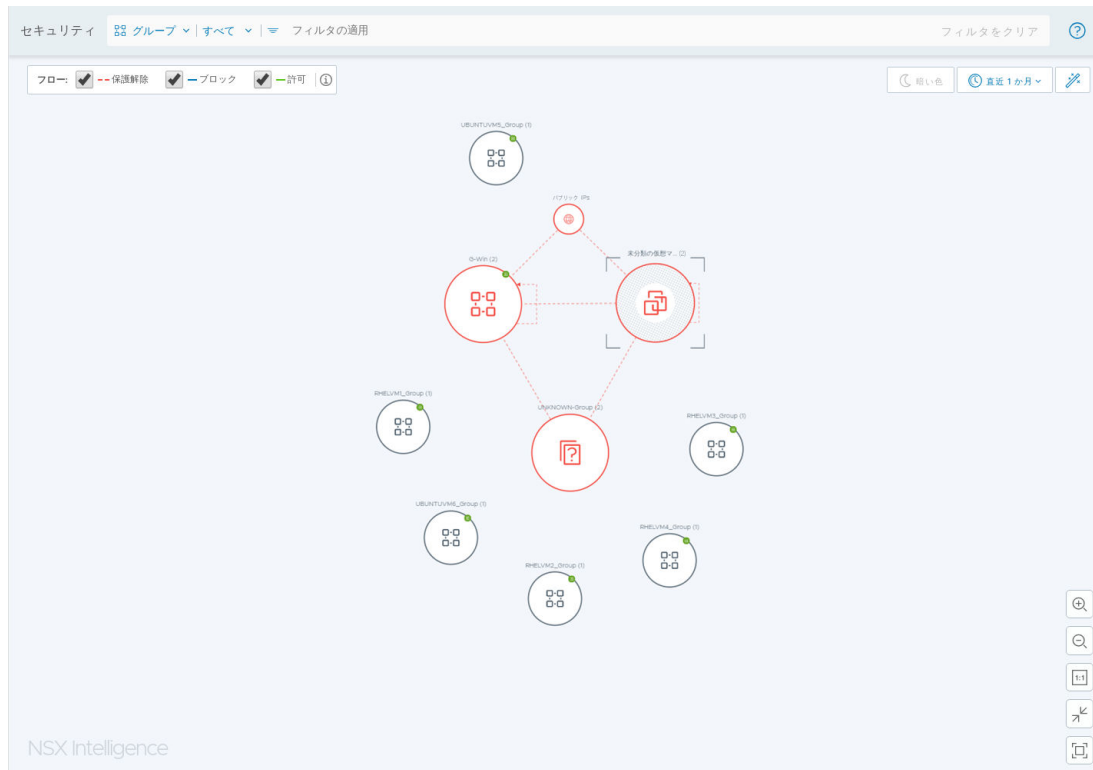
グループ ビュー、仮想マシン ビュー、さまざまなトラフィック フローの操作方法については、このセクションの情報を参照してください。

グループ ビューの操作

NSX Intelligence ホームページのデフォルト ビューはグループ ビューです。グループ ビューでは、直近の 24 時間に未保護のトラフィック フローが発生しているグループを表示するようにフィルタリングされます。

グループ ビューのノードと矢印

グループ ビューのノードは、仮想マシン、IP セットなど、NSX-T Data Center 環境内の NSX オブジェクトを表します。次のスクリーンショットは、グループ ビューの例を表しています。



次の表に、グループ ビューに表示されるグループ ノードの種類を示します。

グループ ノードの種類	アイコン	説明
通常グループ		NSX Intelligence の通常グループ ノードは、NSX-T Data Center 環境内の NSX オブジェクトのコレクションを表します。このリリースでは、これらの NSX オブジェクトは仮想マシンになります。NSX Intelligence は、仮想マシンのメンバー タイプのみから構成される通常グループをサポートします。1つの NSX オブジェクトが複数のグループに属している場合もあります。このため、1 台の仮想マシンが複数のグループ ノードに表示される場合があります。
未分類グループ		未分類グループ ノードは、どのグループにも属していない仮想マシンのコレクションを表します。
不明グループ		不明グループ ノードは、NSX-T Data Center インベントリで見つからなかったその他のオブジェクト セットを表します。ただし、これらのオブジェクトは、NSX-T Data Center 環境内の 1 つ以上の NSX オブジェクトと通信しています。
パブリック IP グループ		パブリック IP グループ ノードは、NSX-T Data Center 内の NSX オブジェクトと通信しているパブリック IP アドレス (IPv4 または IPv6) のコレクションを表します。

グループ ビューのノード サイズは、そのグループに属する NSX オブジェクト（仮想マシンなど）の数に基づきます。グループのノードが大きいくほど、そのグループに属している仮想マシンが多くなります。ノードの上にグループの名前と、そのグループに含まれるメンバー仮想マシンの合計数が表示されます。

グループ ノード間の矢印は、これらの接続されたグループ ノードの仮想マシン間で選択期間内に発生したトラフィック フローを表します。グループ ノードの自己参照矢印は、1 台以上の仮想マシンが同じグループ内の別の仮想マシンと通信していることを表します。詳細については、[トラフィック フローの操作](#)を参照してください。

赤い境界線のノードでは、選択期間内にグループの仮想マシンで保護解除のフローが発生しています。ブロックされたフローまたは許可されたフローの検出数は様々です。青い境界線のノードでは、選択期間内に保護解除のトラフィック フローが検出されていませんが、ブロックされたフローが1つ以上検出されています。許可されたフローの検出数は様々です。緑の境界線のノードでは、選択期間内に保護解除のフローまたはブロックされたフローは検出されていませんが、許可されたフローが1つ以上検出されています。灰色の境界線のノードでは、選択期間内にそのグループに属する仮想マシンのトラフィック フローが検出されていません。

