

NSX 管理ガイド

Update 3

変更日：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

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

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

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

docfeedback@vmware.com

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

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

Copyright © 2010 – 2017 VMware, Inc. All rights reserved. [著作権および商標](#).

内容

NSX 管理ガイド 8

1 NSX のシステム要件 9

2 NSX で必要となるポートおよびプロトコル 11

3 NSX の概要 14

NSX コンポーネント 15

NSX Edge 18

NSX Services 21

4 Cross-vCenter Networking and Security の概要 23

Cross-vCenter NSX の利点 23

Cross-vCenter NSX の仕組み 24

Cross-vCenter NSX での NSX Services のサポート マトリックス 25

ユニバーサル コントローラ クラスター 27

ユニバーサル トランスポート ゾーン 27

ユニバーサル論理スイッチ 27

ユニバーサル分散論理ルーター 27

ユニバーサル ファイアウォール ルール 28

ユニバーサル ネットワークとセキュリティ オブジェクト 28

Cross-vCenter NSX トポロジ 29

NSX Manager ロールの変更 32

5 トランスポート ゾーン 34

トランスポート ゾーンの追加 36

トランスポート ゾーンを表示と編集 38

トランスポート ゾーンの拡張 38

トランスポート ゾーンの縮小 39

6 論理スイッチ 40

論理スイッチの追加 41

論理スイッチへの仮想マシンの接続 46

論理スイッチの接続のテスト 46

論理スイッチでのなりすましの防止 47

論理スイッチの編集 47

論理スイッチのシナリオ 47

- 7 ハードウェア ゲートウェイの設定 53
 - シナリオ：ハードウェア ゲートウェイのサンプル構成 54
- 8 L2 ブリッジ 60
 - L2 ブリッジの追加 61
 - 論理的にルーティングされた環境への L2 ブリッジの追加 61
- 9 ルーティング 63
 - 論理（分散）ルーターの追加 63
 - Edge Services Gateway の追加 77
 - グローバル設定の指定 87
 - NSX Edge 設定 89
 - スタティック ルートの追加 106
 - 論理（分散）ルーター上での OSPF の設定 107
 - Edge Services Gateway 上での OSPF の設定 114
 - BGP の設定 120
 - IS-IS プロトコルの設定 124
 - ルート再配分の設定 126
 - NSX Manager ロケール ID の表示 127
 - ユニバーサル分散論理ルーター上でのロケール ID の設定 127
 - ホストまたはクラスタ上でのロケール ID の設定 128
- 10 論理ファイアウォール 129
 - Distributed Firewall 129
 - Edge ファイアウォール 131
 - ファイアウォール ルール セクションの操作 132
 - ファイアウォール ルールの使用 134
 - ファイアウォールによる保護からの仮想マシンの除外 147
 - 仮想マシンの IP 検出 148
 - ファイアウォール CPU イベントおよびメモリしきい値イベントの表示 149
 - ファイアウォール ログ 150
 - NSX Edge ファイアウォール ルールの使用 152
- 11 Identity Firewall の概要 161
 - Identity Firewall のワークフロー 162
- 12 Active Directory ドメインの操作 163
 - NSX Manager への Windows ドメインの登録 163
 - Windows ドメインと Active Directory の同期 165
 - Windows ドメインの編集 165
 - Windows 2008 で読み取り専用セキュリティ ログ アクセスを有効にする 166
 - ディレクトリ権限の確認 166

- 13 SpoofGuard の使用 168
 - [SpoofGuard ポリシーの作成](#) 169
 - [IP アドレスの承認](#) 169
 - [IP アドレスの編集](#) 170
 - [IP アドレスのクリア](#) 171
- 14 Virtual Private Network (VPN) 172
 - [SSL VPN-Plus の概要](#) 172
 - [IPSec VPN の概要](#) 199
 - [L2 VPN の概要](#) 206
- 15 論理ロード バランサ 216
 - [ロード バランシングの設定](#) 216
 - [アプリケーション プロファイルの管理](#) 234
 - [サービス モニターの管理](#) 236
 - [サーバ プールの管理](#) 237
 - [仮想サーバの管理](#) 238
 - [アプリケーション ルールの管理](#) 239
 - [NTLM 認証を使用する Web サーバのロード バランシング](#) 240
 - [NSX ロード バランサ構成のシナリオ](#) 240
- 16 その他の Edge サービス 251
 - [DHCP サービスの管理](#) 251
 - [DHCP リレーの設定](#) 255
 - [DNS サーバの設定](#) 256
- 17 Service Composer 258
 - [Service Composer の使用](#) 260
 - [Service Composer のグラフィック表示](#) 268
 - [セキュリティ タグの操作](#) 271
 - [有効なサービスの表示](#) 273
 - [セキュリティ ポリシーの操作](#) 275
 - [セキュリティ グループの編集](#) 276
 - [Service Composer のシナリオ](#) 276
- 18 ゲスト イントロスペクション 283
 - [ゲスト イントロスペクション のインストール](#) 283
 - [ゲスト イントロスペクション のステータスの表示](#) 287
 - [ゲスト イントロスペクションのアラーム](#) 287
 - [ゲスト イントロスペクションのイベント](#) 288
 - [ゲスト イントロスペクション の監査メッセージ](#) 289

- ゲスト イントロスペクションのトラブルシューティング データの収集 289
- ゲスト イントロスペクション モジュールのアンインストール 289

19 Data Security 291

- NSX Data Security のインストール 291
- NSX Data Security のユーザー ロール 293
- データ セキュリティ ポリシーの定義 293
- データ セキュリティ スキャンの実行 295
- レポートの表示とダウンロード 295
- 正規表現の作成 296
- NSX Data Security のアンインストール 296

20 ネットワークの拡張性 298

- 分散サービス挿入 299
- Edge ベースのサービス挿入 299
- サードパーティのサービスの統合 299
- パートナー サービスの展開 300
- Service Composer を介したベンダー サービスの使用 301
- 論理ファイアウォールを使用したベンダー ソリューションへのトラフィックのリダイレクト 301
- パートナーのロード バランサの使用 302
- サードパーティ統合の削除 303

21 ユーザー管理 304

- 機能別の NSX ユーザーおよび権限 304
- Single Sign-On の設定 318
- ユーザー権限の管理 320
- デフォルト ユーザー アカウントの管理 321
- vCenter Server ユーザーへのロールの割り当て 321
- ユーザー アカウントの編集 324
- ユーザー ロールの変更 325
- ユーザー アカウントを無効または有効にする 325
- ユーザー アカウントの削除 325

22 ネットワークおよびセキュリティ オブジェクト 327

- IP アドレス グループの操作 327
- MAC アドレス グループの操作 329
- IP アドレス プールの操作 330
- Security Groups の操作 331
- サービスおよびサービス グループの操作 334

23 操作と管理 337

- コントローラ パスワードの変更 337

NSX コントローラ障害からのリカバリ	338
VXLAN ポートの変更	339
通信チャネルの健全性の確認	340
カスタマ エクスペリエンス改善プログラム	341
システム イベントと監査ログ	342
システム設定の管理	347
SNMP トラップの操作	353
NSX のバックアップとリストア	357
フロー モニタリング	361
アクティビティ モニタリング	367
トレースフロー	382

24 NSX Edge VPN 構成例 392

用語集	393
IKE フェーズ 1 とフェーズ 2	393
IPSec VPN サービスの設定例	395
Cisco 2821 を統合したサービス ルーターの使用	397
Cisco ASA 5510 の使用	400
WatchGuard Firebox X500 の設定	402
NSX Edge についてのトラブルシューティング例	403

NSX 管理ガイド

『NSX 管理ガイド』では、NSX Manager ユーザー インターフェイスと vSphere Web Client を使用して VMware[®] NSX[™] システムを構成、監視、保守する方法について説明します。詳細な設定手順や推奨されるベスト プラクティスについても記載しています。

対象読者

本書は、VMware vCenter 環境で NSX をインストールまたは使用するユーザーを対象としています。本書に記載されている情報は、システム管理者としての経験があり、仮想マシン テクノロジーおよび仮想データセンターの操作に詳しい方を対象としています。また、本書は VMware ESX、vCenter Server、vSphere Web Client を含む VMware Infrastructure 5.x についての知識も前提としています。

VMware の技術ドキュメントの用語集

VMware の技術ドキュメントには、新しい用語などを集約した用語集があります。当社の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

NSX のシステム要件

NSX のインストールまたはアップグレードを行う前に、ネットワーク設定とリソースについて検討します。1 台の vCenter Server につき NSX Manager が 1 台、1 台の ESXi™ ホストにつきゲスト イントロスペクションと Data Security のインスタンスが 1 つ、1 つのデータセンターにつき NSX Edge インスタンスを複数インストールできます。

ハードウェア

表 1-1. ハードウェア要件

アプライアンス	メモリ	vCPU	ディスク容量
NSX Manager	16 GB (NSX 環境のサイズ* によっては 24 GB)	4 (NSX 環境のサイズ* によっては 8 GB)	60 GB
NSX コントローラ	4 GB	4	20 GB
NSX Edge	<ul style="list-style-type: none"> ■ [Compact] : 512 MB ■ [Large] : 1 GB ■ [Quad Large] : 1 GB ■ [X-Large] : 8 GB 	<ul style="list-style-type: none"> ■ [Compact] : 1 ■ [Large] : 2 ■ [Quad Large] : 4 ■ [X-Large] : 6 	<ul style="list-style-type: none"> ■ [Compact] : 500 MB のディスク 1 台 ■ [Large] : 500 MB のディスク 1 台 + 512 MB のディスク 1 台 ■ [Quad Large] : 500 MB のディスク 1 台 + 512 MB のディスク 1 台 ■ [X-Large] : 500 MB のディスク 1 台 + 2 GB のディスク 1 台
ゲスト イントロスペクション	1 GB	2	4 GB
NSX Data Security	512 MB	1	ESXi ホスト 1 台あたり 6 GB

一般的なガイドラインとして、NSX 管理環境に 256 を超えるハイパーバイザーがある、または 2,000 台以上の仮想マシンが存在する場合は、NSX Manager のリソースを 8 個の vCPU、24 GB の RAM に増強する必要があります。

特定のサイジングに関する情報については、VMware サポートにお問い合わせください。

仮想アプライアンスへのメモリと vCPU の割り当てを増加させる方法については、『vSphere 仮想マシン管理』の「メモリ リソースの割り当て」と「仮想 CPU 数の変更」を参照してください。

ソフトウェア

最新の相互運用性の情報については、http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php で、製品の相互運用性マトリックスを参照してください。

NSX、vCenter Server、ESXi の推奨バージョンについては、<https://docs.vmware.com/jp/VMware-NSX-for-vSphere/index.html> にあるリリース ノートを参照してください。

NSX Manager を Cross-vCenter NSX 環境に参加させるには、次の条件を満たす必要があります。

コンポーネント	バージョン
NSX Manager	6.2 以降
NSX Controller	6.2 以降
vCenter Server	6.0 以降
ESXi	<ul style="list-style-type: none"> ■ ESXi 6.0 以降 ■ NSX 6.2 以降の VIB が準備されているホスト クラスタ

Cross-vCenter NSX 環境のすべての NSX Manager を 1 つの vSphere Web Client から管理するには、vCenter Server を拡張リンク モードで接続する必要があります。『vCenter Server およびホスト管理』の「拡張リンク モードの使用」を参照してください。

パートナーのソリューションと NSX との互換性を確認するには、VMware 互換性ガイドで Networking and Security (<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>) を参照してください。

クライアントとユーザー アクセス

- vSphere インベントリに ESXi ホスト名を追加している場合は、正引き/逆引きの名前解決が機能していることを確認してください。機能していない場合、NSX Manager は IP アドレスを解決できません。
- 仮想マシンを追加、パワーオンの権限
- 仮想マシンのファイルを保存するデータストアへのアクセス、そのデータストアにファイルをコピーするためのアカウント権限
- NSX Manager ユーザー インターフェイスにアクセスするための Web ブラウザでの Cookie の有効化
- ESXi ホスト、vCenter Server、および展開する NSX アプライアンスからポート 443 にアクセスできることを、NSX Manager で確認します。このポートは、ESXi ホストから OVF ファイルをダウンロードして展開するために必要です。
- 使用している vSphere Web Client のバージョンでサポートされている Web ブラウザは次のとおりです。詳細については、『vCenter Server およびホスト管理』ドキュメントの「vSphere Web Client の使用」を参照してください。

NSX で必要となるポートおよびプロトコル

2

NSX が正常に機能するには、次のポートが開いている必要があります。

表 2-1. NSX で必要となるポートおよびプロトコル

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
クライアント PC	NSX Manager	443	TCP	NSX Manager 管理インターフェイス	×	○	PAM 認証
クライアント PC	NSX Manager	80	TCP	NSX Manager VIB アクセス	×	×	PAM 認証
ESXi ホスト	vCenter Server	443	TCP	ESXi ホストの準備	×	×	
vCenter Server	ESXi ホスト	443	TCP	ESXi ホストの準備	×	×	
ESXi ホスト	NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
ESXi ホスト	NSX Controller	1234	TCP	ユーザー ワールド エージェント接続	×	○	
NSX Controller	NSX Controller	2878、2888、3888	TCP	コントローラ クラスター - 状態同期	×	○	IPsec
NSX Controller	NSX Controller	7777	TCP	内部コントローラ RPC ポート	×	○	IPsec
NSX Controller	NSX Controller	30865	TCP	コントローラ クラスター - 状態同期	×	○	IPsec
NSX Manager	NSX Controller	443	TCP	コントローラと Manager の通信	×	○	ユーザー/パスワード
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	×	○	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	×	○	
NSX Manager	ESXi ホスト	443	TCP	管理とプロビジョニング接続	×	○	
NSX Manager	ESXi ホスト	902	TCP	管理とプロビジョニング接続	×	○	
NSX Manager	DNS サーバ	53	TCP	DNS クライアント接続	×	×	
NSX Manager	DNS サーバ	53	UDP	DNS クライアント接続	×	×	
NSX Manager	Syslog サーバ	514	TCP	Syslog 接続	×	×	

表 2-1. NSX で必要となるポートおよびプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
NSX Manager	Syslog サーバ	514	UDP	Syslog 接続	×	×	
NSX Manager	NTP タイム サーバ	123	TCP	NTP クライアント接続	×	○	
NSX Manager	NTP タイム サーバ	123	UDP	NTP クライアント接続	×	○	
vCenter Server	NSX Manager	80	TCP	ホストの準備	×	○	
REST Client	NSX Manager	443	TCP	NSX Manager REST API	×	○	ユーザー/パスワード
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (NSX 6.2.3 より前のデフォルト) または 4789 (NSX 6.2.3 以降の新規インストールのデフォルト)	UDP	VTEP 間の転送ネットワークのカプセル化	×	○	
ESXi ホスト	ESXi ホスト	6999	UDP	VLAN LIF 上の ARP	×	○	
ESXi ホスト	NSX Manager	8301, 8302	UDP	分散仮想スイッチ同期	×	○	
NSX Manager	ESXi ホスト	8301, 8302	UDP	分散仮想スイッチ同期	×	○	
ゲストイントロセクション仮想マシン	NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
プライマリ NSX Manager	セカンダリ NSX Manager	443	TCP	Cross-vCenter NSX ユニバーサル同期サービス	×	○	
プライマリ NSX Manager	vCenter Server	443	TCP	vSphere API	×	○	
セカンダリ NSX Manager	vCenter Server	443	TCP	vSphere API	×	○	
プライマリ NSX Manager	NSX ユニバーサルコントローラ クラスタ	443	TCP	NSX Controller REST API	×	○	ユーザー/パスワード
セカンダリ NSX Manager	NSX ユニバーサルコントローラ クラスタ	443	TCP	NSX Controller REST API	×	○	ユーザー/パスワード

表 2-1. NSX で必要となるポートおよびプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
ESXi ホスト	NSX ユニバーサル コントローラ クラ スタ	1234	TCP	NSX 制御プレーン プロ トコル	×	○	
ESXi ホスト	プライマリ NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユー ザー/パスワード
ESXi ホスト	セカンダリ NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユー ザー/パスワード

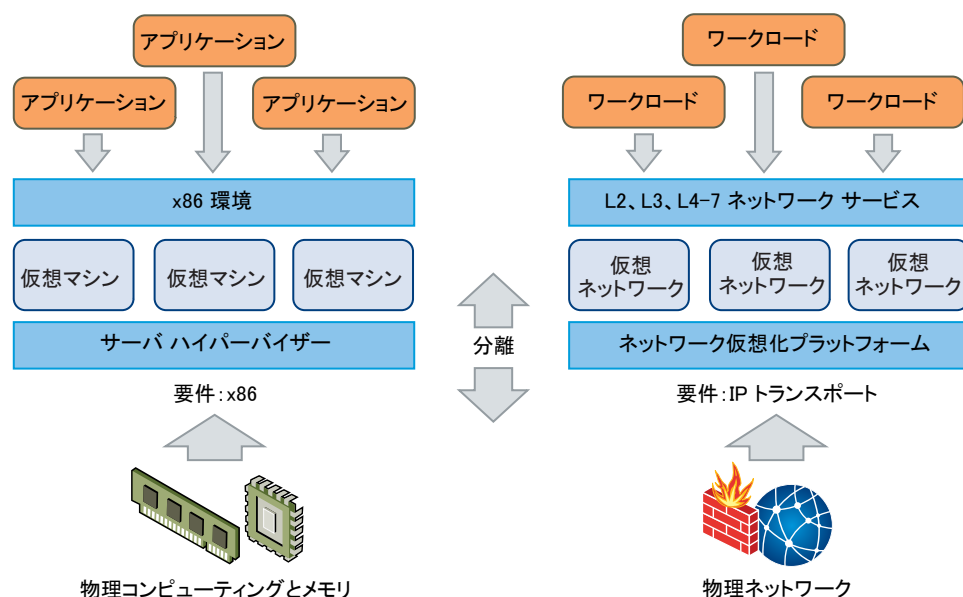
Cross-vCenter NSX と拡張リンク モードのポート

Cross-vCenter NSX 環境で、vCenter Server システムが拡張リンク モードで実行されている場合、vCenter Server システムから NSX Manager を管理するには、各 NSX Manager アプライアンスが環境内の各 vCenter Server システムと接続している必要があります。

NSX の概要

サーバ仮想化は、IT 部門に大きなメリットももたらします。サーバ統合により、物理的な煩雑さが低減し、運用効率が向上します。また、リソースを動的に再利用する能力が高まるため、ますます動的になりつつある業務用アプリケーションの要求を迅速かつ最適な形で満たすことができます

VMware の Software-Defined Data Center (SDDC) アーキテクチャは現在、物理的なデータセンター インフラストラクチャ全体に仮想化技術を拡充しています。ネットワーク仮想化プラットフォームである VMware NSX[®] は、SDDC アーキテクチャにおける主要製品です。NSX を使用すると、仮想化によりコンピューティングやストレージですでに実現されているものを、ネットワークでも実現できます。サーバ仮想化のプログラムが、ソフトウェアベースの仮想マシン (VM) を作成、スナップショット、削除、およびリストアするのと同様の方法で、NSX ネットワーク仮想化のプログラムは、ソフトウェアベースの仮想ネットワークを作成、スナップショット、削除、およびリストアします。その結果、ネットワークに対するアプローチに変革がもたらされ、データセンター マネージャが間違いに高い俊敏性と経済性を実現できるようになるだけでなく、基盤となる物理ネットワークの運用モデルを大幅に簡素化できます。NSX は、既存の従来のネットワーク モデルおよび任意のベンダーの次世代ファブリック アーキテクチャの両方を含む、あらゆる IP ネットワークにデプロイできる完全な無停止ソリューションです。つまり、NSX を使用して Software-Defined Data Center (SDDC) をデプロイするのに必要なのは、すでに所有している物理ネットワーク インフラストラクチャのみです。



上記の図は、コンピューティングとネットワーク仮想化の類似性を示しています。サーバ仮想化では、ソフトウェア抽象レイヤー（サーバハイパーバイザー）により、x86 物理サーバでよく使用される属性（CPU、RAM、ディスク、NIC など）がソフトウェアで再現されるため、それらをプログラムで任意に組み合わせて、瞬時に一意の仮想マシンを作成できます。

ネットワーク仮想化では、ネットワーク ハイパーバイザーと機能的に同等のものが、レイヤー 2 から レイヤー 7 までのネットワーク サービス一式（スイッチング、ルーティング、アクセス制御、ファイアウォール、QoS、ロードバランシングなど）をソフトウェアで完全に再現します。プログラムでこれらのサービスを任意に組み合わせ、独自の隔離された仮想ネットワークをわずか数秒で構築できます。