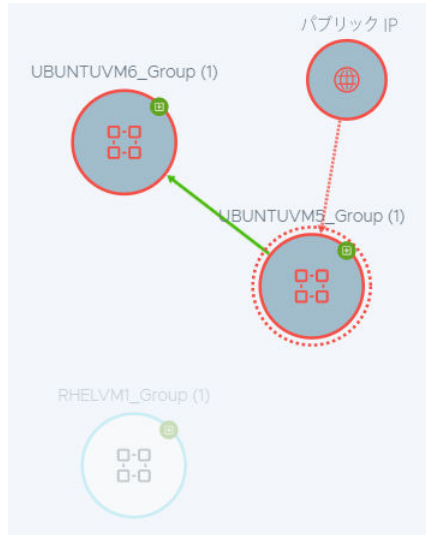
グループ ビューが表示されない場合は、[セキュリティ ビュー] 選択領域の [仮想マシン] の隣にある下矢印をクリックして、[グループ] を選択します。表示された選択ドロップ リストで、[すべてのグループ] を選択するか、リストから特定のグループを選択して、[適用] をクリックします。選択リストをフィルタリングするには、[検索] テキスト ボックスを使用します。何も選択せずに選択ドロップ リスト以外の場所をクリックするか、ドロップ リストから [すべてのグループ] を選択すると、グループ ビューに [すべてのグループ] オプションが適用されます。

グループ ビューでのノードの選択

グループのノードをポイントすると、グループに関する情報が表示されます。次の例では、グループ G-Win の情報が表示されています。選択期間内に検出されたフローの数とタイプも一覧表示されます。選択期間内にグループが追加された場合は、新しいバッジ アイコンと、グループ作成時の詳細も表示されます。



グループのノードをクリックすると、選択範囲が点線の円で囲まれ、固定されたグループ ノードとしてマークされます。選択したグループ ノードに接続している他のグループも分かりやすく表示されます。他のノードはすべて淡色表示になります。たとえば、次のスクリーンショットでは、UBUNTUVM5_Group ノードが選択され、選択期間内に UBUNTUVM5_Group とトラフィック フローを共有していた他のグループが強調表示されています。UBUNTUVM5_Group と通信していない他のすべてのグループはビューに表示されません。



選択内容の固定を解除するには、グループ ビューの空白領域をクリックします。

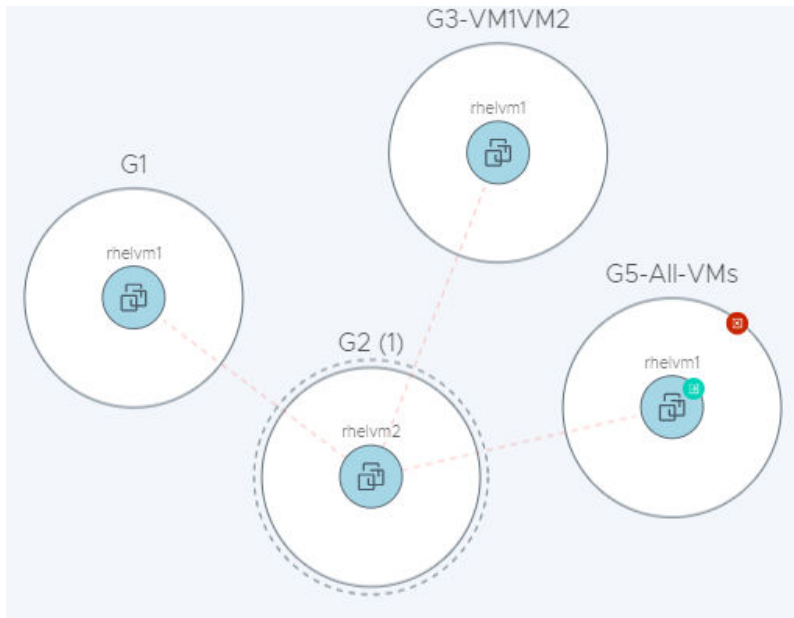
グループ ビューをズームアウトし、ノードの詳細が見えなくなった場合は、ノードの表示部分をポイントすると、詳細が表示されます。

グループ ビューで使用可能なアクション

グループのノードを右クリックすると、次の図のように、使用可能なアクションのコンテキスト メニューが表示されます。



- [詳細: Group_Name] を選択すると、選択したグループのノードが点線の円で囲まれ、固定グループ ノードになるか、現在のグループとしてフォーカスされます。グループに属する仮想マシンは、グループのノード内に表示されます。選択期間に固定グループの仮想マシンとトラフィック フローを共有していたグループもビューに表示されます。次の例では、グループ G2 が固定グループです。選択期間内にグループ G2 の仮想マシン メンバーで rhelm2 とのトラフィック フローが発生しているため、他のグループもビューに表示されています。



- [フィルタ基準] を選択すると、現在のグループ ビューに使用されている表示フィルタにグループが追加されます。
- [仮想マシン] を選択すると、選択した期間内に現在のグループに属していたすべての仮想マシンがテーブル形式で表示されます。[仮想マシンの表示] テーブルで、選択したグループに属する仮想マシンと、各仮想マシンが属する他のグループの詳細を確認できます。仮想マシンを現在の表示フィルタに追加するには、フィルタ アイコンをクリックします。
- [フローの詳細] を選択すると、次のスクリーンショットのように、現在選択されているグループのフロー詳細テーブルが表示されます。ここには、選択期間内に発生し、現在のグループに含まれる仮想マシンでアクティブになっているフローの詳細が表示されます。この詳細には、フロー タイプ、フローの送信元グループと宛先グループ、フローの開始時間と終了時間、使用されたサービスなどが表示されます。詳細情報の一部をクリックすると、より詳しい情報が表示されます。詳細については、[トラフィック フローの操作](#)を参照してください。