ネットワーク仮想化には、サーバ仮想化と同様の利点があります。たとえば、仮想マシンは基盤となる x86 プラットフォームから独立しており、IT 担当者は物理ホストをコンピューティング キャパシティのプールとして扱うことができますのと同様に、仮想ネットワークは基盤となる IP ネットワーク ハードウェアから独立しており、IT 担当者は物理ネットワークを、要求に応じて利用および再利用できる転送キャパシティのプールとして扱うことができます。従来のアーキテクチャとは異なり、仮想ネットワークは、基盤となる物理ハードウェアやトポロジを再構成しなくても、プログラムでプロビジョニング、変更、格納、削除、リストアできます。ネットワークへのこの斬新なアプローチは、扱い慣れたサーバおよびストレージ仮想化ソリューションの機能と利点を組み合わせることで、Software-Defined Data Center (SDDC) の可能性を最大限に引き出します。

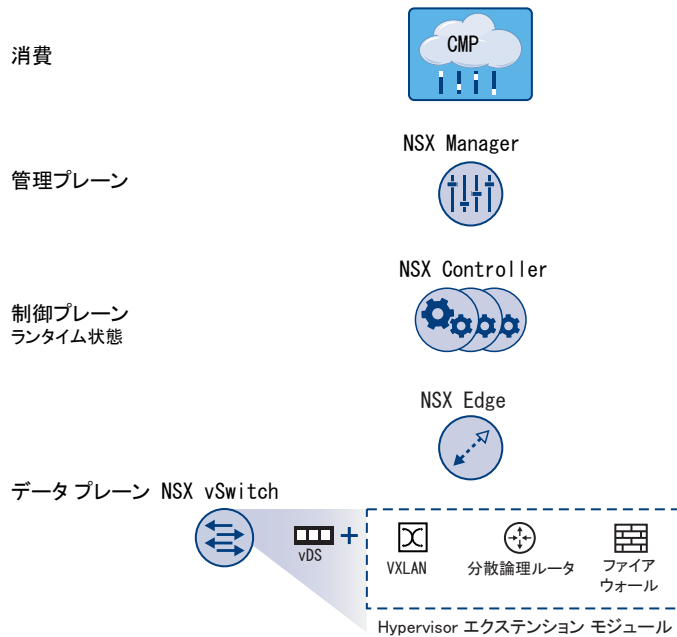
NSX は、vSphere Web Client、コマンドライン インターフェイス (CLI)、および REST API を使用して設定できます。

この章には、次のトピックが含まれています。

- [NSX コンポーネント](#)
- [NSX Edge](#)
- [NSX Services](#)

NSX コンポーネント

このセクションでは、NSX ソリューションのコンポーネントについて説明します。



Cloud Management Platform (CMP) は NSX のコンポーネントではありませんが、NSX では、REST API を使用して仮想的に任意の CMP を統合したり、VMware の CMP を設定なしで統合したりできます。

データ プレーン

NSX データ プレーンは vSphere Distributed Switch (VDS) をベースにした NSX vSwitch で設定され、サービスを有効にするためのコンポーネントが追加されています。NSX カーネル モジュール、ユーザー領域のエージェント、構成ファイル、およびインストール スクリプトが VIB にパッケージ化され、ハイパーバイザー カーネル内で実行されます。これにより、分散ルーティングや論理ファイアウォールなどのサービスの提供や VXLAN ブリッジ機能を有効にすることができます。

NSX vSwitch (vDS ベース) は、物理ネットワークを抽象化して、ハイパーバイザー内でアクセスレベルでのスイッチングを実現します。NSX vSwitch は、VLAN などの物理構成に依存しない論理的なネットワークを可能にするため、ネットワーク仮想化の中核を成します。vSwitch のいくつかのメリットを次に示します。

- (VXLAN などの) プロトコルや一元化されたネットワーク設定によるオーバーレイ ネットワークのサポート。オーバーレイ ネットワークにより、次のことが可能になります。
 - 物理ネットワークにおける VLAN ID の使用を削減
 - データセンター ネットワークを再設計せずに、既存の物理インフラストラクチャの既存の IP ネットワーク上に柔軟性のある論理的なレイヤー 2 (L2) オーバーレイを作成
 - テナント間の分離を維持しながら、通信（水平方向および垂直方向の通信）を提供
 - オーバーレイ ネットワークに依存せず、物理 L2 ネットワークに接続しているように機能する、アプリケーション ワークロードと仮想マシン
- ハイパーバイザーの大規模な拡張を促進
- 複数の機能（ポート ミラーリング、NetFlow/IPFIX、のバックアップとリストア、ネットワークの健全性チェック、QoS、LACP）により、仮想ネットワークにおけるトラフィックの管理、監視、およびトラブルシューティング用の包括的なツールキットを実現

分散論理ルーターは、論理ネットワーク領域 (VXLAN) から物理ネットワーク (VLAN) までの L2 ブリッジを提供できます。

ゲートウェイ デバイスは、通常、NSX Edge 仮想アプライアンスです。NSX Edge は、L2、L3、境界ファイアウォール、ロード バランシングやその他のサービス (SSL VPN、DHCP など) を提供します。

制御プレーン

NSX 制御プレーンは、NSX Controller クラスタ内で実行されます。NSX Controller は、NSX の論理スイッチングおよびルーティング機能の制御プレーンとして機能する高度な分散状態管理システムです。これは、ネットワーク内のすべての論理スイッチの中央制御点であり、すべてのホスト、論理スイッチ (VXLAN)、および分散論理ルーターの情報を管理します。

コントローラ クラスタで、ハイパーバイザー内の分散スイッチング モジュールとルーティング モジュールを管理します。コントローラを通過するデータプレーン トラフィックはありません。3 つのメンバーのクラスタにコントローラ ノードをデプロイして、高可用性とスケーリングを可能にします。コントローラ ノードに障害が発生しても、データプレーン トラフィックに影響はありません。

NSX Controller は、ネットワーク情報をホスト間に分散することによって機能します。高レベルの復元性を達成するため、NSX Controller はクラスタ化によって、スケーラブルおよび高可用性を実現しています。NSX Controller は、3 ノード クラスタにデプロイする必要があります。3 台の仮想アプライアンスによって、NSX ドメイン内のすべてのネットワーク機能の状態を把握、保持、および更新します。NSX Manager は、NSX Controller ノードをデプロイするために使用されます。

3 台の NSX Controller ノードがコントロール クラスタを形成します。コントローラ クラスタには、「スプリット ブレイン問題」を回避するためにクォーラム (マジョリティともいう) が必要です。スプリット ブレイン問題では、重複する 2 つの異なるデータセットのメンテナンスが原因でデータの不整合が生じます。この不整合は、エラー条件およびデータ同期の問題により発生する可能性があります。3 台の NSX Controller ノードがあることで、いずれか 1 台の NSX Controller ノードで障害が発生したとしても、データの冗長性が維持されます。

コントローラ クラスタには、以下に示すいくつかのロールがあります。

- API プロバイダ
- セッション維持サーバ
- スイッチ マネージャ
- 論理マネージャ
- ディレクトリ サーバ

各ロールには、マスター コントローラ ノードがあります。あるロールのマスター コントローラ ノードで障害が発生すると、クラスタはそのロールの新しいマスターを、利用可能な NSX Controller ノードから選択します。そのロールの新しいマスター NSX Controller ノードは、ワークの失われた部分を残りの NSX Controller ノードに再割り当てします。

NSX は、マルチキャスト、ユニキャスト、およびハイブリッドの 3 つの論理スイッチ制御プレーン モードをサポートします。コントローラ クラスタを使用して VXLAN ベースの論理スイッチを管理すると、物理ネットワーク インフラストラクチャからのマルチキャスト サポートの必要がなくなります。マルチキャスト グループの IP アドレスをプロビジョニングする必要はありません。また、物理スイッチまたはルーターで PIM ルーティング機能や IGMP スヌー

ピング機能を有効にする必要もありません。このため、ユニキャストおよびハイブリッドモードでは、NSX が物理ネットワークから分離されます。ユニキャスト制御プレーンモードの VXLAN では、論理スイッチ内でブロードキャスト、不明なユニキャスト、およびマルチキャスト (BUM) トラフィックを処理するためのマルチキャストをサポートする上で、物理ネットワークが不要になります。ユニキャストモードでは、すべての BUM トラフィックがホストでローカルにレプリケートされ、物理ネットワーク設定が不要です。ハイブリッドモードでは、パフォーマンス向上のために、一部の BUM トラフィック レプリケーションが第 1 ホップの物理スイッチにオフロードされます。ハイブリッドモードでは、最初のホップのスイッチでの IGMP スヌーピング、および各 VTEP サブネット内の IGMP クエリアにアクセスすることが必要です。

管理プレーン

NSX 管理プレーンは、NSX Manager によって構築される、NSX の集中ネットワーク管理コンポーネントであり、一元的な設定と REST API のエントリポイントを提供します。

NSX Manager は、vCenter Server 環境内の ESX™ ホストに仮想アプライアンスとしてインストールされます。NSX Manager と vCenter Server は 1 対 1 の関係を持ちます。つまり、1 つの NSX Manager のインスタンスに対し、vCenter Server は 1 台です。これは、Cross-vCenter NSX 環境でも同じです。

Cross-vCenter NSX 環境には、1 つのプライマリ NSX Manager と 1 つ以上のセカンダリ NSX Manager があります。プライマリ NSX Manager を使用すると、ユニバーサル論理スイッチ、ユニバーサル分散論理ルーター、およびユニバーサル ファイアウォールルールを作成できます。セカンダリ NSX Manager は、特定の NSX Manager のローカルなネットワーク サービスの管理に使用されます。Cross-vCenter NSX 環境では、プライマリ NSX Manager に最大 7 つのセカンダリ NSX Manager を関連付けることができます。

使用プラットフォーム

vSphere Web Client で提供される NSX Manager ユーザー インターフェイスから NSX を直接利用することができます。通常、エンドユーザーはネットワークの仮想化を Cloud Management Platform に関連付けてアプリケーションをデプロイします。NSX には豊富な統合が用意されており、REST API を介して事実上どのような CMP とも統合できます。また、VMware vCloud Automation Center、vCloud Director、および OpenStack と NSX 用の Neutron プラグインを使用する、設定不要の簡単な統合も利用できます。

NSX Edge

NSX Edge は、Edge Services Gateway (ESG) または分散論理ルーター (DLR) としてインストールできます。ESG や分散論理ルーターを含むエッジ アプライアンスの数は、ホストあたり 250 個までに制限されています。

Edge Services Gateway

この ESG を利用することで、ファイアウォール、NAT、DHCP、VPN、ロード バランシング、高可用性などのすべての NSX Edge サービスにアクセスできます。データセンターには、複数の ESG 仮想アプライアンスをインストールできます。各 ESG 仮想アプライアンスには、アップリンクと内部のネットワーク インターフェイスを合計で 10 個指定できます。トランクを使用すると、ESG には最大で 200 のサブインターフェイスを指定できます。内部インター

フェイスは保護されたポート グループに接続され、そのポート グループ内の保護された仮想マシンすべてのゲートウェイとして機能します。内部インターフェイスに割り当てられたサブネットは、パブリックにルーティングされる IP 空間にも、ネットワーク アドレス変換またはルーティングされる RFC 1918 専用空間にもなります。ファイアウォール ルールなどの NSX Edge サービスは、ネットワーク インターフェイス間のトラフィックに適用されます。

ESG のアップリンク インターフェイスは、社内共有ネットワークや、アクセス レイヤー ネットワーキングを提供するサービスに対するアクセス権を持つアップリンク ポート グループに接続します。ロード バランサ、サイト間 VPN、NAT サービス用に複数の外部 IP アドレスを設定できます。

分散論理ルーター

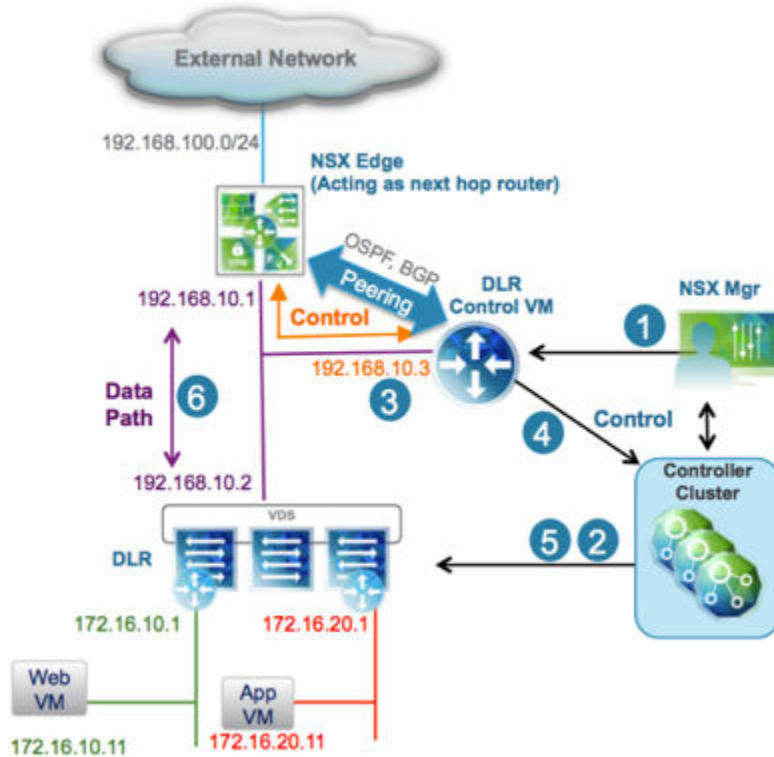
分散論理ルーターは、テナント IP アドレス空間とデータ パス分離による水平方向の分散ルーティングを提供します。複数のサブネットにわたっている同一ホスト上に存在する仮想マシンまたはワークロードは、従来のルーティング インターフェイスをトラバースすることなく相互に通信できます。

分散論理ルーターには、8 個のアップリンク インターフェイスと、最大 1,000 個の内部インターフェイスを割り当てることができます。分散論理ルーター上のアップリンク インターフェイスは、分散論理ルーターと ESG 間のレイヤー 2 論理中継スイッチを介して、ESG とピアを形成します。分散論理ルーターの内部インターフェイスは、仮想マシンと分散論理ルーター間の論理スイッチを介して、ESX ハイパーバイザーにホストされている仮想マシンとピアを形成します。

分散論理ルーターには、以下の 2 つの主なコンポーネントがあります。

- 分散論理ルーター制御プレーンが分散論理ルーター仮想アプライアンスから提供されます（制御仮想マシンとも呼ばれます）。この仮想マシンは、動的なルーティング プロトコル（BGP または OSPF）をサポートし、ルーティングの更新情報を次のレイヤー 3 ホップ デバイス（通常、Edge Services Gateway）と交換し、NSX Manager および NSX Controller クラスタと通信します。分散論理ルーター仮想アプライアンスでは、アクティブ-スタンバイ構成による高可用性がサポートされます。高可用性を有効にして分散論理ルーターを作成すると、アクティブ-スタンバイ モードで機能する仮想マシンのペアが提供されます。
- データプレーン レベルで分散論理ルーター カーネル モジュール (VIB) が存在します。これは、NSX ドメインに含まれる ESXi ホストにインストールされます。このカーネル モジュールは、レイヤー 3 ルーティングをサポートするモジュール型シャーシに組み込まれたライン カードに似ています。カーネル モジュールには、コントローラ クラスタからプッシュされるルーティング情報ベース (RIB)（ルーティング テーブルとも呼ばれる）が含まれます。ルート参照と ARP エントリ参照のデータ プレーン機能はカーネル モジュールによって実行されます。カーネル モジュールには論理インターフェイス (LIF と呼ばれる) が搭載されており、さまざまな論理スイッチと、VLAN にバックアップされたあらゆるポート グループに接続されます。各 LIF には、接続先の論理 L2 セグメントのデフォルト IP ゲートウェイを表す IP アドレスと、vMAC アドレスが割り当てられます。IP アドレスは LIF ごとに一意ですが、定義されたすべての LIF に同じ vMAC が割り当てられます。

図 3-1. 論理ルーティング コンポーネント



- 1 NSX Manager のユーザー インターフェース（または API 呼び出し）を使用して分散論理ルーター インスタンスを作成し、ルーティングを有効にして、OSPF または BGP を利用します。
- 2 NSX Controller は、ESXi ホストが含まれる制御プレーンを利用して、LIF および関連付けられた IP アドレスと vMAC アドレスを含め、新しい分散論理ルーター設定をプッシュします。
- 3 ネクスト ホップ デバイス（この例では NSX Edge [ESG]）でルーティング プロトコルも有効になっていると仮定すると、ESG と分散論理ルーター制御仮想マシンとの間で OSPF または BGP のピアリングが確立されます。これで、ESG と分散論理ルーターはルーティング情報を交換できます。
 - 接続されたすべての論理ネットワーク用の IP プリフィックスを OSPF に再配分するように分散論理ルーター制御仮想マシンを設定できます（この例では 172.16.10.0/24 と 172.16.20.0/24）。この結果、このルートのアドパイズが NSX Edge にプッシュされます。このプリフィックスのネクスト ホップは、制御仮想マシンに割り当てられた IP アドレス (192.168.10.3) ではなく、分散論理ルーターのデータプレーン コンポーネントを特定する IP アドレス (192.168.10.2) です。前者は分散論理ルーターの「プロトコル アドレス」、後者は「転送アドレス」と呼ばれます。
 - NSX Edge は、外部ネットワーク内の IP ネットワークに到達するためのプリフィックスを制御仮想マシンにプッシュします。多くのシナリオで、NSX Edge は 1 つのデフォルトルートを送信します。そのデフォルトルートが物理ネットワーク インフラストラクチャへの単一出口点を表しているためです。
- 4 分散論理ルーター制御仮想マシンは、NSX Edge から学習した IP ルートをコントローラ クラスタにプッシュします。

- 5 コントローラ クラスタは、分散論理ルーター制御仮想マシンから学習したルートをハイパーバイザーに配布します。クラスタ内の各コントローラ ノードは、特定の分散論理ルーター インスタンスに対する情報を配布します。複数の分散論理ルーター インスタンスがデプロイされているデプロイでは、コントローラ ノード全体で負荷が分散されます。通常、個々の分散論理ルーター インスタンスは、デプロイされた各テナントに関連付けられます。
- 6 ホスト上の分散論理ルーター ルーティング カーネル モジュールは、NSX Edge 経由で外部ネットワークと通信するためのデータパス トラフィックを処理します。

NSX Services

NSX コンポーネントは連携して、次の機能的なサービスを提供します。

論理スイッチ

クラウド デプロイ環境や仮想データセンターでは、多数のテナント間にさまざまなアプリケーションが存在します。セキュリティ、障害の隔離、および IP アドレス重複の回避のために、これらのアプリケーションとテナントは互いに分離させる必要があります。NSX では、それぞれが単一の論理的なブロードキャスト ドメインである複数の論理スイッチを作成できます。アプリケーションまたはテナントの仮想マシンは、論理的に論理スイッチに接続できます。これにより、デプロイの柔軟性および速度が確保され、同時に、物理レイヤー 2 のスプロールやスパニング ツリーといった問題が生じることなく、物理ネットワークのブロードキャスト ドメイン (VLAN) のすべての特性が引き続き提供されます。

論理スイッチは分散され、vCenter Server 内のすべてのホスト（または Cross-vCenter NSX 環境内のすべてのホスト）にまたがって設置できます。これにより、物理レイヤー 2 (VLAN) 境界の制限を受けることなく、データセンター内での仮想マシンのモビリティ (vMotion) が確保されます。論理スイッチのソフトウェアにはブロードキャスト ドメインが含まれているため、物理インフラストラクチャが MAC/FIB テーブルの制限に制約されることはありません。

分散論理ルーター

ルーティングは、レイヤー 2 ブロードキャスト ドメイン間の必要な転送情報を提供します。これにより、レイヤー 2 ブロードキャスト ドメインのサイズを削減し、ネットワークの効率と拡張性を向上できます。NSX は、このインテリジェンスをワークロードが存在する場所に拡張し、水平方向のルーティングを行います。これにより、コストと時間をかけてホップを拡張することなく、より直接的に仮想マシン間の通信ができます。同時に、NSX 分散論理ルーターは垂直方向の接続も提供するため、テナントはパブリック ネットワークにアクセスできます。