フローの詳細

🕒 直近 24 時間

×

未分類の仮想マシン のフローの詳細を表示しています

完了したフロー アクティブなフロー

検索

送信元	送信元グループ	宛先	宛先グループ	サービス	終了時間	最新のフロー
ubuntu12.04.1-2G-LA...	G5	ubuntu12.04-pa...	UNCATEGORIZED	SSH... さらに 2 件	2019/11/06 8:05	● 保護解除
ubuntu12.04.1-2G-LA...	G1	ubuntu12.04-pa...	UNCATEGORIZED	SSH... さらに 2 件	2019/11/06 8:05	● 保護解除

🔄 更新

1 - 2 of 2 フロー

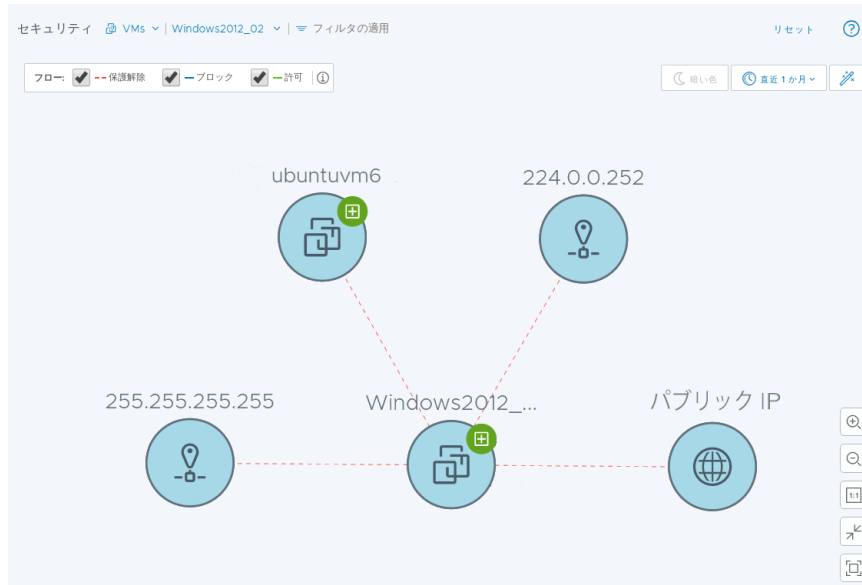
閉じる

仮想マシン ビューの操作

仮想マシン ビューのノードは、オンプレミスの NSX-T Data Center 環境内の仮想マシン (VM) を表します。

仮想マシン ビューのノードと矢印

仮想マシン ビューでは、グループの境界が表示されません。NSX-T Data Center 環境内のいずれかの仮想マシンと通信していて、NSX-T Data Center インベントリに属していないと判断されたノードも、仮想マシン ビューに表示されます。次に、シンプルな仮想マシン ビューを示します。



次の表に、ビューに表示される仮想マシン ノードの種類を示します。

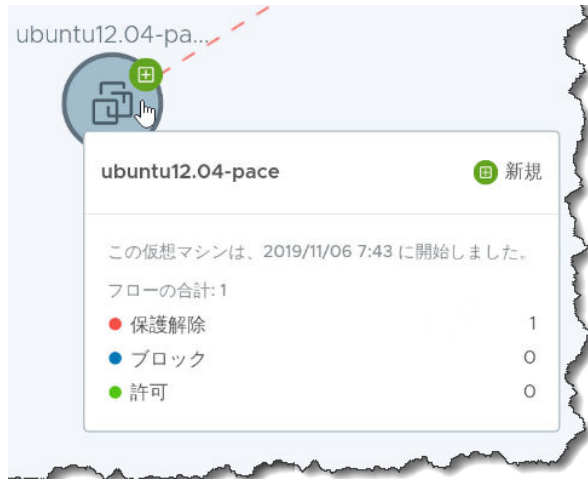
仮想マシン ノードの種類	アイコン	説明
通常の仮想マシン		通常の仮想マシン ノードは、NSX-T Data Center 環境内に存在する 1 台の仮想マシン (VM) を表します。1 台の仮想マシンが複数のグループに属している場合もあります。
パブリック IP		パブリック IP ノードは、NSX-T Data Center 環境と通信を行っているパブリック IP アドレス (IPv4 または IPv6) を表します。
IP アドレス		IP ノードは、選択期間にネットワーク トラフィック アクティビティに参加した IP アドレスを表します。この IP アドレスは、ユニキャスト IP、ブロードキャスト IP、マルチキャスト IP の場合があります。

仮想マシン ビューが表示されない場合は、[セキュリティ ビュー] 選択領域の [グループ] の隣にある下矢印をクリックして、[仮想マシン] を選択します。表示された選択ドロップ リストで、[すべての仮想マシン] を選択するか、リストから特定の仮想マシンを選択して、[適用] をクリックします。選択リストをフィルタリングするには、[検索] テキスト ボックスを使用します。何も選択せずに選択ドロップ リスト以外の場所をクリックするか、ドロップ リストから [すべての仮想マシン] を選択すると、仮想マシン ビューに [すべての仮想マシン] オプションが適用されます。

仮想マシン ノード間の矢印は、選択期間内に仮想マシン間で発生したトラフィック フローを表します。詳細については、[トラフィック フローの操作](#)を参照してください。

仮想マシン ビューでのノードの選択

仮想マシン ノードをポイントすると、次の例のように、ノードに関する情報が表示されます。選択期間内に検出された仮想マシンのフロー数と種類も表示されます。選択期間内にグループが追加された場合、新しいバッジ アイコンと、仮想マシンの追加先に関する詳細が表示されます。



仮想マシンのノードをクリックすると、選択範囲が点線の円で囲まれ、固定された仮想マシン ノードとしてマークされます。仮想マシン ビューでは、固定された仮想マシン ノードとトラフィック フローを共有している他の仮想マシン ノードも分かりやすく表示されます。他のノードはすべて淡色表示になり、見づらくなります。選択内容の固定を解除するには、仮想マシン ビューの空白領域をクリックします。

仮想マシン ビューをズームアウトし、仮想マシン ノードの詳細が見えなくなった場合は、仮想マシン ノードの表示部分をポイントすると、詳細が表示されます。

仮想マシン ビューで使用可能なアクション

仮想マシンのノードを右クリックすると、次の図のように、使用可能なアクションのコンテキスト メニューが表示されます。






選択	説明
[フィルタ基準]	現在の仮想マシン ビューに使用されている表示フィルタに仮想マシンが追加されます。
[仮想マシン情報]	選択期間内の仮想マシンの詳細が表示されます。
[関連グループ]	選択期間内に仮想マシンが属していたグループの情報がグループ テーブルに表示されます。
[フローの詳細]	<p>選択期間内に仮想マシンでアクティブになっているフローの詳細が表示されます。次の情報が含まれます。</p> <ul style="list-style-type: none"> ■ フロー タイプ ■ フローの送信元と宛先のグループ ■ フローの開始時刻と終了時刻 ■ 使用されたサービス <p>詳細情報の一部をクリックすると、より詳しい情報が表示されます。詳細については、トラフィック フローの操作を参照してください。</p>
[推奨の開始]	新しい推奨開始ウィザードを表示します。詳細については、 NSX Intelligence 推奨事項の操作 を参照してください。

トラフィック フローの操作

グループ ノードまたは仮想マシン ノード間の矢印は、選択した期間内に仮想マシン間で発生したネットワーク トラフィック フローを表します。

ネットワーク トラフィック フローは、設定されている L3 分散ファイアウォール (DFW) ルールと、選択期間内に発生したトラフィック フローに基づきます。IPv4 または IPv6 と TCP、UDP、GRE、ESP、SCTP プロトコルを使用して、ステートフル L3 分散ファイアウォール ルールに一致するすべてのネットワーク トラフィック フローの詳細が表示されます。TCP または UDP フローの場合、IP とポート レベルの詳細があり、他のフローの場合、IP レベルでのみ詳細のみが表示されます。

トラフィック フローは次のタイプに分類されます。

フロー タイプ	グラフィック	説明
保護解除		赤い点線の矢印は、トラフィック フローがルール（送信元：任意 宛先：任意 アクション：許可、却下またはドロップ）を満たし、よりきめ細かいセキュリティ ポリシーが必要であることを表します。このルールは、デフォルトのルールにすることも、East-West 分散ファイアウォールの任意の場所に配置することもできます。
ブロック		青い実線の矢印は、「保護解除」のフロー定義よりもきめ細かい「却下」または「ドロップ」のルールに一致するトラフィック フローが検出されたことを意味します。
許可		緑色の実線の矢印は、「保護解除」のフロー定義よりもきめ細かい「許可」ルールに一致するトラフィック フローが検出されたことを表します。

特定のタイプのトラフィック フローに関連するオブジェクトにのみフォーカスを移動するには、セキュリティ ビューの選択領域でビューのタイプを選択し、フロー タイプ フィルタ属性を使用して選択を絞り込みます。

フロー タイプの選択を解除すると、表示されているグラフからそのフロー タイプのフロー線が表示されなくなります。特定のオブジェクトを除外フィルタが有効になっている場合を除き、これらのオブジェクトで選択期間内に発生したトラフィック フロー タイプに関係なく、すべてのグループまたは仮想マシン オブジェクトが表示されたままになります。たとえば、「許可」フロー タイプの選択を解除すると、すべての「許可」フローの線がグラフから消えます。ただし、オブジェクトで選択期間内に「許可」トラフィック フローのみが発生した場合でも、すべてのオブジェクトが表示されます。

フローの矢印の方向は、検出されたトラフィック フローの送信元と宛先を表します。グループ ビューの場合、グループ ノードの自己参照矢印は、1 台以上の仮想マシンが同じグループ内の別の仮想マシンと通信していることを表します。仮想マシン ビューの自己参照矢印は、仮想マシン内の NSX オブジェクトが同じ仮想マシン内の別の NSX オブジェクトと通信していることを表します。

フローの矢印をポイントすると、グループまたは仮想マシンに関連する情報が表示されます。次の例では、グループ G2 に関する情報が表示されています。



フロー矢印をクリックすると、[フローの詳細] ダイアログ ボックスが表示されます。選択した期間内に発生したフロー（完了したフローとアクティブなフロー）に関する詳細が表示されます。フローの送信元、宛先、サービスのタイプ、フローの種類に関する詳細を表示するには、テーブルのリンクをクリックします。

NSX Intelligence 推奨事項の操作

NSX Intelligence は、選択した期間内に NSX-T Data Center 環境の仮想マシン間で発生したトラフィック フローのパターンに基づいてマイクロセグメンテーションの推奨を提供します。