論理ファイアウォール

論理ファイアウォールは、動的仮想データセンターにセキュリティ メカニズムを提供します。論理ファイアウォールの Distributed Firewall コンポーネントでは、仮想マシンの名前および属性、ユーザー ID、vCenter オブジェクト（データセンターなど）、ホスト、および従来のネットワーク属性（IP アドレスや VLAN など）に基づき、仮想マシンなどの仮想データセンター エンティティをセグメント化できます。また、Edge ファイアウォール コンポーネントにより、IP/VLAN 構造に基づく DMZ の構築、マルチテナント仮想データセンター内のテナント分離などの、主要な境界セキュリティのニーズに応えることができます。

フロー モニタリング機能では、アプリケーション プロトコル レベルでの仮想マシン間のネットワーク アクティビティが表示されます。この情報を使用して、ネットワーク トラフィックの監査、ファイアウォール ポリシーの定義と調整、およびネットワークに対する脅威の識別を行うことができます。

論理 Virtual Private Network (VPN)

SSL VPN-Plus を使用することで、リモート ユーザーがプライベートの企業アプリケーションにアクセスできます。IPsec VPN は、NSX またはサードパーティ ベンダーのハードウェア ルーター/VPN ゲートウェイを使用して、NSX Edge インスタンスとリモート サイトとのサイト間接続を提供します。また L2 VPN では、地理的境界を越えて同じ IP を保持しながら、仮想マシンによるネットワーク接続を維持できるようにすることで、データセンターを拡張できます。

論理ロード バランサ

NSX Edge ロード バランサは、単一の仮想 IP アドレス (VIP) を対象とするクライアント接続を、ロード バランシング プールのメンバーとして設定された複数のターゲットに分散します。受信サービス リクエストは、負荷配分がユーザーにとって透過的になるように、複数のサーバ間で均等に配分されます。このように、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。

Service Composer

Service Composer では、ネットワークおよびセキュリティ サービスを仮想インフラストラクチャ内のアプリケーションにプロビジョニングして割り当てることができます。これらのサービスをセキュリティ グループにマップすると、サービスがセキュリティ ポリシーに基づいてセキュリティ グループの仮想マシンに適用されます。

Data Security は、組織の仮想化されたクラウド環境内に格納されている機密データを表示できるようにし、データセキュリティ違反を報告します。

NSX の拡張性

サードパーティのソリューション プロバイダはソリューションを NSX プラットフォームに統合することができるため、お客様に VMware 製品とパートナーのソリューションを統合した環境を提供することができます。データセンターのオペレータは、基盤となるネットワーク トポロジやコンポーネントに関係なく、複雑なマルチティア仮想ネットワークを数秒でプロビジョニングできます。

Cross-vCenter Networking and Security の概要

NSX 6.2 では、複数の vCenter Server NSX 環境を 1 つのプライマリ NSX Manager から管理できます。

この章には、次のトピックが含まれています。

- [Cross-vCenter NSX の利点](#)
- [Cross-vCenter NSX の仕組み](#)
- [Cross-vCenter NSX での NSX Services のサポート マトリックス](#)
- [ユニバーサル コントローラ クラスター](#)
- [ユニバーサル トランスポート ゾーン](#)
- [ユニバーサル論理スイッチ](#)
- [ユニバーサル分散論理ルーター](#)
- [ユニバーサル ファイアウォール ルール](#)
- [ユニバーサル ネットワークとセキュリティ オブジェクト](#)
- [Cross-vCenter NSX トポロジ](#)
- [NSX Manager ロールの変更](#)

Cross-vCenter NSX の利点

2 つ以上の vCenter Server システムが存在する NSX 環境を、一元管理できます。

複数の vCenter Server システムが必要となる理由はいくつもあります。以下に例を挙げます。

- vCenter Server のスケール制限に対処するため
- 専用の vCenter Server、または複数の vCenter Server を必要とする製品（Horizon View や Site Recovery Manager など）に対応するため
- ビジネス ユニット、テナント、組織、または環境タイプなどで環境を分割するため

NSX 6.1 以前のバージョンでは、複数の vCenter NSX 環境をデプロイする場合、それらを別々に管理する必要があります。NSX 6.2 では、プライマリ NSX Manager 上にユニバーサル オブジェクトを作成すると、それらのオブジェクトが環境内のすべての vCenter Server システムで同期されます。

Cross-vCenter NSX には以下の特長があります。

- NSX 論理ネットワークのスパンの拡大。vCenter NSX 環境全体で同じ論理ネットワークが使用できるため、任意の vCenter Server システム上の任意のクラスターにある仮想マシンを同じ論理ネットワークに接続できます。
- セキュリティ ポリシー管理の一元化。ファイアウォール ルールが 1 か所で集中管理され、場所または vCenter Server システムに関係なく仮想マシンに適用されます。
- 複数の Cross-vCenter Server や論理スイッチをまたぐ長距離の vMotion など、vSphere 6 での新しいモビリティ境界のサポート。
- 都市全体をカバーする距離から 150ms RTT まで、マルチサイト環境のサポートの強化。これには、アクティブ-アクティブ データセンターとアクティブ-パッシブ データセンターが含まれます。

Cross-vCenter NSX 環境には多くの利点があります。

- ユニバーサル オブジェクトの一元管理。これにより、管理作業が軽減されます。
- ワークロードのモビリティの向上。仮想マシンの再構成やファイアウォール ルールの変更を行わずに、vCenter Server 間で仮想マシンの vMotion を実行できます。
- NSX の複数サイト機能およびディザスタ リカバリ機能の強化。

注: Cross-vCenter NSX 機能は、vSphere 6.0 でのみサポートされます。

Cross-vCenter NSX の仕組み

Cross-vCenter NSX 環境では、複数の vCenter Server を設定できます。各 vCenter Server は、それぞれの NSX Manager とペアリングされている必要があります。1 つの NSX Manager にはプライマリ NSX Manager のロールが割り当てられ、その他の NSX Manager にはセカンダリ NSX Manager のロールが割り当てられます。

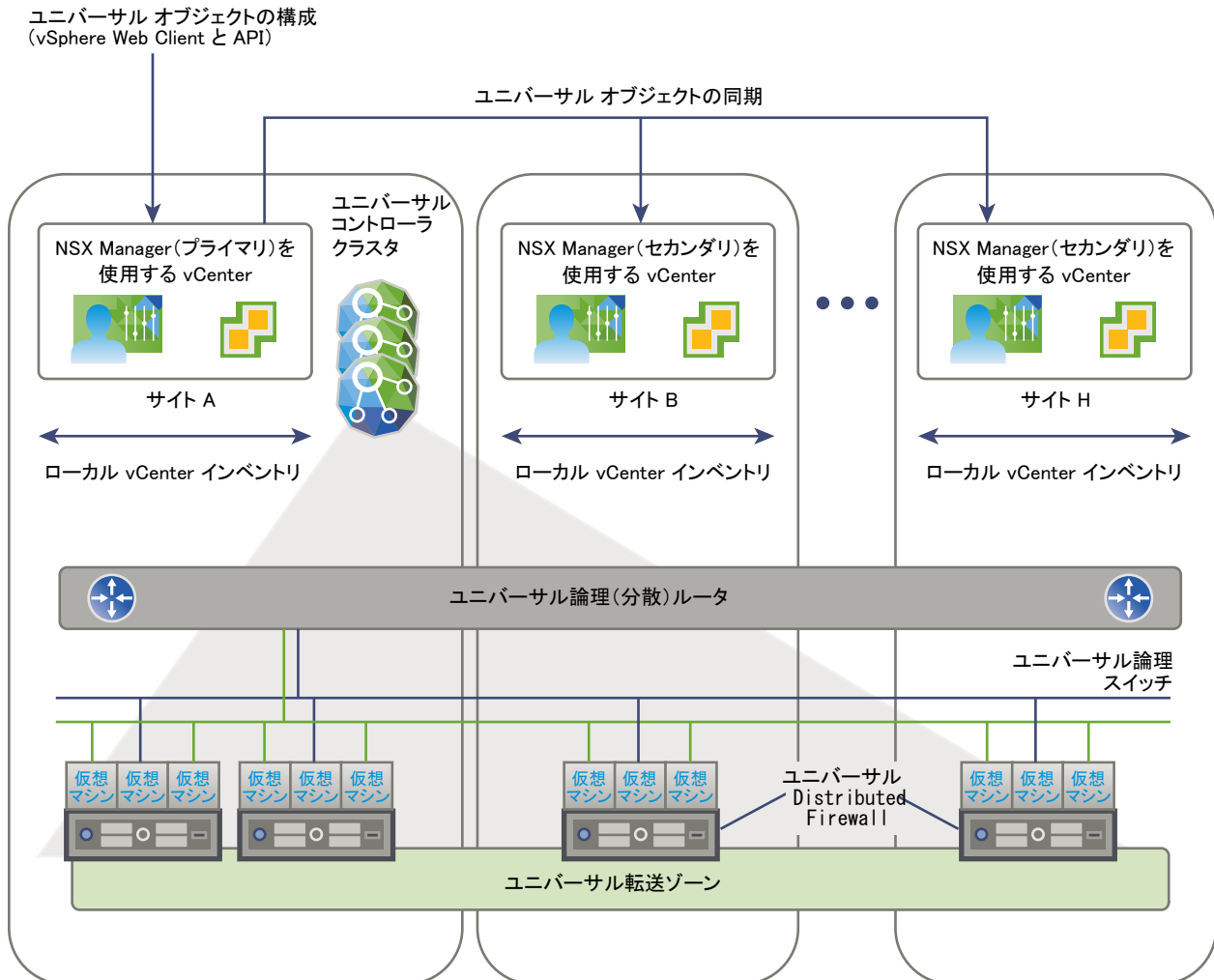
プライマリ NSX Manager は、Cross-vCenter NSX 環境の制御プレーンを提供するユニバーサル コントローラ クラスターをデプロイするために使用されます。セカンダリ NSX Manager には、各自のコントローラ クラスターはありません。

プライマリ NSX Manager は、ユニバーサル論理スイッチなどのユニバーサル オブジェクトを作成できます。これらのオブジェクトは、NSX ユニバーサル同期サービスによってセカンダリ NSX Manager に同期されます。セカンダリ NSX Manager では、これらのオブジェクトを表示できますが、編集することはできません。ユニバーサル オブジェクトを管理するには、プライマリ NSX Manager を使用する必要があります。プライマリ NSX Manager を使用して、環境内の任意のセカンダリ NSX Manager を設定できます。

プライマリ NSX Manager とセカンダリ NSX Manager のどちらでも、その特定の vCenter Server NSX 環境に対してローカルなオブジェクト（論理スイッチや分散論理ルーターなど）を作成できます。それらのオブジェクトは、作成された vCenter Server NSX 環境内だけにのみ存在するようになります。Cross-vCenter NSX 環境の他の NSX Manager には表示されません。

NSX Manager には、スタンドアロンロールを割り当てることができます。これは、NSX Manager と vCenter Server がそれぞれ 1 つずつある NSX 6.2 以前の環境に相当します。スタンドアロン NSX Manager は、ユニバーサル オブジェクトを作成できません。

注: NSX 環境にユニバーサル オブジェクトが存在する場合に、プライマリ NSX Manager のロールをスタンドアロンに変更すると、その NSX Manager に移行ロールが割り当てられます。ユニバーサル オブジェクトはそのまま残されますが、変更することはできません。また、他のユニバーサル オブジェクトを作成することもできません。ユニバーサル オブジェクトは、移行ロールから削除できます。移行ロールは、プライマリにする NSX Manager を変更する場合など、一時的な使用に限定する必要があります。



Cross-vCenter NSX での NSX Services のサポート マトリックス

Cross-vCenter NSX でのユニバーサル同期で、NSX Services のサブセットを使用できます。

表 4-1. Cross-vCenter NSX での NSX Services のサポート マトリックス

NSX Service	詳細	NSX 6.2 での Cross-vCenter NSX 同期のサポートの有無
論理スイッチ	トランスポート ゾーン	はい
	論理スイッチ	はい
L2 ブリッジ		いいえ
ルーティング	論理 (分散) ルーター	はい
	論理 (分散) ルーター アプライアンス	仕様により未サポート。ユニバーサル論理ルーターごとに複数のアプライアンスが必要な場合は、NSX Manager ごとにアプライアンスを作成する必要があります。これにより、アプライアンスごとに異なる設定が可能となります。これは、ローカル出力側が構成されている環境で必要となります。
	NSX Edge Services Gateway	いいえ
論理ファイアウォール	Distributed Firewall	はい
	除外リスト	いいえ
	SpoofGuard	いいえ
	集約フローの フロー モニタリング	いいえ
	ネットワーク サービス挿入	いいえ
	Edge ファイアウォール	いいえ
VPN		いいえ
論理ロード バランサ		いいえ
その他の Edge サービス		いいえ
Service Composer		いいえ
Data Security		いいえ
ネットワークの拡張性		いいえ
ネットワークおよびセキュリティ オブジェクト	IP アドレス グループ (IP セット)	はい
	MAC アドレス グループ (MAC セット)	はい
	IP アドレス プール	いいえ
	Security Group	サポートあり。ただし、ユニバーサル Security Group には、包含オブジェクトのみを追加でき、動的メンバーシップまたは除外オブジェクトは追加できません
	サービス	はい
	サービス グループ	はい

ユニバーサル コントローラ クラスタ

各 Cross-vCenter NSX 環境には、プライマリ NSX Manager に関連付けられたユニバーサル コントローラ クラスタが 1 つあります。セカンダリ NSX Manager には、コントローラ クラスタはありません。

ユニバーサル コントローラ クラスタは、Cross-vCenter NSX 環境の唯一のコントローラ クラスタであるため、ユニバーサル論理スイッチ、ユニバーサル分散論理ルーター、および vCenter Server NSX ペアに対してローカルな論理スイッチおよび分散論理ルーターに関する情報を保持します。

オブジェクト ID の重複を避けるため、ユニバーサル オブジェクトとローカル オブジェクトにはそれぞれ異なる ID プールが保持されます。

ユニバーサル トランスポート ゾーン

Cross-vCenter NSX 環境では、ユニバーサル トランスポート ゾーンは 1 つしか設定できません。

ユニバーサル トランスポート ゾーンはプライマリ NSX Manager 上に作成され、セカンダリ NSX Manager と同期されます。ユニバーサル論理ネットワークに参加する必要があるクラスタは、NSX Manager からユニバーサル トランスポート ゾーンに追加する必要があります。

ユニバーサル論理スイッチ

ユニバーサル論理スイッチを使用すると、レイヤー 2 ネットワークを複数のサイトにまたがって設置できます。

ユニバーサル トランスポート ゾーンに論理スイッチを作成すると、ユニバーサル論理スイッチを作成することになります。このスイッチは、ユニバーサル トランスポート ゾーン内のすべてのクラスタで使用できます。ユニバーサル トランスポート ゾーンには、Cross-vCenter NSX 環境にある任意の vCenter Server のクラスタを含めることができます。

VNI を論理スイッチに割り当てるにはセグメント ID プールが使用され、VNI をユニバーサル論理スイッチに割り当てるにはユニバーサル セグメント ID プールが使用されます。これらのプール間には重複がないようにしてください。

ユニバーサル論理スイッチ間でルーティングを行う場合は、ユニバーサル分散論理ルーターを使用する必要があります。ユニバーサル論理スイッチと論理スイッチの間でルーティングを行う必要がある場合は、Edge Services Gateway を使用する必要があります。

ユニバーサル分散論理ルーター

ユニバーサル分散論理ルーターにより、ユニバーサル分散論理ルーター、クラスタ、またはホスト レベルでカスタマイズできる一元管理とルーティング構成を実現できます。

ユニバーサル分散論理ルーターを作成するときは、Local Egress（ローカル出力方向）を有効にするかどうかを選択する必要があります。この選択は、ルーター作成後に変更できません。Local Egress（ローカル出力方向）を使用すると、識別子であるロケール ID に基づいて、どのルートが ESXi ホストに提供されるかを制御できます。

各 NSX Manager には、デフォルトで NSX Manager の UUID に設定されているロケール ID が割り当てられています。次のレベルでロケール ID をオーバーライドできます。

- ユニバーサル分散論理ルーター

- クラスタ
- ESXi ホスト

Local Egress（ローカル出力方向）を有効にしない場合、ロケール ID は無視され、ユニバーサル分散論理ルーターに接続されているすべての ESXi ホストは同じルートを受信します。Cross-vCenter NSX 環境で Local Egress（ローカル出力方向）を有効にするかどうかは設計上の考慮事項ですが、すべての Cross-vCenter NSX 構成で必要というわけではありません。

ユニバーサル ファイアウォール ルール

Cross-vCenter NSX 環境の Distributed Firewall により、使用環境内のすべての vCenter Server に適用されるルールを一元管理できます。Cross-vCenter vMotion がサポートされているため、ワークロードや仮想マシンを vCenter Server 間で移動したり、ソフトウェア定義によるデータセンターのセキュリティをシームレスに拡張したりできます。

データセンターのスケールアウトが必要なときに、既存の vCenter Server を同じレベルにスケーリングできないことがあります。このため、アプリケーション一式を、別の vCenter Server が管理する新しいホストに移動しなければならない場合があります。あるいは、ステージング サーバが 1 つの vCenter Server に管理され、本番サーバが別の vCenter Server に管理されている環境で、アプリケーションをステージングから本番に移動しなければならない場合もあります。Distributed Firewall では、プライマリ NSX Manager に対して定義したファイアウォール ポリシーを最大 7 つのセカンダリ NSX Manager にレプリケートすることにより、これらの Cross-vCenter vMotion シナリオをサポートします。

ユニバーサル同期の対象としてマークした Distributed Firewall ルール セクションをプライマリ NSX Manager から作成できます。1 つのユニバーサル L2 ルール セクションと 1 つのユニバーサル L3 ルール セクションを作成できます。これらのセクションと各ルールは、環境内のすべてのセカンダリ NSX Manager に同期されます。他のセクションのルールは、引き続き、該当する NSX Manager でローカルに使用されます。

次の Distributed Firewall 機能は、Cross-vCenter NSX 環境でサポートされていません。

- 除外リスト
- SpoofGuard
- 集約フローの フロー モニタリング
- ネットワーク サービス挿入
- Edge ファイアウォール

Service Composer はユニバーサル同期をサポートしないため、Service Composer を使用して、ユニバーサル セクションに Distributed Firewall ルールを作成できません。

ユニバーサル ネットワークとセキュリティ オブジェクト

ユニバーサル セクションの Distributed Firewall ルールで使用する、カスタム ネットワークとセキュリティ オブジェクトを作成できます。

- ユニバーサル IP セット
- ユニバーサル MAC セット
- ユニバーサル Security Group

- ユニバーサル サービス
- ユニバーサル サービス グループ

ユニバーサル ネットワークおよびセキュリティ オブジェクトは、プライマリ NSX Manager からのみ作成できます。

ユニバーサル セキュリティ グループには、ユニバーサル IP セット、ユニバーサル MAC セット、およびユニバーサル セキュリティ グループのみを含めることができます。メンバーシップは、含まれているオブジェクトのみを使用して定義されます。動的メンバーシップや除外されたオブジェクトを使用することはできません。

ユニバーサル セキュリティ グループを Service Composer から作成することはできません。Service Composer から作成されたセキュリティ グループは、その NSX Manager に対してローカルになります。

Cross-vCenter NSX トポロジ

Cross-vCenter NSX は、単一の物理サイトか、または複数のサイトにまたがってデプロイできます。

複数サイトおよび単一サイトの Cross-vCenter NSX

Cross-vCenter NSX 環境では、複数の vCenter NSX 設定で、同じ論理スイッチとその他のネットワーク オブジェクトを使用できます。複数の vCenter Server は、同一サイトにも、異なるサイトにも配置できます。

Cross-vCenter NSX 環境が 1 つのサイト内に収まっているか、複数のサイトにまたがっているかに関係なく、同様の構成を使用できます。次の 2 つのトポロジ例は、以下で構成されます。

- 特定のサイトまたは複数のサイトに存在するすべてのクラスタを含むユニバーサルトランスポート ゾーン。
- ユニバーサルトランスポート ゾーンに接続されたユニバーサル論理スイッチ。仮想マシンの接続には 2 つのユニバーサル論理スイッチが使用され、1 つは、ルーター アップリンクの移行ネットワークとして使用されます。
- ユニバーサル論理スイッチに追加された仮想マシン
- 動的なルーティングを実現するための、NSX Edge アプライアンスを使用したユニバーサル分散論理ルーター
ユニバーサル分散論理ルーター アプライアンスには、仮想マシン ユニバーサル論理スイッチ上の内部インターフェイスと、移行ネットワーク ユニバーサル論理スイッチ上のアップリンク インターフェイスがあります。
- 移行ネットワークと物理出力方向ルーター ネットワークに接続された Edge Services Gateway (ESG)

図 4-1. 単一サイト内の Cross-vCenter NSX

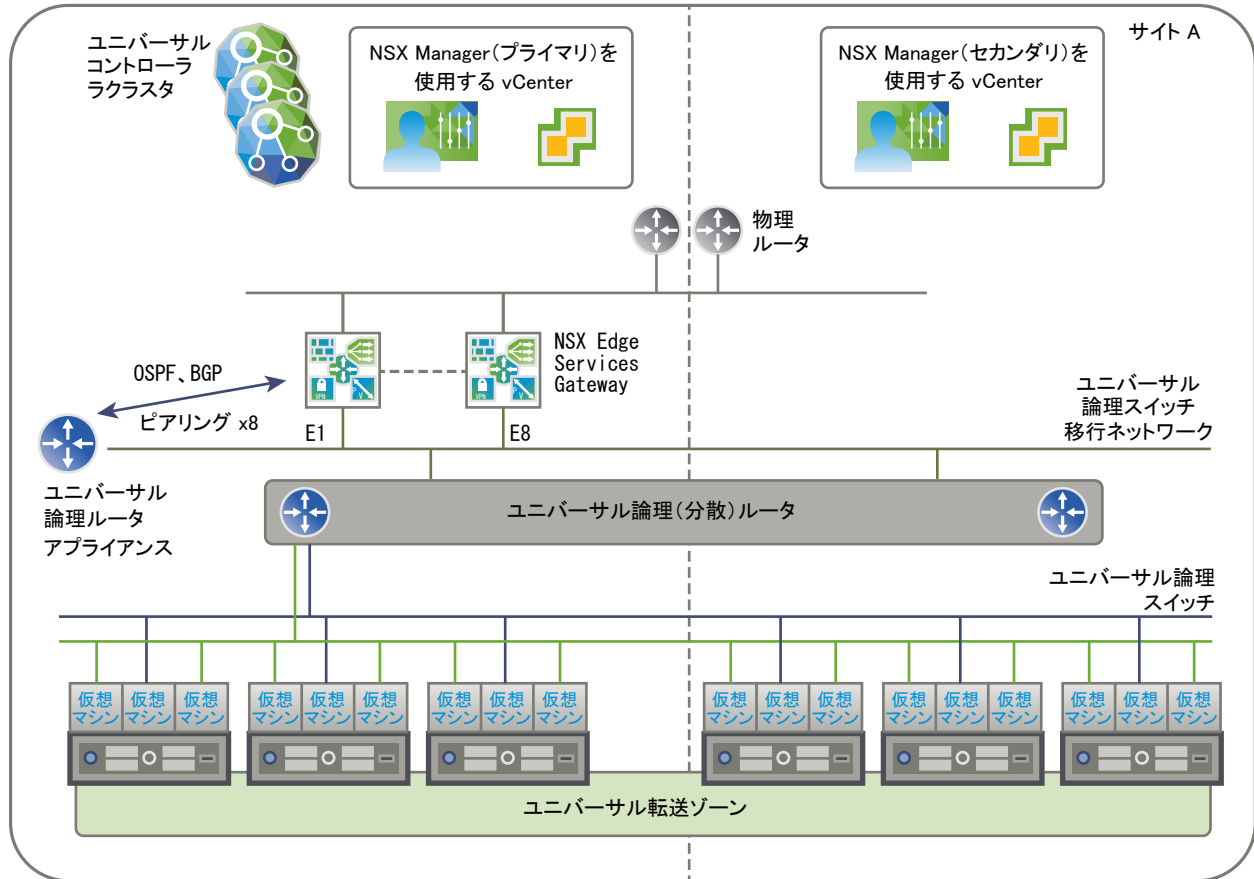
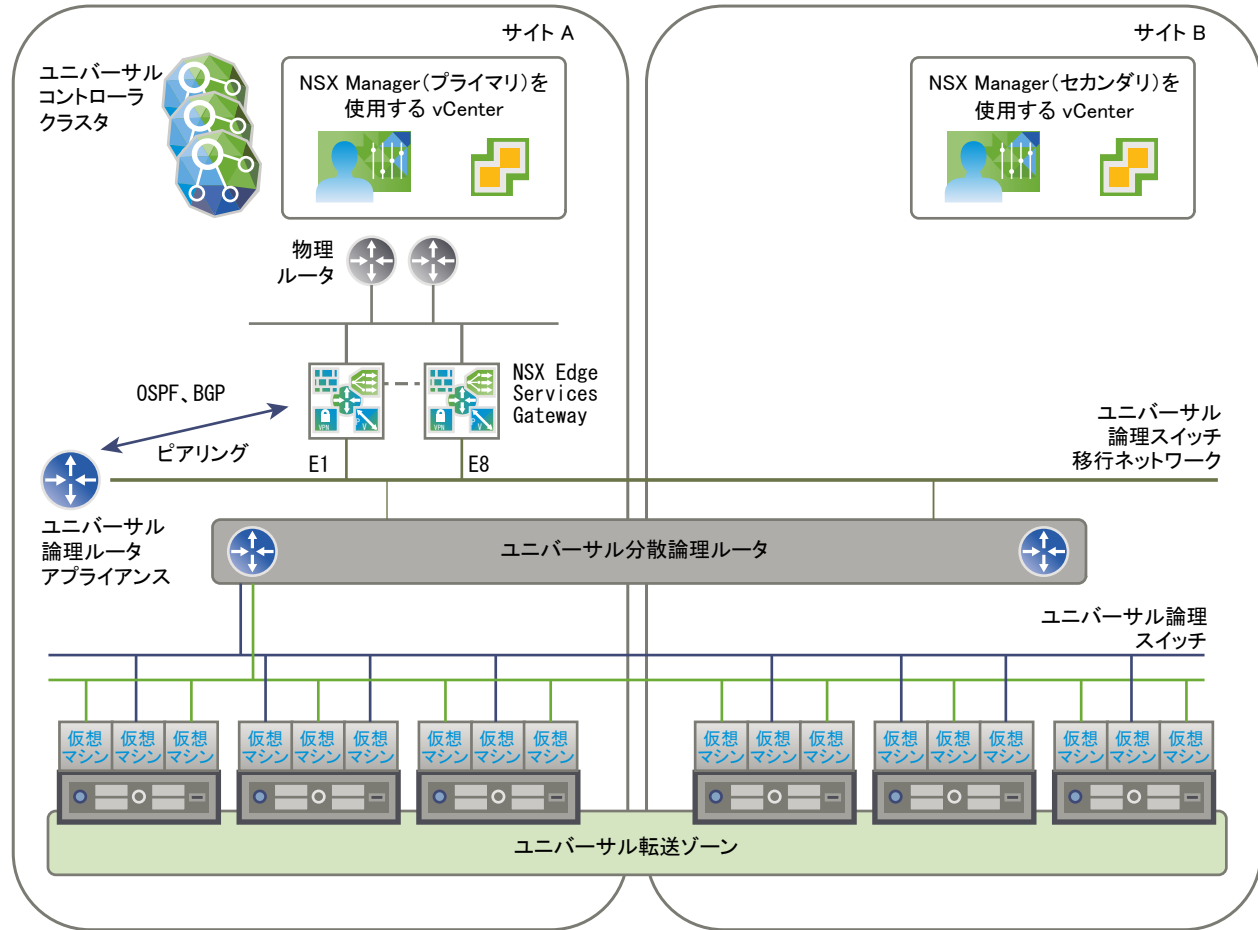


図 4-2. 2 つのサイトにまたがる Cross-vCenter NSX

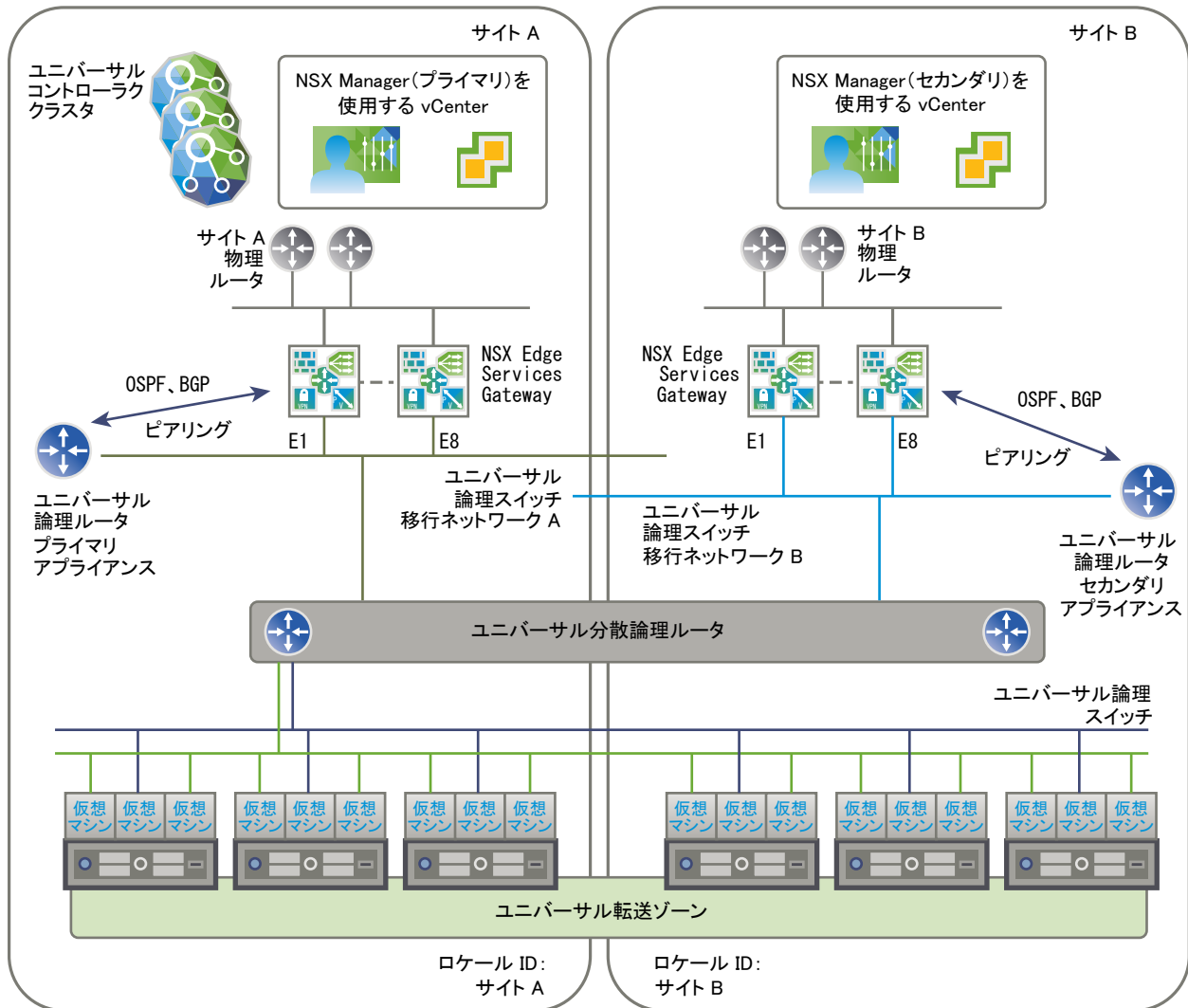


Local Egress（ローカル出力側）

マルチサイト Cross-vCenter NSX 環境のすべてのサイトは、出力側トラフィックに同じ物理ルーターを使用できます。ただし、出力側ルートをカスタマイズする必要がある場合は、ユニバーサル分散論理ルーターを作成するとき、Local Egress（ローカル出力側）機能を有効にする必要があります。これにより、ユニバーサル分散論理ルーター、クラスター、またはホスト レベルでルートをカスタマイズできます。

マルチサイトにおける Cross-vCenter NSX 環境を示す次の例では、Local Egress（ローカル出力側）が有効になっています。各サイトの Edge Services Gateway (ESG) には、そのサイトの物理ルーター経由でトラフィックを送出するデフォルトのルートがあります。ユニバーサル分散論理ルーターは、各サイトに 1 つずつ、計 2 台のアプライアンスで設定されています。アプライアンスは、自サイトの ESG からルートを学習します。学習したルートはユニバー

サル コントローラ クラスタに送信されます。Local Egress（ローカル出力側）が有効になっているため、サイトのロケール ID がこれらのルートに関連付けられます。ユニバーサル コントローラ クラスタは、対応するロケール ID を持つルートホストに送信します。サイト A のアプライアンスで学習されたルートはサイト A のホストに、サイト B のアプライアンスで学習されたルートはサイト B のホストに送信されます。



NSX Manager ロールの変更

NSX Manager には、プライマリ ロール、セカンダリ ロール、またはスタンドアロン ロールの 3 つのロールがあります。プライマリ NSX Manager では特殊な同期ソフトウェアが動作しており、すべてのユニバーサル オブジェクトがセカンダリ NSX Manager と同期されます。

NSX Manager のロールを変更する際には、それによって何が行われるのかを理解しておくことが重要です。

プライマリとして設定	NSX Manager のロールをプライマリに設定して、同期ソフトウェアを開始します。NSX Manager のロールがすでにプライマリまたはセカンダリになっている場合、この操作は失敗します。
(セカンダリから) スタンドアロンとして設定	NSX Manager のロールをスタンドアロン モードまたは移行モードに設定します。この操作は、NSX Manager がすでにスタンドアロン ロールになっている場合、失敗することがあります。
(プライマリから) スタンドアロンとして設定	プライマリ NSX Manager をスタンドアロン モードまたは移行モードにリセットし、同期ソフトウェアを停止して、すべてのセカンダリ NSX Manager の登録を解除します。この操作は、NSX Manager がすでにスタンドアロンになっているか、いずれかのセカンダリ NSX Manager が到達不能の場合、失敗することがあります。
プライマリから接続解除	セカンダリ NSX Manager に対してこの操作を実行すると、そのセカンダリ NSX Manager は、プライマリ NSX Manager から一方的に接続解除されます。この操作は、プライマリ NSX Manager でリカバリ不能な障害が発生しており、セカンダリ NSX Manager を新しいプライマリに登録する必要がある場合に使用します。元のプライマリ NSX Manager が正常な状態に復帰した場合、データベースには、このセカンダリ NSX Manager が登録されたままの状態になっています。この問題を解決するには、元のプライマリ NSX Manager からセカンダリ NSX Manager を接続解除（登録解除）する際に、[force] オプションを指定します。[force] オプションを指定すると、元の NSX Manager のデータベースからセカンダリ NSX Manager が削除されます。

トランスポート ゾーン

トランスポート ゾーンは、論理スイッチがアクセスできるホストを制御します。トランスポート ゾーンは 1 つ以上の vSphere クラスタにまたがって設定できます。トランスポート ゾーンでは、特定のネットワークを使用できるクラスタと仮想マシンを指定します。Cross-vCenter NSX 環境では、ユニバーサルトランスポート ゾーンを作成し、そこに環境内の任意の vCenter Server からのクラスタを含めることができます。ユニバーサルトランスポート ゾーンは 1 つしか作成できません。

NSX 環境には、要件に基づいて 1 つ以上のトランスポート ゾーンを設定できます。ホスト クラスタは、複数のトランスポート ゾーンに属することができます。論理スイッチは、1 つのトランスポート ゾーンのみに属することができます。

NSX は、異なるトランスポート ゾーンに属する仮想マシンの接続を許可しません。論理スイッチの範囲は 1 つのトランスポート ゾーンに制限されるため、異なるトランスポート ゾーンにある仮想マシンは同じレイヤー 2 ネットワーク上に配置できません。分散論理ルーターを、異なるトランスポート ゾーンに属する論理スイッチに接続することはできません。最初の論理スイッチを接続したら、それ以降の論理スイッチは、同じトランスポート ゾーンにある論理スイッチから選択する必要があります。同様に、Edge Services Gateway (ESG) は、1 つのトランスポート ゾーンの論理スイッチにのみアクセスできます。

トランスポート ゾーンを設計する際には、次のガイドラインを参考にしてください。

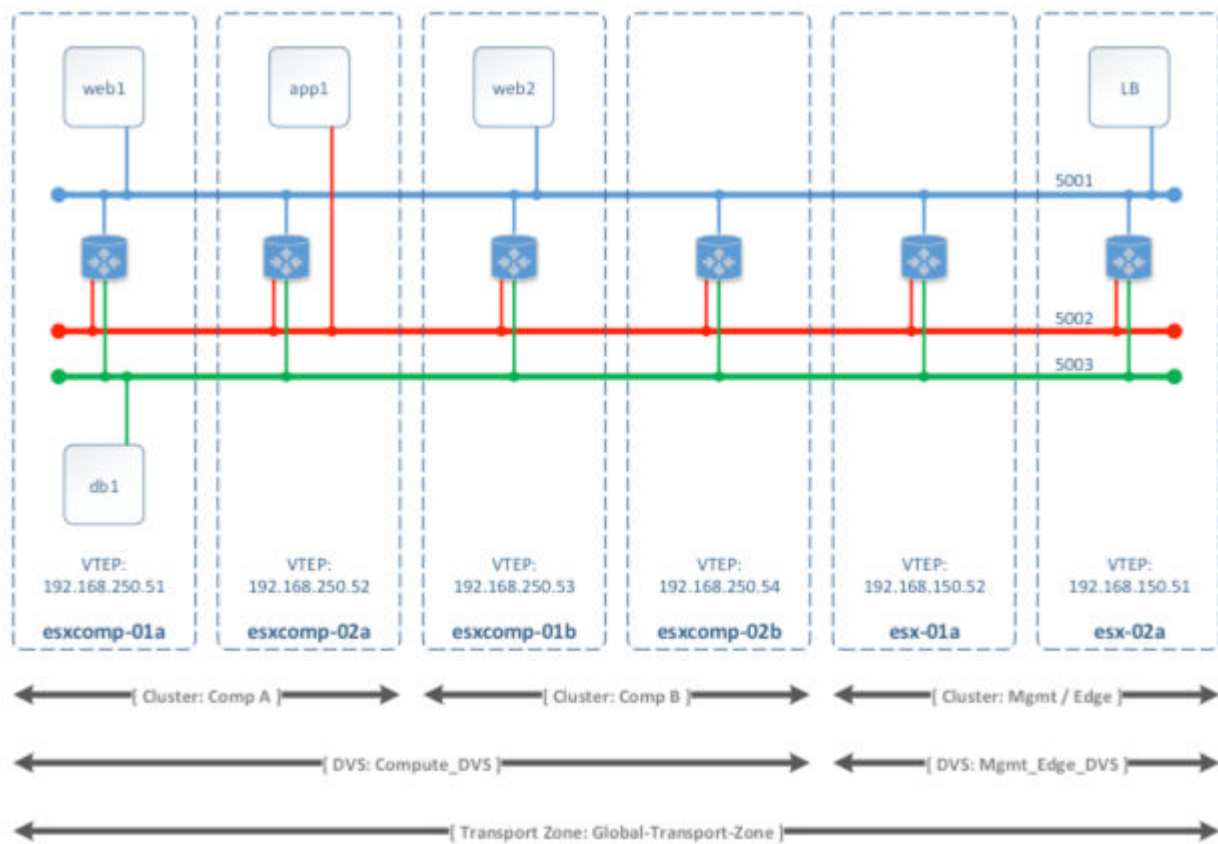
NSX は、異なるトランスポート ゾーンに属する仮想マシンの接続を許可しません。論理スイッチの範囲は 1 つのトランスポート ゾーンに制限されるため、異なるトランスポート ゾーンにある仮想マシンは同じレイヤー 2 ネットワーク上に配置できません。分散論理ルーターを、異なるトランスポート ゾーンに属する論理スイッチに接続することはできません。最初の論理スイッチを接続したら、それ以降の論理スイッチは、同じトランスポート ゾーンにある論理スイッチから選択する必要があります。同様に、Edge Services Gateway (ESG) は、1 つのトランスポート ゾーンの論理スイッチにのみアクセスできます。

トランスポート ゾーンを設計する際には、次のガイドラインを参考にしてください。

- レイヤー 3 接続が必要なクラスタは、Edge クラスタ（レイヤー 3 Edge デバイス（分散論理ルーターや Edge Services Gateway）があるクラスタ）と同じトランスポート ゾーンに属している必要があります。
- Web サービス用とアプリケーション サービス用の 2 つのクラスタがあるとしします。これらの 2 つのクラスタの仮想マシン間で VXLAN 接続を行うには、両方のクラスタが同じトランスポート ゾーンに属している必要があります。