NSX Intelligence の推奨事項について

NSX Intelligence が生成する推奨事項には、セキュリティ ポリシー、ポリシー セキュリティ グループ、アプリケーションのサービスが含まれます。

推奨事項は、vCenter Server で管理されている ESXi ホストの仮想マシン ワークロード間のネットワーク トラフィック フローのパターンに基づいています。NSX-T Data Center 環境内で発生した通信トラフィック パターンを関連付けることで、より動的なセキュリティ ポリシーを適用できます。

セキュリティ ポリシーの推奨事項は、アプリケーション カテゴリの East-West 分散ファイアウォール セキュリティ ポリシーです。セキュリティ グループの推奨事項は、指定した期間と仮想マシン境界で分析されたネットワーク トラフィック フローに表示される仮想マシンのリストで構成されます。サービスの推奨事項は、指定した仮想マシンのアプリケーションによって特定のポートで使用され、NSX-T Data Center インベントリに定義されていないサービス オブジェクトです。

推奨事項を取得する方法は複数ありますが、[プランとトラブルシューティング] - [推奨] タブの順にクリックし、[新しい推奨の開始] をクリックするのが最も簡単な方法です。アプリケーション境界を構成する仮想マシン (VM) と、これらの仮想マシンでネットワーク トラフィック フローが分析される期間を指定します。推奨事項の分析が完了したら、推奨事項の詳細を表示し、必要に応じて変更してから発行することができます。詳細については、[新しい NSX Intelligence の推奨事項の生成](#)を参照してください。

新しい NSX Intelligence の推奨事項の生成

NSX Intelligence 推奨機能は、アプリケーションのマイクロセグメント化に役立つ推奨事項を提供します。

NSX Intelligence の推奨事項を生成すると、セキュリティ ポリシー、ポリシー セキュリティ グループ、アプリケーションのサービスの推奨事項が生成されます。推奨事項は、NSX-T Data Center の仮想マシン間で発生している通信トラフィックのパターンに基づいて作成されます。NSX Intelligence UI では、いくつかの方法で推奨事項を生成できます。以下では、3 つの方法について説明します。

前提条件


NSX Intelligence をインストールします。『NSX-T Data Center インストール ガイド』の「NSX Intelligence のインストールと設定」を参照してください。

手順

- 1 ブラウザから、エンタープライズ管理者の権限で NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。

2 新しい推奨事項の生成を開始します。

次の表を参照して、使用する方法を決めてください。

方法	手順
[プランとトラブルシューティング] - [推奨] の順に選択します。	[新しい推奨の開始] をクリックします。
仮想マシン ビューで、仮想マシンを選択して右クリックします。	コンテキスト メニューから [新しい推奨の開始] を選択します。
[プランとトラブルシューティング] - [検出とアクションの実行] の順に選択します。	<ol style="list-style-type: none"> [セキュリティ状態] フィルタで下矢印をクリックし、[仮想マシン] を選択します。 アプリケーションの境界を構成する仮想マシンを選択して、[適用] をクリックします。 推奨を表す、杖の形のアイコン  をクリックします。 [推奨] ダイアログ ボックスで、[新しい推奨の開始] をクリックします。

3 [新しい推奨の開始] ウィザードで、必要に応じて [推奨名] のデフォルト値を変更します。

4 セキュリティ ポリシーの推奨の境界として使用する仮想マシンを定義または変更します。

- [仮想マシンの選択] をクリックするか、[選択した仮想マシン] の数をクリックします。
- [仮想マシンの選択] ダイアログ ボックスで、分析の境界として使用する仮想マシンを選択します。追加しない仮想マシンは選択を解除します。

推奨の境界には、最大 100 台までの仮想マシンを選択できます。選択バーに名前を入力して、選択する仮想マシンをフィルタリングすることもできます。

- [保存] をクリックします。

選択した仮想マシンの数が [新しい推奨事項の検出] ダイアログ ボックスに表示されます。

5 推奨の分析に使用する [説明] と [時間範囲] のデフォルト値を変更するには、[その他のオプション] を展開します。デフォルトの [時間範囲] の値は直近 1 か月です。選択した仮想マシン間で直近 1 か月に発生したネットワーク トラフィック フローが推奨の分析に使用されます。

6 [検出の開始] をクリックします。

推奨は順番に処理されます。保留中の推奨があるかどうかによりますが、各推奨が完了するまでに平均で 3 ～ 4 分ほどかかります。分析が必要な仮想マシン間で多くのトラフィック フローが発生している場合、推奨の生成に 10 ～ 15 分ほどかかる場合があります。ステータスは、[推奨] タブで追跡できます。状態が 待機中 から 分析中 に変わり、最後に 発行の準備完了 になります。次のスクリーンショットでは、ステータスの異なる 3 つの推奨事項が生成されています

推奨事項 ?					
新しい推奨の開始		名前、パスなどでフィルタリング 			
	名前	状態	仮想マシン	作成時間	最終更新日
⋮ >	REC 20191107 10:09:19	使用可能な推奨事項はありません	6	2019/11/07 2:09	2019/11/07 2:09
⋮ >	REC 20191106 16:39:30	使用可能な推奨事項はありません	1	2019/11/06 8:39	2019/11/06 8:39
⋮ >	REC 20191106 16:15:53	使用可能な推奨事項はありません	1	2019/11/06 8:16	2019/11/06 8:16

推奨が正常に発行されると、ステータスが発行済みに変わります。

次のステップ

生成された推奨事項を確認し、発行するかどうかを決定します。[生成された推奨事項の確認と発行](#) を参照してください。

生成された推奨事項の確認と発行

生成された NSX Intelligence の推奨事項が「発行の準備完了」状態になったら、推奨事項を確認し、必要に応じて変更を行い、発行するかどうかを決めます。