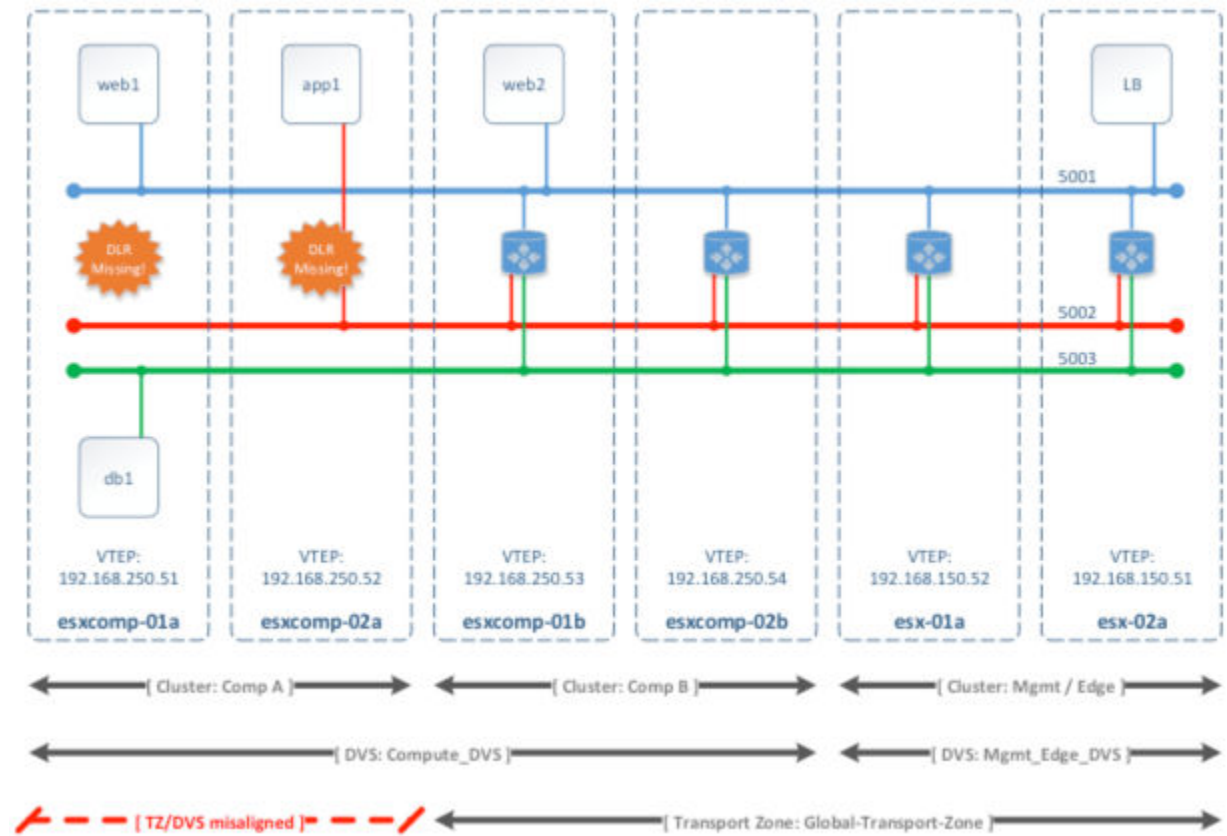
- 同じトランスポート ゾーンに属しているすべての論理スイッチは、そのトランスポート ゾーンに属しているクラスタ内のすべての仮想マシンで認識され、使用することができます。セキュリティで保護された環境がクラスタに含まれている場合、他のクラスタの仮想マシンがその環境を使用できることは望ましくありません。この場合は、セキュリティで保護されたクラスタを隔離されたトランスポート ゾーンに配置できます。
- vSphere Distributed Switch (VDS または DVS) の範囲は、トランスポート ゾーンの範囲と一致している必要があります。マルチクラスタ VDS 構成でトランスポート ゾーンを作成する場合、選択した VDS 内のすべてのクラスタがそのトランスポート ゾーンに属していることを確認します。これにより、VDS dvPortgroup が使用可能なすべてのクラスタで DLR が使用できるようになります。

次の図では、トランスポート ゾーンが VDS 境界に正しく合わせられています。



このベスト プラクティスを使用しない場合に注意すべき点があります。それは、VDS が複数のホスト クラスタにまたがっている場合に、トランスポート ゾーンにそれらのクラスタの 1 つ（またはサブセット）が含まれていると、そのトランスポート ゾーン内のすべての論理スイッチが、VDS の範囲に含まれるすべてのクラスタの仮想マシンにアクセスできることです。つまり、トランスポート ゾーンによって論理スイッチの範囲をクラスタのサブセットに制限することはできません。この論理スイッチが後で DLR に接続される場合、レイヤー 3 の問題を回避するために、トランスポート ゾーンに属しているクラスタにのみルーター インスタンスが作成されていることを確認する必要があります。

たとえば、トランスポートゾーンがVDS境界と合っていないと、論理スイッチ（5001、5002、5003）とそれらの論理スイッチが接続される DLR インスタンスの範囲の結合が解除されて、クラスタ Comp A 内の仮想マシンが DLR 論理インターフェイス (LIF) にアクセスできなくなります。



この章には、次のトピックが含まれています。

- [トランスポートゾーンの追加](#)
- [トランスポートゾーンの表示と編集](#)
- [トランスポートゾーンの拡張](#)
- [トランスポートゾーンの縮小](#)

トランスポートゾーンの追加

トランスポートゾーンは、論理スイッチがアクセスできるホストを制御します。1つのトランスポートゾーンは1つ以上のvSphereクラスタにまたがることができます。トランスポートゾーンでは、特定のネットワークを使用できるクラスタと仮想マシンを指定します。ユニバーサルトランスポートゾーンは、Cross-vCenter NSX環境内のvSphereクラスタにまたがる可能性があります。


Cross-vCenter NSX環境に配置できるユニバーサルトランスポートゾーンは1つだけです。

前提条件

変更を加える適切な NSX Manager を決定します。

- スタンドアロン環境や単一の vCenter NSX の環境では、NSX Manager は 1 つしか存在しないため、NSX Manager を選択する必要はありません。
- ユニバーサル オブジェクトはプライマリ NSX Manager から管理する必要があります。
- NSX Manager に対してローカルなオブジェクトは、NSX Manager から管理する必要があります。
- 拡張リンク モードが有効になっていない Cross-vCenter NSX 環境で設定の変更を行うには、変更する NSX Manager にリンクされた vCenter Server から変更を行う必要があります。
- 拡張リンク モードの Cross-vCenter NSX 環境では、リンクされた任意の vCenter Server から、任意の NSX Manager の設定を変更できます。NSX Manager ドロップダウン メニューから、適切な NSX Manager を選択します。

手順


- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール手順 (Installation)] に移動し、[論理ネットワークの準備 (Logical Network Preparation)] タブを選択します。
- 2 [トランスポート ゾーン (Transport Zones)] をクリックし、[新規トランスポート ゾーン (New Transport Zone)] () アイコンをクリックします。
- 3 (オプション) ユニバーサル トランスポート ゾーンを追加するには、[このオブジェクトをユニバーサル同期の対象としてマーク (Mark this object for universal synchronization)] を選択します。
- 4 次のように、レプリケーション モードを選択します。
 - [マルチキャスト (Multicast)] : 物理ネットワーク上のマルチキャスト IP アドレスを制御プレーンに使用します。このモードは、古い VXLAN デプロイからアップグレードする場合にのみ推奨されます。物理ネットワークに PIM/IGMP が必要です。
 - [ユニキャスト (Unicast)] : 制御プレーンは、NSX コントローラによって処理されます。すべてのユニキャストトラフィックで、最適化されたヘッドエンド レプリケーションを利用します。マルチキャスト IP アドレスや特別なネットワーク設定は必要ありません。
 - [ハイブリッド (Hybrid)] : ローカルトラフィック レプリケーションを物理ネットワーク (L2 マルチキャスト) にオフロードします。最初のホップのスイッチで IGMP スヌーピング、各 VTEP サブネットの IGMP クエリアへのアクセスが必要ですが、PIM は不要です。最初のホップスイッチは、サブネットのトラフィック レプリケーションを処理します。

重要: ユニバーサルトランスポート ゾーンを作成し、レプリケーション モードとしてハイブリッドを選択する場合、使用するマルチキャスト アドレスが、環境内の NSX Manager 上で割り当てられた他のどのマルチキャスト アドレスとも競合しないようにする必要があります。

- 5 トランスポート ゾーンに追加するクラスタを選択します。

Transport-Zone は、このトランスポート ゾーンが作成された NSX Manager にローカルなトランスポート ゾーンです。

Universal-Transport-Zone は、Cross-vCenter NSX 環境内のすべての NSX Manager で使用できる、ユニバーサル トランスポート ゾーンです。

Name	1 ▲ Description	Control Plane Mode	Logical Switches
 Transport-Zone		Unicast	1
 Universal-Transport-Zone		Unicast	4

次のステップ

トランスポート ゾーンを追加した場合は、論理スイッチを追加できます。

ユニバーサル トランスポート ゾーンを追加した場合は、ユニバーサル論理スイッチを追加できます。

ユニバーサル トランスポート ゾーンを追加した場合は、セカンダリ NSX Manager を選択し、そのクラスタをユニバーサル トランスポート ゾーンに追加できます。

トランスポート ザーンの表示と編集

選択したトランスポート ザーンの論理ネットワーク、そのトランスポート ザーンのクラスタ、およびそのトランスポート ザーンの制御プレーン モードを表示できます。

手順

- 1 [転送ゾーン] で、トランスポート ザーンをダブルクリックします。

[サマリ] タブには、トランスポート ザーンの名前と説明、およびそのトランスポート ザーンに関連付けられている論理スイッチの数が表示されます。[転送ゾーンの詳細] には、トランスポート ザーン内のクラスタが表示されます。

- 2 [転送ゾーンの詳細 (Edit Settings)] セクションで [設定の編集 (Transport Zone Details)] アイコンをクリックしてトランスポート ザーンの名前、説明、または制御プレーン モードを編集します。

トランスポート ザーンの制御プレーン モードを変更する場合は、[既存の論理スイッチを新しい制御プレーン モードに移行する (Migrate existing Logical Switches to the new control plane mode)] を選択し、このトランスポート ザーンにリンクされている既存の論理スイッチの制御プレーン モードを変更してください。このチェック ボックスを選択しないと、編集後にこのトランスポート ザーンにリンクされている論理スイッチのみが新しい制御プレーン モードになります。

- 3 [OK] をクリックします。

トランスポート ザーンの拡張


トランスポート ザーンにクラスタを追加できます。新しく追加されたクラスタで、既存のトランスポート ザーンすべてが利用できるようになります。

前提条件

トランスポート ザーンに追加するクラスタは、インストール済みのネットワーク インフラストラクチャがある、VXLAN 用に構成されたものとします。『NSX インストール ガイド』を参照してください。

手順


- 1 [トランスポート ザーン] で、トランスポート ザーンをクリックします。

- 2 [クラスタの追加 (Add Cluster)] () アイコンをクリックします。
- 3 トランスポート ゾーンに追加するクラスタを選択し、[OK] をクリックします。

トランスポート ゾーンの縮小

クラスタをトランスポート ゾーンから削除できます。既存のトランスポート ゾーンのサイズは、縮小されたスコープに合わせて削減されます。

手順

- 1 [転送ゾーン (Transport Zones)] で、トランスポート ゾーンをダブルクリックします。
- 2 [転送ゾーンの詳細 (Transport Zones Details)] で [クラスタの削除 (Remove Clusters)] () アイコンをクリックします。
- 3 削除するクラスタを選択します。
- 4 [OK] をクリックします。

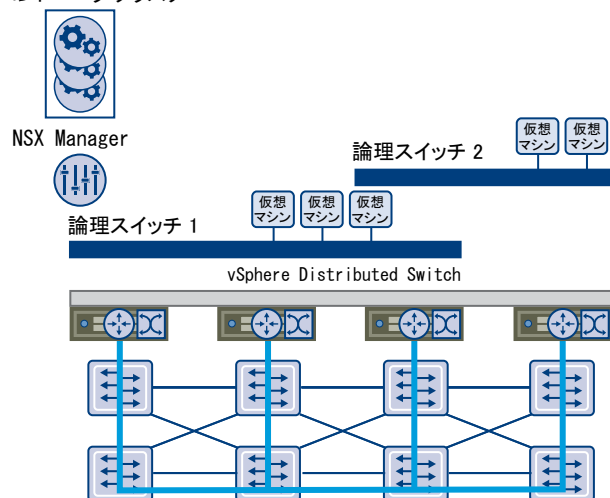
論理スイッチ

クラウド デプロイ環境や仮想データセンターでは、複数のテナント間にさまざまなアプリケーションが存在します。セキュリティ、障害分離および IP アドレス重複の問題を回避するために、これらのアプリケーションおよびテナントは互いに分離させる必要があります。NSX の論理スイッチにより、論理ブロードキャスト ドメインまたはセグメントが作成され、アプリケーションまたはテナントの仮想マシンを論理的に接続できます。これにより、デプロイの柔軟性および速度が確保され、同時に、物理レイヤー 2 のスプロールやスパンニングツリーといった問題が生じることなく、物理ネットワークのブロードキャスト ドメイン (VLAN) のすべての特性が引き続き提供されます。

論理スイッチは分散され、大規模な計算クラスタに任意に拡張できます。これにより、物理レイヤー 2 (VLAN) 境界の制限を受けることなく、データセンター内での仮想マシンのモビリティ (vMotion) が確保されます。論理スイッチのソフトウェアにはブロードキャスト ドメインが含まれているため、物理インフラストラクチャで MAC/FIB テーブルの制限に対処する必要はありません。

論理スイッチは一意の VXLAN にマッピングされますが、これにより仮想マシンのトラフィックがカプセル化されて物理 IP ネットワークを越えて転送されます。

コントローラ クラスタ



NSX Controller は、ネットワーク内のすべての論理スイッチの集中制御ポイントであり、すべての仮想マシン、ホスト、論理スイッチ、および VXLAN の情報を管理します。このコントローラは、ユニキャストとハイブリッドという 2 つの新しい論理スイッチ制御プレーン モードをサポートします。これらのモードは、物理ネットワークから NSX を切り離します。VXLAN では、論理スイッチ内でブロードキャスト、不明なユニキャスト、およびマルチキャスト (BUM) トラフィックを処理するためのマルチキャストをサポートする上で、物理ネットワークが不要になります。ユニキャスト モードでは、すべての BUM トラフィックがホストでローカルにレプリケートされ、物理ネットワーク設

定が不要です。ハイブリッドモードでは、パフォーマンス向上のために、一部の BUM トラフィック レプリケーションが第 1 ホップの物理スイッチにオフロードされます。このモードでは、最初の物理ホップスイッチをオンにするために IGMP スヌーピングが必要です。論理スイッチ内の仮想マシンは、IPv6 やマルチキャストなどの任意のタイプのトラフィックを使用して送信します。

L2 ブリッジを追加することで、論理スイッチを物理デバイスにまで拡張することができます。章 8 [L2 ブリッジ] を参照してください。

論理スイッチを管理するには、Super Administrator または Enterprise Administrator ロールの権限が必要です。

この章には、次のトピックが含まれています。

- [論理スイッチの追加](#)
- [論理スイッチへの仮想マシンの接続](#)
- [論理スイッチの接続のテスト](#)
- [論理スイッチでのなりすましの防止](#)
- [論理スイッチの編集](#)
- [論理スイッチのシナリオ](#)

論理スイッチの追加

前提条件

- 論理スイッチを設定および管理するための、Super Administrator または Enterprise Administrator ロールの権限を所有している。
- ファイアウォールルールで VXLAN UDP ポートが開いている（該当する場合）。VXLAN UDP ポートは API を使用して設定できます。
- 物理インフラストラクチャの MTU が、仮想マシン vNIC の MTU より最低でも 50 バイト大きい。
- vCenter Server の [ランタイム設定] で、各 vCenter Server の管理対象 IP アドレスが設定されている。『vCenter Server and Host Management』を参照してください。
- VMKNic への IP 割り当てで DHCP を使用する場合は、VXLAN 転送 VLAN で DHCP を使用できる。
- 指定されたトランスポートゾーン内では、一貫性のある分散仮想スイッチタイプ（ベンダーなど）とバージョンが使用されている。スイッチタイプに一貫性がないと、定義されていない動作が論理スイッチで実行される可能性があります。
- 適切な LACP チーミングポリシーを設定し、物理 NIC をポートに接続している。チーミングモードの詳細については、VMware vSphere のマニュアルを参照してください。
- Link Aggregation Control Protocol (LACP) に対して、5 タプル ハッシュ分散が有効になっている。
- マルチキャストモードでは、VXLAN トラフィックがルーターをトラバースしている場合に、マルチキャストルーティングが有効になっている。マルチキャストアドレス範囲をネットワーク管理者から取得している必要があります。
- ESX ホストがコントローラと通信するために、ポート 1234（デフォルトのコントローラ待機ポート）がファイアウォール上で開いている。

- (推奨) マルチキャストおよびハイブリッドモードでは、VXLAN 参加ホストが接続する L2 スイッチで、IGMP スヌーピングを有効にしている。IGMP スヌーピングが L2 で有効になっている場合は、マルチキャスト対応のネットワークと接続しているルーター または L3 スイッチ上で IGMP クエリアが有効になっている必要があります。

論理スイッチの追加

NSX 論理スイッチは、基盤となるハードウェアから完全に分離された仮想環境内で、切り替え機能（ユニキャスト、マルチキャスト、ブロードキャスト）を再現します。論理スイッチは、仮想マシンを接続できるネットワーク接続を提供する点で、VLAN と似ています。論理スイッチは、単一の vCenter NSX のデプロイに対してローカルです。Cross-vCenter NSX 環境では、すべての vCenter Server にわたって使用可能なユニバーサル論理スイッチを作成できます。トランスポートゾーンのタイプによって、新しいスイッチが論理スイッチまたはユニバーサル論理スイッチのどちらであるかが決まります。

前提条件

表 6-1. 論理スイッチまたはユニバーサル論理スイッチの作成の前提条件


論理スイッチ	ユニバーサル論理スイッチ
<ul style="list-style-type: none"> ■ vSphere Distributed Switch が設定されている ■ NSX Manager をインストールがインストールされている ■ コントローラがデプロイされている ■ ホスト クラスタが NSX 用に準備されている ■ VXLAN が設定されている ■ セグメント ID プールが設定されている ■ トランスポート ゾーンが作成されている 	<ul style="list-style-type: none"> ■ vSphere Distributed Switch が設定されている ■ NSX Manager をインストールがインストールされている ■ コントローラがデプロイされている ■ ホスト クラスタが NSX 用に準備されている ■ VXLAN が設定されている ■ プライマリ NSX Manager が割り当てられている必要があります。 ■ ユニバーサル セグメント ID アドレス プールが設定されている必要があります。 ■ ユニバーサルトランスポート ゾーンが作成されている必要があります。

変更を加える適切な NSX Manager を決定します。

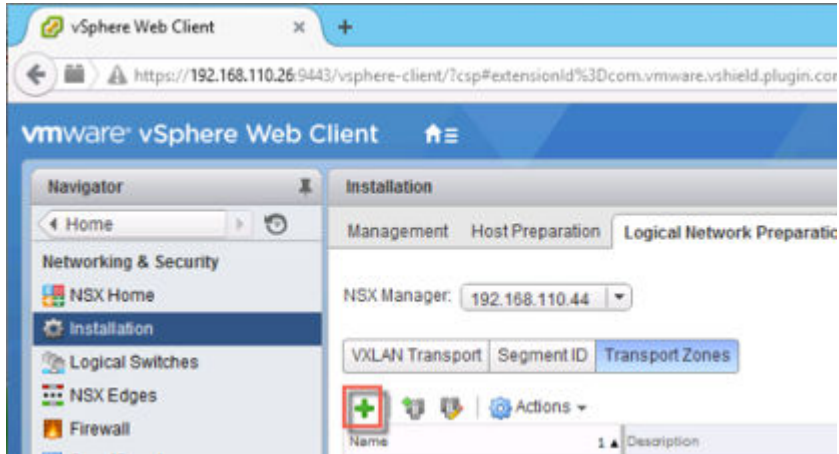
- スタンドアロン環境や単一の vCenter NSX の環境では、NSX Manager は 1 つしか存在しないため、NSX Manager を選択する必要はありません。
- ユニバーサル オブジェクトはプライマリ NSX Manager から管理する必要があります。
- NSX Manager に対してローカルなオブジェクトは、NSX Manager から管理する必要があります。
- 拡張リンク モードが有効になっていない Cross-vCenter NSX 環境で設定の変更を行うには、変更する NSX Manager にリンクされた vCenter Server から変更を行う必要があります。
- 拡張リンク モードの Cross-vCenter NSX 環境では、リンクされた任意の vCenter Server から、任意の NSX Manager の設定を変更できます。NSX Manager ドロップダウン メニューから、適切な NSX Manager を選択します。