前提条件

新しい推奨事項を生成します。[新しい NSX Intelligence の推奨事項の生成](#) を参照してください。

手順

- 1 ブラウザから、エンタープライズ管理者の権限で NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 [プランとトラブルシューティング] - [推奨] の順にクリックします。
- 3 表示される推奨のリストを絞り込むには、画面の右上にある [名前、パスなどでフィルタリング] をクリックして、使用するフィルタ条件を指定します。
- 4 推奨事項を使用しない場合は、3 つのドットで示されるメニュー アイコンをクリックして、[削除] を選択します。
- 5 推奨事項のサマリを表示するには、推奨名の横にある矢印をクリックして、行を展開します。
生成されたルールの数と、影響を受けるグループの数が表示されます。
- 6 推奨事項の詳細を確認して、管理します。
 - a 推奨名をクリックします。

次の図のように、[推奨] ウィザードが表示されます。

Recommendations

REC 20190719 15:59:02

Showing discovered recommendations. Review, Edit and Proceed with your selections to place the rules in the existing Firewall context.

Recommended FW Rules Recommended Groups Recommended Services

Category: Application Recommended Rules: 6 Recommended Groups: 3 Recommended Services: 0

Name	Sources	Destinations	Services	Profiles	Applied To	Action	
Policy-1 (REC 20190719 15:59:02)	(6)						
Rule-1 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	Win - RPC, DCOM, EP...	None	DFW	Allow	On
Rule-2 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBDS-Broadcast-V1	None	DFW	Allow	On
Rule-3 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCP-Server	None	DFW	Allow	On
Rule-4 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCPv6 Server	None	DFW	Allow	On
Rule-5 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBNS-Broadcast-V1	None	DFW	Allow	On
Rule-6 (REC 20190719 15:59:02)	Group-2 (REC 20190719 15:59:02)	Group-3 (REC 20190719 15:59:02)	SSH	None	Group-2 (REC 20190719 15:59:02)	Allow	On

1 of 1 Policy

CANCEL CONTINUE LATER NEXT

- b [推奨ファイアウォール ルール] タブで、ファイアウォール ルールの詳細を確認します。詳細を変更するには、該当する列の値をクリックして、編集（鉛筆）アイコンを選択します。

- c バケットの処理方法を定義するには、[アクション] 列で [許可]、[ドロップ] または [却下] を選択します。
 - d 右側のボタンを使用して、ルールを有効または無効にします。前の手順のイメージのように、デフォルトでは、生成されたルールは発行時に有効に設定されます。
 - e [推奨グループ] をクリックします。
 - f [メンバー] 列のリンクをクリックして、グループ推奨に設定された仮想マシンと IP の詳細情報を確認します。
 - g グループ名の横にあるメニュー アイコン (3 つのドット) をクリックし、[編集] を選択してグループの推奨を変更します。
 - h [推奨サービス] をクリックして、詳細を確認します。
 - i サービス名の横にあるメニュー アイコン (3 つのドット) をクリックし、[編集] を選択して説明または名前を変更します。サービスを削除する前に、サービスを使用しているルールがないことを確認してください。
 - j [次へ] をクリックします。
- 7 [ファイアウォール コンテキストにルールを追加] ペインで、既存のファイアウォール ルールにルールの推奨を適用する順序を変更できます。強調表示されているセクションをドラッグします。または、3 つのドットで示されているメニュー アイコンをクリックして、[選択したセクションの上へ移動] または [選択したセクションの下へ移動] を選択します。
- 8 [発行] をクリックします。
- 9 [推奨の公開] ダイアログ ボックスで、[はい] をクリックします。
- 10 [適用のサマリ] ページで、セキュリティ ポリシーが正常に発行されていることを確認し、[閉じる] をクリックします。

推奨の表で、推奨の [ステータス] 列が [発行済み] に変更されます。

結果

セキュリティ ポリシーの推奨が正常に発行されると、これらの推奨は [プランとトラブルシューティング] - [推奨] タブで読み取り専用になります。発行済みのルールの推奨を表示または管理するには、[セキュリティ] - [分散ファイアウォール] の順に移動します。

重要： 推奨ルールを発行した後も、関連する仮想マシン間で新しいフローが生成されるまで、影響する仮想マシン間のフローがオレンジ色の矢印（保護解除のフロー）で表示されます。この表示では、ホスト上で発生した時間に基づいてトラフィック フローが報告されるだけで、これらのトラフィック フローが発生した後に発行されたルール セットは反映されていません。ルール セットが発行され、新しいトラフィック フローが生成されると、新しいフローは緑色の矢印（許可されたフロー）で表示されます。

NSX Intelligence のバックアップとリストア

現在の NSX Intelligence 構成が動作不能になった場合や、以前の状態にリストアする場合は、バックアップから構成をリストアできます。バックアップとリストアのワークフローは、NSX Intelligence CLI を使用した場合にのみサポートされます。

バックアップを作成する場合、NSX Intelligence は NSX Intelligence アプライアンスを構成するすべてのサービスで使用される設定ファイルのみをバックアップします。バックアップに可視化データは含まれません。

NSX Intelligence でデータの損失や破損が発生すると、関連するフローと推奨に関するすべての既存データが失われます。NSX Intelligence を再インストールすると、ネットワーク トラフィック データの収集が再開され、その時点以降に収集されたデータの表示が可能になります。

バックアップの設定が完了したら、必要なときに NSX Intelligence アプライアンスでバックアップ コマンドを手動で実行できます。バックアップには暗号化と圧縮が行われ、バックアップの設定時に定義されたりモート サーバに保存されます。バックアップを作成すると、ファイル名が一意になるように、バックアップ ファイルの作成日時がバックアップ ファイル名に追加されます。例：config-backup-2019-06-21T21_06_07UTC.tar.gz