手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [論理スイッチ (Logical Switches)] の順に移動します。

- 2 論理スイッチを作成する NSX Manager を選択します。ユニバーサル論理スイッチを作成する場合は、プライマリ NSX Manager を選択する必要があります。
- 3 [新規論理スイッチ (New Logical Switch)] () アイコンをクリックします。

次はその例です。



- 4 論理スイッチの名前と説明（説明は任意）を入力します。
- 5 論理スイッチを作成するトランスポートゾーンを選択します。ユニバーサルトランスポートゾーンを選択すると、ユニバーサル論理スイッチが作成されます。

デフォルトでは、論理スイッチはトランスポートゾーンから制御プレーンレプリケーションモードを継承します。このモードは、他の選択可能なモードの1つに変更できます。選択可能なモードはユニキャスト、ハイブリッド、およびマルチキャストです。

ユニバーサル論理スイッチを作成し、レプリケーションモードとしてハイブリッドを選択する場合、使用するマルチキャストアドレスが、環境内の NSX Manager 上で割り当てられた他のどのマルチキャストアドレスとも競合しないようにする必要があります。

- 6 (オプション) [IP 検出の有効化 (Enable IP Discovery)] をクリックして ARP 抑制を有効にします。

この設定により、個々の VXLAN セグメント内、つまり同じ論理スイッチに接続されている仮想マシン間の ARP トラフィックのフラッドを最小限に抑えることができます。IP 検出はデフォルトで有効になっています。

- 7 (オプション) 仮想マシンに複数の MAC アドレスが存在する場合や、VLAN をトランッキングしている仮想 NIC を仮想マシンで使用している場合は、[MAC ラーニングの有効化 (Enable MAC learning)] をクリックします。

MAC ラーニングを有効にすると、VLAN/MAC ペアのラーニング テーブルが各 vNIC に構築されます。このテーブルは dvfilter データの一部として保管されます。vMotion の実行時に、dvfilter はこのテーブルを新しい場所に保存してリストアします。次に、スイッチはテーブル内のすべての VLAN/MAC エントリに対して RARP を発行します。

この例には、デフォルト設定の app 論理スイッチが表示されています。

New Logical Switch

Name: * app

Description:

Transport Zone: * tz1 Change Remove

Replication mode:

- ☐ Multicast
Multicast on Physical network used for VXLAN control plane.
- ☒ Unicast
VXLAN control plane handled by NSX Controller Cluster.
- ☐ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

☒ Enable IP Discovery

☐ Enable MAC Learning

OK Cancel

DB-Tier-00 は、トランスポートゾーンに接続された論理スイッチです。この論理スイッチは、これが作成された NSX Manager でのみ使用できます。

DB-Tier-01 は、ユニバーサルトランスポートゾーンに接続されたユニバーサル論理スイッチです。このユニバーサル論理スイッチは、Cross-vCenter NSX 環境内のどの NSX Manager でも使用できます。

論理スイッチとユニバーサル論理スイッチには、異なるセグメント ID アドレス プールからのセグメント ID があります。

DB-Tier-00	✓ Normal	Transport-Zone	10000	Unicast
DB-Tier-01	✓ Normal	Universal-Transport-Zone	900003	Unicast

次のステップ

論理スイッチまたはユニバーサル論理スイッチに仮想マシンを追加します。


分散論理ルーターを作成して論理スイッチに接続します。これにより、異なる論理スイッチに接続された仮想マシン間の接続が可能になります。

ユニバーサル分散論理ルーターを作成してユニバーサル論理スイッチに接続します。これにより、異なるユニバーサル論理スイッチに接続された仮想マシン間の接続が可能になります。

論理スイッチの NSX Edge への接続

論理スイッチを NSX Edge Services Gateway または NSX Edge 分散論理ルーターに接続すると、外部に接続する、または高度なサービスを提供する水平方向のトラフィック ルーティング（論理スイッチ間）あるいは垂直方向のトラフィック ルーティングになります。

手順

- 1 [論理スイッチ] で、NSX Edge を接続する論理スイッチを選択します。
- 2 [NSX Edge の接続 (Connect an Edge)] () アイコンをクリックします。
- 3 論理スイッチを接続する NSX Edge を選択して、[次へ (Next)] をクリックします。
- 4 論理スイッチに接続するインターフェイスを選択して、[次へ (Next)] をクリックします。
論理ネットワークは通常、内部インターフェイスに接続されています。
- 5 [NSX Edge インターフェイスの編集] ページで、NSX Edge インターフェイスの名前を入力します。
- 6 [内部 (Internal)] または [アップリンク (Uplink)] をクリックして、内部とアップリンクのどちらのインターフェイスなのかを指定します。
- 7 インターフェイスの接続ステータスを選択します。
- 8 論理スイッチを接続する NSX Edge に [手動高可用性の設定 (Manual HA Configuration)] が選択されている場合は、2 つの管理 IP アドレスを CIDR 形式で指定します。
- 9 必要に応じてデフォルトの MTU を編集します。
- 10 [次へ (Next)] をクリックします。
- 11 NSX Edge 接続の詳細を確認し、[終了 (Finish)] をクリックします。

論理スイッチでのサービスのデプロイ

サードパーティのサービスを論理スイッチにデプロイできます。

前提条件

インフラストラクチャにサードパーティの仮想アプライアンスが 1 つ以上インストールされている必要があります。

手順


- 1 [論理スイッチ (Logical Switches)] で、サービスをデプロイする論理スイッチを選択します。
- 2 [サービス プロファイルの追加 (Add Service Profile)] () アイコンをクリックします。
- 3 適用するサービスとサービス プロファイルを選択します。

- 4 [OK] をクリックします。

論理スイッチへの仮想マシンの接続

仮想マシンを、論理スイッチまたはユニバーサル論理スイッチに接続できます。

手順

- 1 [論理スイッチ (Logical Switches)] で、仮想マシンを追加する論理スイッチを選択します。
- 2 [仮想マシンの追加 (Add Virtual Machine)] () アイコンをクリックします。
- 3 論理スイッチに追加する仮想マシンを選択します。
- 4 接続する vNIC を選択します。
- 5 [次へ (Next)] をクリックします。
- 6 選択した vNIC を確認します。
- 7 [終了 (Finish)] をクリックします。

論理スイッチの接続のテスト

ping テストで、VXLAN 転送ネットワーク内の 2 つのホストが相互にアクセス可能かどうかを確認します。

- 1 [論理スイッチ (Logical Switches)] で、テストする論理スイッチを [名前 (Name)] 列でダブルクリックします。
- 2 [監視 (Monitor)] タブをクリックします。
- 3 [ホスト (Hosts)] タブをクリックします。
- 4 [送信元のホスト] セクションで [参照 (Browse)] をクリックします。[ホストの選択] ダイアログ ボックスで、接続先ホストを選択します。
- 5 テスト パケットのサイズを選択します。

VXLAN の標準サイズは、断片化なしで 1550 バイト（物理インフラストラクチャの MTU に一致）です。このサイズによって NSX は接続をチェックし、VXLAN トラフィック用にインフラストラクチャが準備されているかどうかを検証できます。

パケット サイズを最小化すると、断片化が可能になります。したがって、最小化されたパケット サイズでは、NSX は接続をチェックできますが、インフラストラクチャが大きなフレーム サイズに対応できるかどうかはチェックできません。

- 6 [宛先のホスト] セクションで [参照 (Browse)] をクリックします。[ホストの選択] ダイアログ ボックスで、接続先ホストを選択します。
- 7 [テストの開始 (Start Test)] をクリックします。

ホスト間の ping テストの結果が表示されます。

論理スイッチでのなりすましの防止

vCenter Server と同期した後、NSX Manager は各仮想マシン上の VMware Tools から、または有効になっていれば IP アドレス検出からすべての vCenter Server ゲスト仮想マシンの IP アドレスを収集します。NSX は、VMware Tools または IP アドレス検出で取得されるすべての IP アドレスを信頼するわけではありません。仮想マシンのセキュリティが侵害された場合は、IP アドレスのなりすましにより、悪意のあるデータ転送がファイアウォール ポリシーを通り抜ける可能性があります。

SpoofGuard では VMware Tools または IP アドレス検出から報告された IP アドレスを認証し、なりすましを防ぐために必要に応じて変更することができます。SpoofGuard は本質的に VMX ファイルと vSphere SDK から集められた仮想マシンの MAC アドレスを信用します。Firewall ルールと別に運用することにより、SpoofGuard を使用して、なりすましと判断されたトラフィックをブロックすることができます。

詳細については、[章 13 「SpoofGuard の使用」](#) を参照してください。

論理スイッチの編集

論理スイッチの名前、説明、および制御プレーン モードを編集できます。

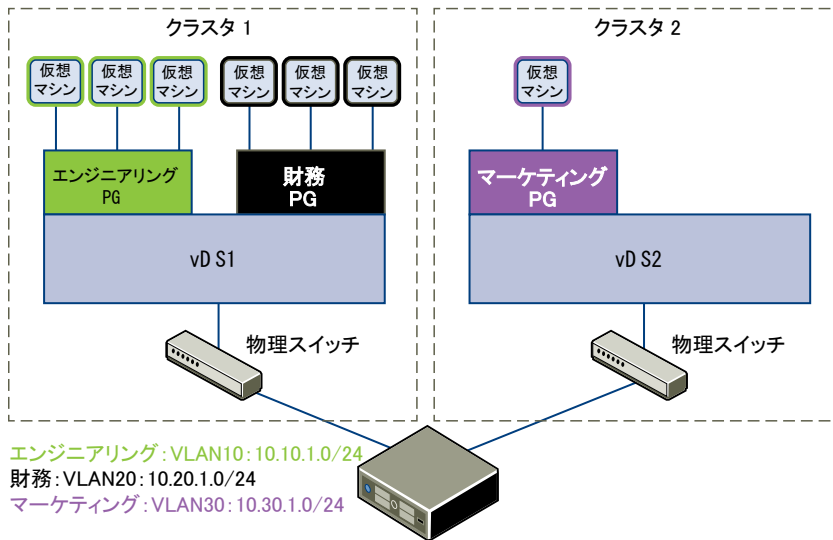
手順

- 1 [論理スイッチ (Logical Switches)] で、編集する論理スイッチを選択します。
- 2 [編集 (Edit)] アイコンをクリックします。
- 3 必要な変更を行います。
- 4 [OK] をクリックします。

論理スイッチのシナリオ

このシナリオでは、ACME Enterprise という会社のデータセンター ACME_Datacenter に、2 つのクラスタに属するいくつかの ESX ホストが存在する状況を示します。エンジニアリング部門（ポート グループ PG - エンジニアリング）と財務部門（ポート グループ PG - 財務）は Cluster1 に属しています。マーケティング部門（PG - マーケティング）は Cluster2 に属しています。クラスタは両方とも、1 つの vCenter Server 5.5 によって管理されています。

図 6-1. 論理スイッチを実装する前の ACME Enterprise のネットワーク

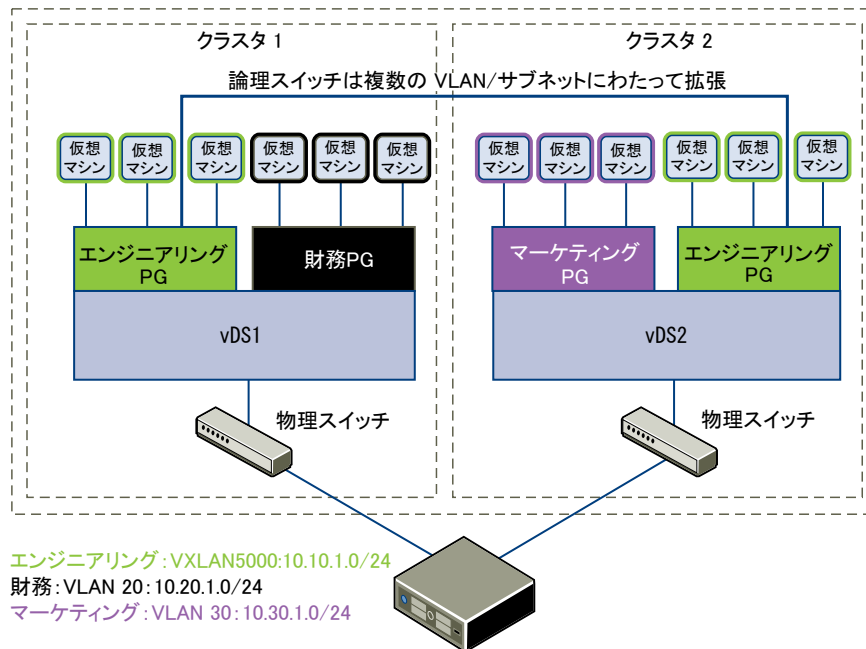


ACME では、Cluster2 の使用率が低いのに対し、Cluster1 の計算領域は使い果たそうとしています。ACME のネットワーク管理者は、管理者 John（ACME の仮想化管理者）に対して、エンジニアリング部門を Cluster2 に拡張し、両方のクラスタのエンジニアリングに属する仮想マシンが相互に通信できるようにする方法を見つけ出すよう依頼します。これにより ACME は、ACME の L2 レイヤーを拡張することによって両方のクラスタのコンピューティング能力を活用することができます。

管理者 John がこの処理を従来の方法で行った場合には、特殊な方法で別々の VLAN に接続することによって、2 つのクラスタが同じ L2 ドメインに含まれるようにする必要があります。この場合、ACME には新しい物理デバイスを購入してトラフィックを分離することが求められ、VLAN スプロール、ネットワーク ループ、および運用管理上のオーバーヘッドなどの問題が発生する可能性があります。

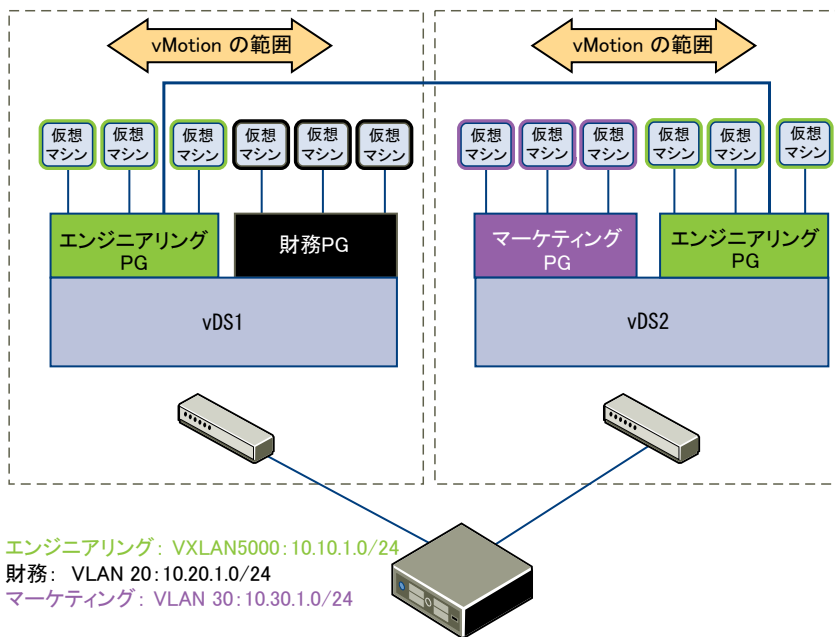
管理者 John は、VMworld で見た論理ネットワークのデモを思い出し、NSX を評価することにします。John は、dvSwitch1 と dvSwitch2 にわたる論理スイッチを構築することによって、ACME の L2 レイヤーを拡張できるという結論を下します。John は NSX Controller を利用できるため、既存の IP ネットワーク上で NSX を機能させることができ ACME の物理インフラストラクチャに手を加える必要がありません。

図 6-2. ACME Enterprise による論理スイッチの実装



管理者 John は 2 つのクラスターにわたる論理スイッチを構築した後、vDS 内の仮想マシンを vMotion で移動できます。

図 6-3. 論理ネットワーク上の vMotion



管理者 John が ACME Enterprise で論理ネットワークを構築する手順を見ていきましょう。

管理者 John による NSX Manager へのセグメント ID プールとマルチキャストアドレス範囲の割り当て

管理者 John は、受信したセグメント ID プールを指定して Company ABC のネットワーク トラフィックを分離する必要があります。

前提条件

- 1 管理者 John は、dvSwitch1 と dvSwitch2 が VMware Distributed Switch バージョン 5.5 であることを確認します。
- 2 管理者 John は、vCenter Server の管理 IP アドレスを設定します。
 - a [管理 (Administration)] - [vCenter Server 設定 (vCenter Server Settings)] - [ランタイム設定 (Runtime Settings)] を選択します。
 - b [vCenter Server の管理 IP] に **10.115.198.165** と入力します。
 - c [OK] をクリックします。
- 3 管理者 John は、Cluster1 と Cluster2 にネットワーク仮想化コンポーネントをインストールします。『NSX インストール ガイド』を参照してください。
- 4 管理者 John は、ACME の NSX Manager 管理者から、セグメント ID プール (5000 - 5250) を受け取ります。John は NSX Controller を利用しているため、物理ネットワーク内でマルチキャストを必要としません。
- 5 管理者 John は IP プールを作成して、その IP アドレス プールから VXLAN VTEP に対して固定 IP アドレスを割り当てることができるようにします。[\[IP アドレス プールの追加\]](#) を参照してください。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] をクリックします。
- 2 [論理ネットワークの準備 (Logical Network Preparation)] タブをクリックし、[セグメント ID (Segment ID)] をクリックします。
- 3 [編集 (Edit)] をクリックします。
- 4 [セグメント ID アドレス プール] に **5000 - 5250** と入力します。
- 5 [マルチキャスト アドレス指定の有効化 (Enable multicast addressing)] は選択しないでください。
- 6 [OK] をクリックします。

管理者 John による VXLAN 転送パラメータの設定

管理者 John は、Cluster1 および Cluster2 で VXLAN を設定します。この設定では、John は各クラスタを vDS にマッピングします。クラスタをスイッチにマッピングすると、そのクラスタ内の各ホストが論理スイッチで使用可能になります。

手順

- 1 [ホストの準備 (Host Preparation)] タブをクリックします。
- 2 Cluster1 で、[VXLAN] 列の [設定 (Configure)] を選択します。
- 3 [VXLAN ネットワークの] ダイアログ ボックスで、クラスタの仮想分散スイッチとして dvSwitch1 を選択します。
- 4 ACME 転送 VLAN として使用する dvSwitch1 に対して **10** と入力します。
- 5 [転送属性の指定] で、dvSwitch1 の最大転送ユニット (MTU) を 1600 のままにします。

MTU は、それ以上小さなパケットに分割しなくても 1 つのパケットで伝送することができる最大データ量です。管理者 John は、VXLAN の論理スイッチのトラフィック フレームのサイズがカプセル化のために若干大きくなっており、そのため各スイッチの MTU を 1550 以上に設定する必要があることを認識しています。

- 6 [Vmknic IP アドレス (VMKNic IP Addressing)] で、[IP アドレス プールの使用 (Use IP Pool)] を選択し、IP アドレス プールを選択します。
- 7 [VMKNic チーミング ポリシー (VMKNic Teaming Policy)] で [フェイルオーバー (Failover)] を選択します。
管理者 John は、平常時でも障害時でも、論理スイッチのパフォーマンスが一定になるようにすることで、ネットワークのサービス品質を維持しようと考えています。このため、チーミング ポリシーとしてフェイルオーバーを選択することにしました。
- 8 [追加 (Add)] をクリックします。
- 9 ステップ 4 ~ 8 を繰り返して、Cluster2 で VXLAN を設定します。

管理者 John が Cluster1 と Cluster2 を適切なスイッチにマッピングした後、それらのクラスタのホストが論理スイッチ用に準備されます。

- 1 VXLAN カーネル モジュールと vmknick が Cluster1 と Cluster2 の各ホストに追加されます。
- 2 論理スイッチに関連付けられている vSwitch 上に特別な dvPortGroup が作成され、VMKNic がそのグループに接続されます。

管理者 John によるトランスポート ゾーンの追加

論理ネットワークをバックアップする物理ネットワークは、transport zone と呼ばれます。トランスポート ゾーンは、仮想ネットワークによってスパンニングされたコンピューティング範囲です。

手順

- 1 [論理ネットワークの準備 (Logical Network Preparation)] をクリックして、[トランスポート ゾーン (Transport Zones)] をクリックします。
- 2 [新規トランスポート ゾーン (New Transport Zone)] アイコンをクリックします。
- 3 [名前] に [ACME ゾーン (ACME Zone)] と入力します。
- 4 [説明] に [ACME のクラスタを含むゾーン (Zone containing ACME's clusters)] と入力します。
- 5 Cluster 1 と Cluster 2 を選択して、トランスポート ゾーンに追加します。
- 6 [制御プレーン モード (Control Plane Mode)] で [ユニキャスト (Unicast)] を選択します。

7 [OK] をクリックします。

管理者 John による論理スイッチの作成

VXLAN 転送パラメータの設定が完了すると、管理者 John が論理スイッチを作成する準備が整ったことになります。

手順

- 1 [論理スイッチ (Logical Switches)] をクリックし、次に [新しい論理ネットワーク (New Logical Network)] アイコンをクリックします。
- 2 [名前] に **ACME logical network** と入力します。
- 3 [説明] に **Logical Network for extending ACME Engineering network to Cluster2** と入力します。
- 4 [トランスポート ゾーン (Transport Zone)] で、ACME Zone を選択します。
- 5 [OK] をクリックします。

NSX は、dvSwitch1 と dvSwitch2 の間の L2 接続を可能にする論理スイッチを作成します。

次のステップ

これで管理者 John は、ACME の本番仮想マシンを論理スイッチに接続し、その論理スイッチを NSX Edge Services Gateway または分散論理ルーターに接続できます。

ハードウェア ゲートウェイの設定

ハードウェア ゲートウェイの設定で、物理ネットワークを仮想ネットワークにマッピングします。マッピングを設定することにより、NSX が Open vSwitch Database (OVSDb) を利用できるようになります。

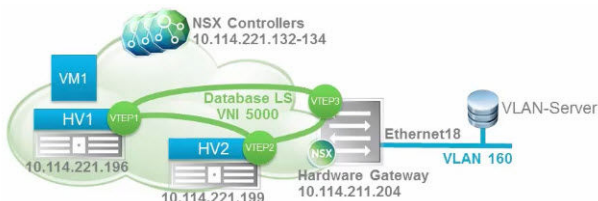
OVSDb データベースには、物理ハードウェアと仮想ネットワークについての情報が含まれます。ベンダーのハードウェアがデータベース サーバをホストします。

NSX 論理ネットワーク内のハードウェア ゲートウェイ スイッチは、VXLAN トンネルの終端となります。そのハードウェア ゲートウェイは、仮想ネットワークからはハードウェア VTEP として認識されます。VTEP の詳細については、『NSX インストール ガイド』と『NSX Network Virtualization Design Guide』を参照してください。

ハードウェア ゲートウェイの最小トポロジには、次のコンポーネントが含まれます。

- 物理サーバ
- ハードウェア ゲートウェイ スイッチ (L2 ポート)
- IP ネットワーク
- 4 個以上のハイパーバイザー。仮想マシンを持つ 4 個以上のレプリケーション クラスタを含む
- 3 台以上のノードがあるコントローラ クラスタ

次に示すのは、ハードウェア ゲートウェイを利用するトポロジのサンプルで、HV1 と HV2 はそれぞれハイパーバイザーです。VM1 は HV1 上の仮想マシンです。VTEP1 は HV1、VTEP2 は HV2、VTEP3 はハードウェア ゲートウェイ上にあります。ハードウェア ゲートウェイのサブネットは 211 です。これは、2 つのハイパーバイザーのサブネット 221 とは異なります。



ハードウェア ゲートウェイの基盤となる構成では、次のコンポーネントのうちいずれかを利用できます。

- 1 台のスイッチ
- IP アドレスが異なる複数の物理バス スイッチ

■ ハードウェア スイッチ コントローラと複数のスイッチ

NSX コントローラは、NSX コントローラの IP アドレスから、ポート 6640 でハードウェア ゲートウェイと通信します。この接続を利用して、ハードウェア ゲートウェイの OVSDB のトランザクションを送受信します。

シナリオ：ハードウェア ゲートウェイのサンプル構成

このシナリオでは、NSX 環境でハードウェア ゲートウェイ スイッチを構成するための一般的なタスクについて説明します。一連のタスクを通じて、ハードウェア ゲートウェイを使用して仮想マシン VM1 を物理サーバに接続する方法と、ハードウェア ゲートウェイを使用して WebService 論理スイッチを VLAN-Server VLAN 160 に接続する方法を説明します。

サンプルのトポロジでは、仮想マシン VM1 と VLAN-Server にサブネット 10 の IP アドレスが設定されています。VM1 は WebService 論理スイッチに接続されています。VLAN-Server は物理サーバ上の VLAN 160 に接続されています。



前提条件

- ベンダーのドキュメントを参照して、物理ネットワークの要件を満たしていることを確認してください。
- ハードウェア ゲートウェイを構成するために、NSX のシステムとハードウェアの要件を満たしていることを確認してください。章 1 「NSX のシステム要件」を参照してください。
- 論理ネットワークが正しく設定されていることを確認してください。『NSX インストール ガイド』を参照してください。
- VXLAN トランスポート パラメータが正確にマッピングされていることを確認してください。『NSX インストール ガイド』を参照してください。
- ハードウェア ゲートウェイのベンダーの証明書を取得してください。
- VXLAN ポートの値が 4789 に設定されていることを確認してください。『NSX アップグレード ガイド』を参照してください。

REST API のコマンド `PUT /2.0/vdn/config/vxlan/udp/port/4789` を使用してポート番号を修正することができます。この API は応答を返しません。

手順

1 レプリケーション クラスタの設定

レプリケーション クラスタは、ハードウェア ゲートウェイから送信されたブロードキャスト トラフィックを転送する、ハイパーバイザーのセットです。ブロードキャスト トラフィックは、不明なユニキャストまたはマルチキャスト トラフィックの場合があります。

2 ハードウェア ゲートウェイの NSX Controller への接続

ハードウェア ゲートウェイを NSX Controller に接続するには、トップオブブラック (ToR) 物理スイッチ上に OVSDB 管理テーブルを設定する必要があります。

3 ハードウェア ゲートウェイの証明書の追加

構成を機能させるには、ハードウェア ゲートウェイの証明書をハードウェア デバイスに追加する必要があります。

4 論理スイッチの物理スイッチへのバインド

仮想マシン VM1 に接続された WebService 論理スイッチは、同じサブネット上にあるハードウェア ゲートウェイと通信する必要があります。

レプリケーション クラスタの設定

レプリケーション クラスタは、ハードウェア ゲートウェイから送信されたブロードキャスト トラフィックを転送する、ハイパーバイザーのセットです。ブロードキャスト トラフィックは、不明なユニキャストまたはマルチキャスト トラフィックの場合があります。

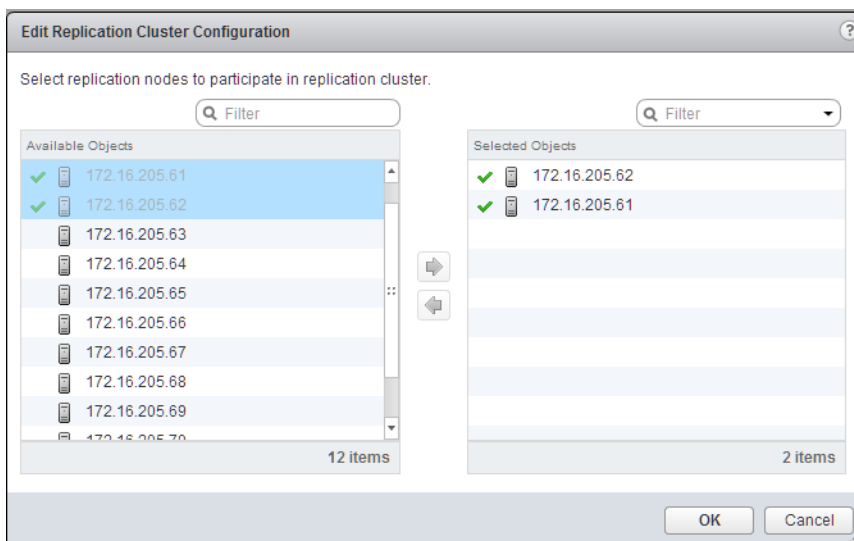
注: レプリケーション ノードとハードウェア ゲートウェイ スイッチの IP サブネットを同じにすることはできません。

前提条件

レプリケーション ノードとして機能するハイパーバイザーを利用できることを確認してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] - [サービス定義]の順に選択します。
- 3 [ハードウェア デバイス] タブをクリックします。
- 4 [レプリケーション クラスタ] セクションで [編集] をクリックして、このレプリケーション クラスタでレプリケーション ノードとして機能するハイパーバイザーを選択します。
- 5 ハイパーバイザーを選択して青い矢印をクリックします。



選択されたハイパーバイザーが [選択したオブジェクト] 列に移動します。

- 6 [OK] をクリックします。

レプリケーション ノードがレプリケーション クラスタに追加されました。レプリケーション クラスタには、1 台以上のホストが必要です。

ハードウェア ゲートウェイの NSX Controller への接続

ハードウェア ゲートウェイを NSX Controller に接続するには、トップオブラック (ToR) 物理スイッチ上に OVSDB 管理テーブルを設定する必要があります。

NSX コントローラは、ToR 物理スイッチからの接続を待機します。そのため、ハードウェア ゲートウェイは、接続を開始するために OVSDB 管理テーブルを使用する必要があります。

手順

- 1 環境に適したコマンドを使用して、ハードウェア ゲートウェイを NSX Controller に接続します。

ハードウェア ゲートウェイを NSX Controller に接続するためのサンプルのコマンドは次のとおりです。

```
prmh-nsx-tor-7050sx-3#enable
prmh-nsx-tor-7050sx-3#configure terminal
prmh-nsx-tor-7050sx-3(config)#cvx
prmh-nsx-tor-7050sx-3(config-cvx)#service hsc
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#manager 172.16.2.95 6640
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#no shutdown
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#end
```

- 2 ハードウェア ゲートウェイ上で OVSDB 管理テーブルを設定します。
- 3 OVSDB のポート番号を 6640 に設定します。
- 4 (オプション) ハードウェア ゲートウ NSX Controller に接続していることを確認します。
 - 接続状態が [UP] であることを確認します。
 - VM1 と VLAN 160 に ping を実行して、接続が成功したことを確認します。
- 5 (オプション) ハードウェア ゲートウェイが適切な NSX Controller に接続していることを確認します。
 - a vSphere Web Client にログインします。
 - b [Networking and Security] - [インストール手順] - [NSX Controller ノード]の順に選択します。

ハードウェア ゲートウェイの証明書の追加

構成を機能させるには、ハードウェア ゲートウェイの証明書をハードウェア デバイスに追加する必要があります。

前提条件

導入環境のハードウェア ゲートウェイの証明書が利用できることを確認します。

手順

- 1 vSphere Web Client にログインします。
- 2 [ネットワークとセキュリティ (Networking & Security)] - [サービス定義 (Service Definitions)]の順に選択します。

- 3 [ハードウェア デバイス (Hardware Devices)] タブをクリックします。
- 4 追加 (+) アイコンをクリックして、ハードウェア ゲートウェイ プロファイルの詳細を作成します。

Add Hardware Device

Name: * hardware_registration

Description:

Certificate: * -----BEGIN CERTIFICATE REQUEST-----
 MII/CujCCAaICAQAwdTElMAkGA1UEBhMCVVMx
 EzARBgNVBAGTCkNhbgGimb3JuaWEx
 EJAQBgNVBAGTCVBhbG8gQWx0bzESMBAGA1U
 ECxMjVGVjaCBQdWJzMRQwEgYDVQQK
 EwtWTXdhcmUgSW5JLJETMBEGA1UEAxiMKdm1
 3YXJILmNvbTCCASIwDQYJKoZIhvdN
 AQEBBQADggEPADCCAQoCggEBAlZaGpix6LIF
 f8DMKpeU4TG39K2OY1P3OWOqX3ev
 wLYkS6WwMRN7TpnA1/OR28HKYiCXZHgqQz

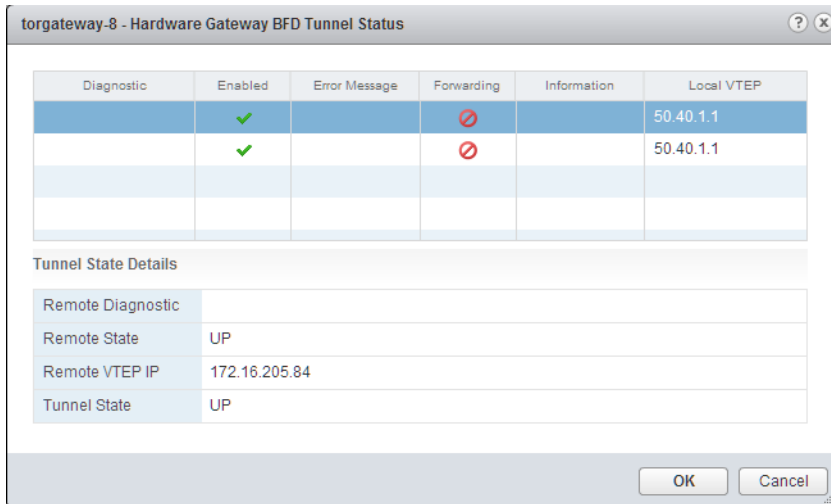
☒ Enable BFD

OK Cancel

オプション	説明
名前と説明	ハードウェア ゲートウェイの名前を指定します。 プロファイルの詳細を説明セクションに追加できます。
証明書	導入環境で利用している証明書をコピーアンドペーストします。
BFD の有効化	双方向フォワーディング検出 (BFD) プロトコルはデフォルトで有効化されています。 BFD プロトコルは、ハードウェア ゲートウェイの設定情報を同期するために使用されます。

- 5 [OK] をクリックします。
ハードウェア ゲートウェイを表すプロファイルが作成されました。
- 6 画面を更新して、ハードウェア ゲートウェイが利用可能であり、稼動していることを確認します。
接続状態は [UP] となります。

- 7 (オプション) ハードウェア ゲートウェイのプロファイルをクリックし、右クリックしてドロップダウン メニューから [BFD トンネル ステータスの表示 (View the BFD Tunnel Status)] を選択します。



ダイアログ ボックスには、トラブルシューティング用にトンネル ステータスの詳細が表示されます。

論理スイッチの物理スイッチへのバインド

仮想マシン VM1 に接続された WebService 論理スイッチは、同じサブネット上にあるハードウェア ゲートウェイと通信する必要があります。

注: ハードウェアのポートに複数の論理スイッチをバインドする場合、それぞれの論理スイッチに対して次の手順を実行する必要があります。

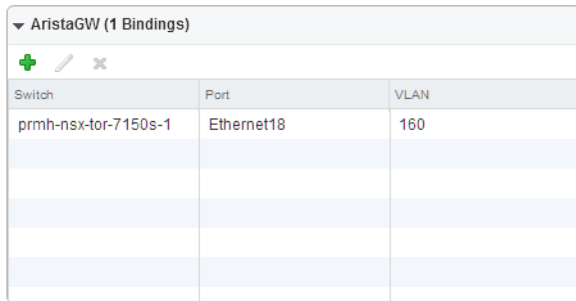
前提条件

- WebService 論理スイッチが使用可能であることを確認します。[「論理スイッチの追加」](#)を参照してください。
- 物理スイッチが使用可能であることを確認します。

手順

- 1 vSphere Web Client にログインします。
- 2 [ネットワークとセキュリティ (Networking & Security)] - [論理スイッチ (Logical Switches)]の順に選択します。
- 3 WebService 論理スイッチを右クリックし、ドロップダウンメニューから [ハードウェア バインドの管理 (Manage Hardware Bindings)] を選択します。
- 4 ハードウェア ゲートウェイのプロファイルを選択します。
- 5 追加 (+) アイコンをクリックし、ドロップダウン メニューから物理スイッチを選択します。
例 : AristaGW
- 6 [選択 (Select)] をクリックし、[使用可能なオブジェクト] の一覧から物理ポートを 1 つ選択します。
例 : Ethernet 18

- 7 [OK] をクリックします。
- 8 VLAN 名を指定します。



▼ AristaGW (1 Bindings)		
+ ✎ ✕		
Switch	Port	VLAN
prmh-nsx-tor-7150s-1	Ethernet18	160

例：160

- 9 [OK] をクリックします。

バインドが完了しました。

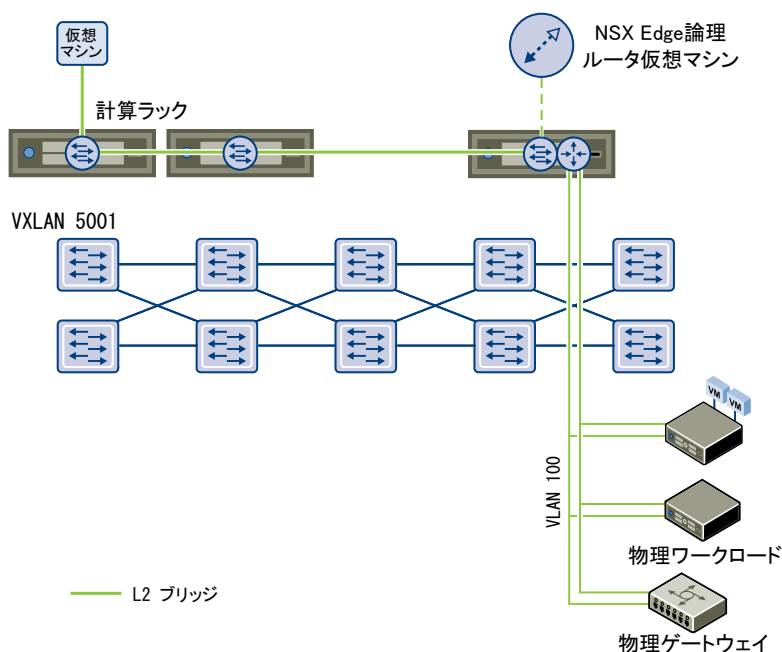
NSX Controller により、物理構成および論理構成の情報がハードウェア ゲートウェイと同期されます。

L2 ブリッジ

論理スイッチと VLAN の間に L2 ブリッジを作成することができます。これにより IP アドレスに影響を与えずに仮想ワークロードを物理デバイスに移行することができます。論理ネットワークでは、論理スイッチ ブロードキャストドメインと VLAN ブロードキャストドメインをブリッジすることで、物理 L3 ゲートウェイを利用して既存の物理ネットワークやセキュリティ リソースにアクセスできます。

L2 ブリッジは、NSX Edge 論理ルーター仮想マシンが設定されたホストで動作します。L2 ブリッジ インスタンスは、単一の VLAN にマッピングされますが、複数のブリッジ インスタンスを存在させることができます。論理ルーターは、ブリッジに接続したデバイスのゲートウェイとして使用することはできません。

論理ルーターで高可用性を有効にしている、プライマリ NSX Edge 仮想マシンが停止した場合は、ブリッジはセカンダリ仮想マシンが設定されたホストに自動的に移動されます。このシームレスな移行を行うためには、セカンダリ NSX Edge 仮想マシンが設定されたホストで VLAN を構成しておく必要があります。



L2 ブリッジを使用して、論理スイッチ同士の接続、VLAN ネットワーク同士の接続、またはデータセンターの相互接続を行わないでください。また、ユニバーサル論理ルーターを使用してブリッジを構成したり、ユニバーサル論理スイッチにブリッジを追加することはできません。

この章には、次のトピックが含まれています。

- [L2 ブリッジの追加](#)
- [論理的にルーティングされた環境への L2 ブリッジの追加](#)

L2 ブリッジの追加

論理スイッチから分散仮想ポート グループへのブリッジを追加できます。

前提条件

環境に NSX 分散論理ルーターがデプロイされている必要があります。

ユニバーサル分散論理ルーターを使用してブリッジを設定することはできません。また、ブリッジをユニバーサル論理スイッチに追加することはできません。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 分散論理ルーターをダブルクリックします。
- 4 [管理] をクリックして、[ブリッジ] をクリックします。
- 5 [追加 (+)] アイコンをクリックします。
- 6 ブリッジの名前を入力します。
- 7 ブリッジを作成する論理スイッチを選択します。
- 8 論理スイッチのブリッジ先である分散仮想ポート グループを選択します。
- 9 [OK] をクリックします。