NSX Intelligence バックアップをリストアすると、バックアップが作成されたときの構成状態がリストアされます。バックアップ ファイルを作成した NSX Intelligence アプライアンスと同じバージョンの NSX Intelligence アプライアンスにバックアップをリストアする必要があります。既存の NSX Intelligence アプライアンスや新しくインストールされた NSX Intelligence アプライアンスにもリストアできますが、その場合は、バックアップした NSX Intelligence アプライアンスと同じバージョンを使用する必要があります。

NSX Intelligence のバックアップの設定

NSX Intelligence の構成をバックアップする前に、バックアップ ファイル サーバを設定する必要があります。バックアップ ファイル サーバを設定した後は、いつでも NSX Intelligence のバックアップを作成できます。

前提条件

- NSX Intelligence CLI に対する CLI 管理者認証情報を確認します。
- リモート サーバのユーザー名とパスワードを確認します。
- リモート サーバでバックアップ ファイルを保存する場所のファイル パスを取得します。

手順

- 1 コマンドライン プロンプトから、NSX Intelligence CLI ホストに管理者権限でログインします。

```
$ ssh admin@cli-ip-address
admin@cli-ip-address's password:
```

- 2 バックアップ ファイル サーバを設定します。

コマンド構文は次のとおりです。

```
set backup remote-host remote_host_address remote-path remote_folder_path remote-host-username remote_host_username remote-host-password remote_host_password passphrase
pass_phrase
```

remote_host_address は、リモート ホストの IP アドレスまたはバックアップ ファイル サーバの FQDN アドレスです。remote_host_username アカウントには、remote_folder_path にバックアップ ファイルを作成するための権限が必要です。passphrase パラメータには、堅牢な値を指定する必要があります。少なくとも 8 文字以上にし、大文字、小文字、特殊文字をそれぞれ 1 個以上含める必要があります。次はその例です。

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

3 設定を確認します。

```
get configuration
```

出力で、set backup を含む行が正しいことを確認します。前の手順の例では、出力に次の行が含まれている必要があります。

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

NSX Intelligence のバックアップ

CLI コマンドを使用して、NSX Intelligence アプライアンスの設定ファイルをバックアップできます。

前提条件

- NSX Intelligence CLI に管理者権限でアクセスできることを確認します。
- バックアップ ファイル サーバを設定します。[NSX Intelligence のバックアップの設定](#) を参照してください。

手順

- 1 NSX Intelligence CLI サーバに管理者権限でログインします。
- 2 バックアップを作成します。

```
backup intelligence configuration
```

バックアップに成功すると、次のようなメッセージが表示されます。

```
Backup Complete. Archived at: backup_file_server-IP_address:/root/backup_archives/
intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 別の CLI セッションを使用して、バックアップの状況を確認できます。
 - a 別の NSX Intelligence CLI セッションにログインします。
 - b 次のコマンドを入力します。

```
get log-file node-mgmt.log follow
```

NSX Intelligence の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、バックアップが作成された時点の NSX Intelligence 構成の状態がリストアされます。NSX Intelligence のバックアップは、CLI コマンドでリストアできます。

リストアするバックアップと同じバージョンの NSX Intelligence アプライアンスに、バックアップをリストアする必要があります。デフォルトでは、最後に生成されたバックアップ ファイルがリストアされます。新しくインストールした NSX Intelligence アプライアンスにバックアップをリストアする場合は、バックアップをリストアする前にアーカイブ名を設定します。

前提条件

- バックアップ ファイル サーバの管理ログイン認証情報とホスト情報を入手していることを確認します。
- NSX Intelligence CLI に管理者権限でアクセスできることを確認します。

手順

- 1 新しい NSX Intelligence CLI サーバに管理者権限でログインします。
- 2 バックアップが存在するリモート サーバを設定します。

コマンド構文は次のとおりです。

```
set restore remote-host backup_server_IP_address remote-path remote_folder_path remote-host-username remote_host_username remote-host-password remote_host_password passphrase pass_phrase
```

backup_server_IP_address は、リモート ホストの IP またはバックアップ ファイル サーバの FQDN アドレスです。remote_host_username アカウントには、remote_folder_path のバックアップ ファイルにアクセスするための権限が必要です。次はその例です。

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

- 3 リストアの設定を確認します。

```
get configuration
```

出力で、set restore を含む行が正しいことを確認します。前の手順の例では、出力に次の行が含まれている必要があります。

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

- 4 次のコマンドを実行して、バックアップをリストアします。

```
restore intelligence configuration
```

リストアに成功すると、次のようなメッセージが表示されます。

```
NSX Intelligence Restore Complete.
```

5 別の CLI セッションを使用して、バックアップのリストア状況を確認できます。

- a 別の NSX Intelligence CLI セッションにログインします。
- b 次のコマンドを入力します。

```
get log-file node-mgmt.log follow
```

NSX Intelligence の問題のトラブルシューティング

NSX Intelligence アプライアンスが応答しなくなった場合や、アプライアンスの使用中に受信したエラー メッセージについて詳細な情報が必要な場合は、特定のコマンドを実行して NSX Intelligence サービスの状態を確認できます。

また、VMware のサポート担当者が問題のデバッグを行えるように、サポート バンドルを収集することもできます。

NSX Intelligence アプライアンスの状態の確認

たとえば、NSX Intelligence アプライアンスが応答しなくなった場合は、NSX Intelligence サービスの状態を確認します。

問題

NSX Intelligence アプライアンスが応答しなくなりました。あるいは、アプライアンスが予期したとおりに機能していないことを示すエラー メッセージが表示されました。

原因

基盤となる 1 つ以上の NSX Intelligence サービスが停止しているか、良好な状態でない可能性があります。

解決方法

- 1 エンタープライズ管理者ロールを持つアカウントを使用して、NSX Intelligence アプライアンスの CLI ホストにログインします。
- 2 `get services` コマンドを使用して、NSX Intelligence の状態を確認します。

すべての NSX Intelligence サービスが正常に機能している場合は、次のような出力が表示されます。

```
my_nsx-intel> get services
Service name:          druid
Service state:         running
Coordinator health:    good
Broker health:         good
Historical health:     good
Overlord health:       good
MiddleManager health:  good

Service name:          http
Service state:         running
Session timeout:       1800
Connection timeout:    30
```

```

Redirect host:                (not configured)
Client API rate limit:       100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:                 kafka
Service state:                running
Service health:               good

Service name:                 liagent
Service state:                stopped

Service name:                 mgmt-plane-bus
Service state:                stopped

Service name:                 node-mgmt
Service state:                running

Service name:                 nsx-config
Service state:                running

Service name:                 nsx-message-bus
Service state:                stopped

Service name:                 nsx-upgrade-agent
Service state:                running

Service name:                 ntp
Service state:                running
Start on boot:                True

Service name:                 pace-server
Service state:                running

Service name:                 postgres
Service state:                running
Service health:               good

Service name:                 processing
Service state:                running

Service name:                 snmp
Service state:                stopped
Start on boot:                False

Service name:                 spark
Service state:                running
Service health:               good

Service name:                 spark-job-scheduler
Service state:                running

Service name:                 ssh
Service state:                running
Start on boot:                True

```



```

Service name:          syslog
Service state:         running

Service name:          ui-service
Service state:         running

Service name:          zookeeper
Service state:         running
Service health:        good

my_nsx-intel>

```

サービスの状態は、running か stopped のいずれかです。サービスの健全性は、good または degraded です。

- また、syslog ファイルで pace-monitor.sh サービスの健全性チェック スクリプトの出力を検索できます。このスクリプトは、NSX Intelligence サービスの健全性を syslog ファイルに記録します。

すべてのサービスが予期したとおり機能している場合は、`get log-file syslog | find pace-monitor` コマンドを実行した後に次のような出力が表示されます。

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - -      "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -      "href": "/"
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -      "rel":
"self"
<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - -      },
<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - -      "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - -      "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",
<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - -      "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - -      "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - -      },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - -      "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - -      {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -
"druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -
"broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -
"coordinator": "good",

```

```

<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - - "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED -
Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - - }

```

```
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor
```

いずれかのサービスに問題がある場合、`get log-file syslog | grep pace-monitor`を実行すると、次の行が出力されることがあります。

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

- 4 次のいずれかの出力が表示された場合、`restart service service-name` コマンドを実行してサービスを再起動します。

- `get services` コマンドの実行後、サービスの1つが `Service state: stopped` または `Service health: degraded` になります。
- `get log-file syslog | grep pace-monitor` コマンドの実行後、出力に `PACE health DEGRADED.Return code not HTTP OK.` というメッセージが表示されます。

たとえば、`postgres` サービスの状態が `stopped` または `running` で、サービスの健全性が `degraded` の場合は、次のコマンドを実行します。

```
restart service postgres
```

重要： NSX Intelligence サービスを再起動するには、`restart service service-name` コマンドを使用する必要があります。`stop service service-name` と `start service service-name` コマンドを使用する場合は、`service-name` に依存するサービスを手動で再起動する必要があります。次のリストに、NSX Intelligence サービスの再起動が必要な依存関係の順序を示します。

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-
server
```

たとえば、停止していた `nsx-config` サービスを `stop|start service service-name` コマンドで開始した場合、`restart service service-name` コマンドを使用して `processing` と `pace-server` サービスも再起動する必要があります。

さらに、`restart service service-name` コマンドを使用して、依存関係の順序リストにあるサービスを `spark-job-scheduler` サービスより前に再起動する場合は、`restart service spark-job-scheduler` コマンドを使用して、`spark-job-scheduler` サービスを手動で再起動する必要があります。この操作を行わないと、`spark-job-scheduler` サービスが問題のある状態になります。

NSX Intelligence サポート バンドルの収集

サポート バンドルは、NSX Intelligence CLI で収集できます。

サポート バンドル ファイルの内容にはデータが含まれていません。次のディレクトリのファイルが含まれます。

- /opt/vmware/*
- /var/log/*
- /etc/*
- システム状態 (journalctl と systemctl を使用)

前提条件

NSX Intelligence CLI にエンタープライズ管理者権限でアクセスできることを確認します。

手順

- 1 エンタープライズ管理者ロール権限を持つアカウントを使用して、NSX Intelligence CLI にログインします。
- 2 サポート バンドルを生成します。

コマンドの構文は次のとおりです。ここでは、support_filename.tgz の値を指定します。

```
get support-bundle file support_filename.tgz
```

次はその例です。

```
get support-bundle file support_bundle123.tgz
```

バンドル ファイルが正常に作成されると、次のようなメッセージが表示されます。

```
support_bundle123.tgz created, use the following command to transfer the file: copy file
support_bundle123.tgz url <url> After transferring support_bundle123.tgz, extract it
using:tar xvf support_bundle123.tgz
```

- 3 次のコマンドを使用して、サポート バンドルが存在することを確認します。

```
get files
```

次のような出力が表示されます。

```
Directory of filestore:/
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```