論理的にルーティングされた環境への L2 ブリッジの追加

1 台の分散論理ルーターで複数のブリッジ インスタンスに対応できますが、ルーティング インスタンスとブリッジ インスタンスで同じ VXLAN/VLAN ネットワークを共有することはできません。ブリッジされた VLAN およびブリッジされた VXLAN とのトラフィックはブリッジされたネットワークにルーティングすることができず、その逆もまた同様です。

前提条件


- 環境に NSX 分散論理ルーターがデプロイされている必要があります。
- ユニバーサル分散論理ルーターを使用してブリッジを設定することはできません。また、ブリッジをユニバーサル論理スイッチに追加することはできません。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 ブリッジに使用される分散論理ルーターをダブルクリックします。

注: ブリッジ インスタンスは VXLAN が接続された同じルーティング インスタンスで作成する必要があります。1 台のブリッジ インスタンスで 1 つの VXLAN および 1 つの VLAN に対応でき、VXLAN と VLAN は重複できません。同じ VXLAN と VLAN は複数のブリッジ インスタンスに接続できません。

- 4 [管理 (Manage)] をクリックして、[ブリッジ (Bridging)] をクリックします。
ルーターとして使用される論理スイッチは「ルーティングは有効です」の状態になります。
- 5 [追加 () (Add)] アイコンをクリックします。
- 6 ブリッジの名前を入力します。
- 7 ブリッジを作成する論理スイッチを選択します。
- 8 論理スイッチのブリッジ先である分散仮想ポート グループを選択します。
- 9 [OK] をクリックします。
- 10 [ブリッジの追加] ウィンドウで再び [OK] をクリックします。
- 11 [発行] をクリックしてブリッジ設定に対する変更を有効にします。

これで、[ルーティングは有効です (Routing Enabled)] を指定した状態でブリッジに使用される論理スイッチが表示されます。詳細は、「[論理スイッチの追加](#)」および「[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。

ルーティング

NSX Edge ごとに固定および動的ルーティングを指定できます。

動的ルーティングにより、レイヤー 2 ブroadcastドメイン間の必要な転送情報が提供されるため、レイヤー 2 ブroadcastドメインを削減し、ネットワークの効率と規模を改善できます。NSX は、このインテリジェンスをワークロードが存在する場所に拡張し、水平方向のルーティングを行います。これより、余分なコストと時間をかけてホップを拡張することなく、より直接的に仮想マシン間の通信ができます。同時に、NSX は垂直方向の接続も提供するため、テナントはパブリック ネットワークにアクセスできます。

この章には、次のトピックが含まれています。

- [論理（分散）ルーターの追加](#)
- [Edge Services Gateway の追加](#)
- [グローバル設定の指定](#)
- [NSX Edge 設定](#)
- [スタティック ルートの追加](#)
- [論理（分散）ルーター上での OSPF の設定](#)
- [Edge Services Gateway 上での OSPF の設定](#)
- [BGP の設定](#)
- [IS-IS プロトコルの設定](#)
- [ルート再配分の設定](#)
- [NSX Manager ロケール ID の表示](#)
- [ユニバーサル分散論理ルーター上でのロケール ID の設定](#)
- [ホストまたはクラスタ上でのロケール ID の設定](#)

論理（分散）ルーターの追加

ホストの論理ルーター カーネル モジュールは、VXLAN ネットワーク間、および仮想ネットワークと物理ネットワーク間のルーティングを実行します。NSX Edge アプライアンスは必要に応じて動的ルーティング機能を提供します。論理ルーターは、Cross-vCenter NSX 環境内のプライマリとセカンダリの NSX Manager に作成できますが、ユニバーサル論理ルーターはプライマリ NSX Manager にのみ作成できます。

以下のリストでは、論理ルーターでのインターフェイス タイプ（アップリンクおよび内部）別の機能サポートについて説明します。

- 動的ルーティング プロトコル（BGP と OSPF）は、アップリンク インターフェイスでのみサポートされます。
- ファイアウォール ルールはアップリンク インターフェイスでのみ適用可能であり、対象は Edge 仮想アプライアンスに送信される制御トラフィックと管理トラフィックに限定されます。
- DLR 管理インターフェイスの詳細については、ナレッジベース記事の「分散論理ルーター制御仮想マシンの管理インターフェイスの検討事項」(<http://kb.vmware.com/kb/2122060>) を参照してください。

前提条件


- Enterprise Administrator または NSX Administrator のロールが割り当てられている必要があります。
- 論理ルーターをインストールするには、環境内に稼働中のコントローラ クラスタが存在している必要があります。
- NSX 論理スイッチを作成する計画がない場合でも、ローカル セグメント ID プールを作成する必要があります。
- 論理ルーターは、NSX コントローラを利用しないとホストにルーティング情報を配布できません。論理ルーターは、Edge Services Gateway (ESG) とは異なり、NSX コントローラがなければ機能しません。論理ルーターを作成または変更する前に、コントローラ クラスタが稼働していて、使用可能であることを確認してください。
- 論理ルーターを VLAN dvPortgroup に接続する場合、論理ルーターの VLAN ベース ARP プロキシが機能するように、論理ルーター アプライアンスがインストールされているすべてのハイパーバイザー ホストが UDP ポート 6999 で相互にアクセスできることを確認します。
- 論理ルーター インターフェイスおよびブリッジインターフェイスは、VLAN ID が 0 に設定されている dvPortgroup には接続できません。
- 特定の論理ルーター インスタンスは、異なるトランスポート ゾーンに存在する論理スイッチには接続できません。これにより、すべての論理スイッチと論理ルーター インスタンスの整合性が確保されます。
- 論理ルーターが複数の vSphere Distributed Switch (VDS) にまたがる論理スイッチに接続されている場合、その論理ルーターを VLAN がバックアップするポートグループに接続することはできません。これにより、ホスト間で論理ルーター インスタンスが論理スイッチ dvPortgroup に正しく関連付けられるようになります。
- 2 つのネットワークが同じ vSphere Distributed Switch 内にある場合は、2 つの異なる分散ポートグループ (dvPortgroup) 上に同じ VLAN ID の論理ルーター インターフェイスを作成しないでください。
- 2 つのネットワークが別々の vSphere Distributed Switch 内にあっても、それらの vSphere Distributed Switch が同じホストを共有している場合は、2 つの異なる dvPortgroup 上に同じ VLAN ID の論理ルーター インターフェイスを作成しないでください。つまり、2 つの dvPortgroup が 2 つの異なる vSphere Distributed Switch 内にある場合、それらの vSphere Distributed Switch がホストを共有していなければ、2 つの異なるネットワーク上に同じ VLAN ID の論理ルーター インターフェイスを作成できます。
- NSX バージョン 6.0 および 6.1 とは異なり、NSX バージョン 6.2 では、論理ルーターでルーティングされる論理インターフェイス (LIF) を VLAN にブリッジされている VXLAN に接続できます。

- ECMP セットアップで ESG を使用している場合は、論理ルーター仮想アプライアンスの配置を選択する際に、そのアップストリーム ESG のいずれかと同じホストに配置しないようにしてください。これを実現するために DRS 非アフィニティ ルールを使用できます。これにより、論理ルーター転送時のホスト障害の影響を軽減できます。1 つのアップストリーム ESG を単独で使用する場合またはその ESG が HA モードの場合は、このガイドラインが適用されません。詳細については、『VMware NSX for vSphere Network Virtualization Design Guide』 (<https://communities.vmware.com/docs/DOC-27683>) を参照してください。

変更を加える適切な NSX Manager を決定します。

- スタンドアロン環境や単一の vCenter NSX の環境では、NSX Manager は 1 つしか存在しないため、NSX Manager を選択する必要はありません。
- ユニバーサル オブジェクトはプライマリ NSX Manager から管理する必要があります。
- NSX Manager に対してローカルなオブジェクトは、NSX Manager から管理する必要があります。
- 拡張リンク モードが有効になっていない Cross-vCenter NSX 環境で設定の変更を行うには、変更する NSX Manager にリンクされた vCenter Server から変更を行う必要があります。
- 拡張リンク モードの Cross-vCenter NSX 環境では、リンクされた任意の vCenter Server から、任意の NSX Manager の設定を変更できます。NSX Manager ドロップダウン メニューから、適切な NSX Manager を選択します。
- 追加する必要がある論理ルーターの種類を決定します。
 - 論理スイッチの接続には論理ルーターが必要です。
 - ユニバーサル論理スイッチには、ユニバーサル論理ルーターが必要になります。
- ユニバーサル論理ルーターを追加する場合、ローカル出力側を有効にする必要があるかどうかを判断します。ローカル出力側を有効にすると、ルートをホストに選択的に送信できます。NSX デプロイが複数のサイトにまたがる場合は、この機能が必要になることがあります。詳細については「[Cross-vCenter NSX トポロジ](#)」を参照してください。ユニバーサル論理ルーターの作成後にローカル出力側を有効にすることはできません。

手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security] > [NSX Edges] の順に移動します。
- 2 変更を加える適切な NSX Manager を選択します。ユニバーサル論理ルーターを作成する場合、プライマリ NSX Manager を選択する必要があります。
- 3 [追加 (Add)] () アイコンをクリックします。
- 4 追加する論理ルーターのタイプを選択します。
 - 選択した NSX Manager に対してローカルな論理ルーターを追加するには、[論理 (分散) ルーター (Logical (Distributed) Router)] を選択します。
 - Cross-vCenter NSX 環境内をまたがることのできる論理ルーターを追加するには、[ユニバーサル論理 (分散) ルーター (Universal Logical (Distributed) Router)] を選択します。このオプションを使用できるのは、プライマリ NSX Manager が割り当てられており、そのプライマリ NSX Manager から変更を行う場合のみです。
 - a [ユニバーサル論理 (分散) ルーター (Universal Logical (Distributed) Router)] を選択する場合は、ローカル出力側を有効にするか選択する必要があります。

5 デバイスの名前を入力します。

この名前は vCenter インベントリに表示されます。1 つのテナントのすべての論理ルーターの中で一意の名前を付けてください。

必要に応じて、ホスト名を入力することもできます。この名前は CLI に表示されます。ホスト名を指定しない場合は、自動的に作成される Edge ID が CLI に表示されます。

必要に応じて、説明やテナントを入力できます。

6 Edge Appliance をデプロイします。

[Edge Appliance のデプロイ (Deploy Edge Appliance)] はデフォルトで選択されています。Edge Appliance (論理ルーターの仮想アプライアンスとも呼ばれる) は、動的ルーティングおよび論理ルーター アプライアンスのファイアウォールで必要になり、論理ルーターの ping、SSH アクセス、および動的ルーティングトラフィックに適用されます。

スタティックルートのみが必要で、Edge Appliance をデプロイしない場合、Edge Appliance オプションを選択解除できます。論理ルーターの作成後に Edge Appliance を論理ルーターに追加することはできません。

7 (オプション) 高可用性を有効にします。

[高可用性の有効化] はデフォルトで選択されていません。[高可用性の有効化] チェックボックスを選択し、高可用性の有効化と設定を行います。動的ルーティングを行う場合、高可用性が必要になります。

8 論理ルーターのパスワードを入力し、再入力します。

パスワードは 12 ～ 255 文字で、次の文字または数字が含まれている必要があります。

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

9 (オプション) SSH を有効にして、ログ レベルを設定します。

デフォルトでは、SSH は無効になっています。SSH を有効にしない場合でも、仮想アプライアンス コンソールを開いて論理ルーターにアクセスできます。ここで SSH を有効にすると、SSH プロセスが論理ルーターの仮想アプライアンスで実行されますが、SSH で論理ルーターのプロトコル アドレスにアクセスできるように論理ルーターのファイアウォール設定を手動で調整する必要があります。プロトコル アドレスの設定は、論理ルーターに動的ルーティングを設定する際に行います。

デフォルトでは、ログ レベルが「緊急」に設定されます。

次はその例です。

New NSX Edge

✓ 1 Name and description
✓ 2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete

Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: * admin

Password: * *****

Confirm password: * *****

☒ Enable SSH access

☐ Enable High Availability


Enable HA, for enabling and configuring High Availability.

Edge Control Level Logging: EMERGENCY

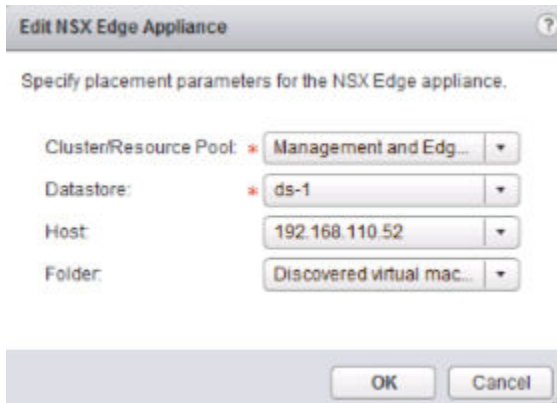
Set the Edge Control Level Logging

Back Next Finish Cancel

10 展開設定を行います。

- ◆ [NSX Edge のデプロイ (Deploy NSX Edge)] を選択しなかった場合、[追加 (Add)] () アイコンはグレイアウトされます。[次へ (Next)] をクリックして、設定を続行します。
- ◆ [NSX Edge のデプロイ (Deploy NSX Edge)] を選択した場合、vCenter インベントリに追加される論理ルーターの仮想アプライアンスの設定を入力します。

次はその例です。



11 インターフェイスを設定します。

論理ルーターでは、IPv4 アドレスのみがサポートされます。

[NSX Edge のデプロイ (Deploy NSX Edge)] を選択した場合は、[高可用性インターフェイスの構成] で、インターフェイスを分散ポート グループに接続する必要があります。高可用性インターフェイス (HA インターフェイス) には、VXLAN 論理スイッチを使用することをお勧めします。2 台の NSX Edge アプライアンスのそれぞれの IP アドレスは、リンク ローカルなアドレス空間 169.250.0.0/16 から選択されます。高可用性サービスの設定はこれで完了です。

注: NSX のこれまでのリリースでは、HA インターフェイスは管理インターフェイスと呼ばれていました。論理ルーターへのリモート アクセスでは、HA インターフェイスはサポートされていません。HA インターフェイスとは異なる IP サブネットから SSH を使用して HA インターフェイスに接続することはできません。HA インターフェイスの外部をポイントするスタティック ルートは設定できません。これは、RPF で受信トラフィックがドロップされることを意味します。理論上は RPF を無効化できますが、高可用性には逆効果です。SSH には論理ルーターのプロトコル アドレスを使用します。これは後で動的ルーティングを設定するときに設定されます。

NSX 6.2 では、論理ルーターの HA インターフェイスは、ルート再配分の対象から自動的に除外されます。

[この NSX Edge のインターフェイスを構成します (Configure interfaces of this NSX Edge)] で、仮想マシン間 (水平方向とも呼ばれます) 通信を可能にするスイッチへの接続には、内部インターフェイスが使用されます。内部インターフェイスは、論理ルーターの仮想アプライアンスの疑似 vNIC として作成されます。アップリンク インターフェイスは、垂直方向の通信を行うためのインターフェイスです。論理ルーター アップリンク インター

フェイスは、NSX Edge Services Gateway、そのサードパーティ製ルーター仮想マシン、または VLAN バックリング dvPortgroup に接続して、論理ルーターを物理ルーターに直接接続できます。動的ルーティングを有効にするには、少なくとも 1 つのアップリンク インターフェイスが必要です。アップリンク インターフェイスは、論理ルーターの仮想アプライアンスの vNIC として作成されます。

ここで入力するインターフェイスの設定は後で変更できます。論理ルーターをデプロイした後で、インターフェイスを追加、削除、および変更できます。

次の例は、管理分散ポートグループに接続された HA インターフェイスを示しています。この例では、2 つの内部インターフェイス (app と web) および 1 つのアップリンク インターフェイス (to-ESG) も示されています。

New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- 4 Configure interfaces**
- 5 Default gateway settings
- 6 Ready to complete

Configure interfaces

HA Interface Configuration

Connected To: [Change](#) [Remove](#)

+ ✎ ✕

IP Address	Subnet Prefix Length
192.168.110.60*	24

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

+ ✎ ✕

Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back Next Finish Cancel

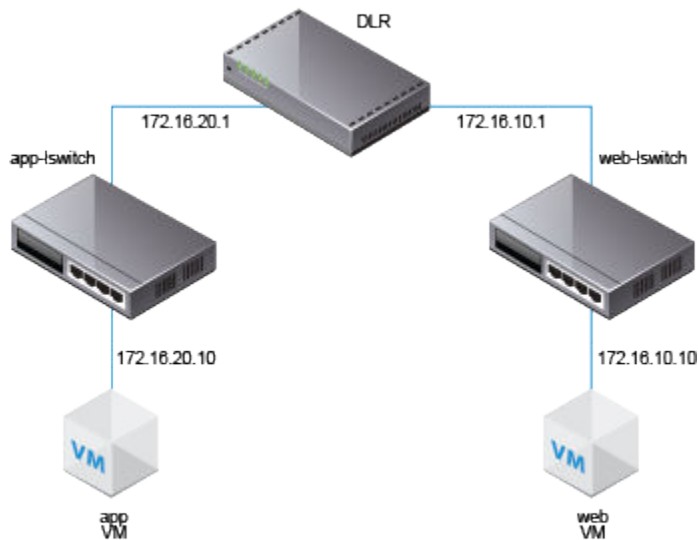
12 デフォルト ゲートウェイを設定します。

次はその例です。

The screenshot shows the 'New NSX Edge' configuration wizard. On the left, a sidebar lists six steps: 1 Name and description, 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings (highlighted), and 6 Ready to complete. The main area is titled 'Default gateway settings' and contains a checkbox 'Configure Default Gateway' which is checked. Below this are three input fields: 'vNIC:' with a dropdown menu showing 'to-ESG', 'Gateway IP:' with the text '192.168.10.1', and 'MTU:' with the text '1500'. At the bottom of the window are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

13 論理スイッチに接続されている仮想マシンのデフォルト ゲートウェイに論理ルーター インターフェイスの IP アドレスが適切に設定されていることを確認します。

次の例のトポロジでは、app 仮想マシンのデフォルト ゲートウェイが 172.16.20.1、web 仮想マシンのデフォルト ゲートウェイが 172.16.10.1 となります。仮想マシンがそのデフォルト ゲートウェイに ping を送信でき、仮想マシン同士でも ping を送信できることを確認します。



SSH を介して NSX Manager にログインし、次のコマンドを実行します。

- すべての論理ルーター インスタンス情報をリストします。

```
nsxmgr-l-01a> show logical-router list all
```

Edge-id	Vdr Name	Vdr id	#Lifs
edge-1	default+edge-1	0x00001388	3

- コントローラ クラスタから論理ルーターのルーティング情報を受信したホストをリストします。

```
nsxmgr-l-01a> show logical-router list dlr edge-1 host
```

ID	HostName
host-25	192.168.210.52
host-26	192.168.210.53
host-24	192.168.110.53

出力には、指定した論理ルーター（この例では edge-1）に接続されている論理スイッチが属するトランスポートゾーンの名前として設定されているすべてのホスト クラスタのホストがすべて表示されます。

- 論理ルーターからホストに通知されるルーティング テーブル情報をリストします。ルーティング テーブル エントリはすべてのホストで一貫している必要があります。

```
nsxmgr-l-01a> show logical-router host host-25 dlr edge-1 route
```

VDR default+edge-1 Route Table

Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]

Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	4101	138800000002
172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10195	13880000000b
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10196	13880000000a
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10196	138800000002
192.168.100.0	255.255.255.0	192.168.10.1	UG	1	AUTO	3802	138800000002

- いずれかのホストに基づいて、ルータに関する追加情報をリストします。これは、ホストと通信しているコントローラを把握するのに便利です。

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

VDR Instance Information :

```
-----
Vdr Name:                default+edge-1
Vdr Id:                  0x00001388
Number of Lifs:          3
Number of Routes:        5
State:                   Enabled
Controller IP:           192.168.110.203
Control Plane IP:        192.168.210.52
Control Plane Active:     Yes
Num unique nexthops:      1
Generation Number:        0
Edge Active:              No
```

`show logical-router host host-25 dlr edge-1 verbose` コマンドの出力で [Controller IP (コントローラ IP)] フィールドを確認します。

SSH を使用してコントローラに接続し、次のコマンドを実行して、コントローラが学習した VNI、VTEP、MAC、および ARP テーブルの状態情報を表示します。

```
192.168.110.202 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled      0
```

VNI 5000 の出力では、接続がゼロであることが示され、VNI 5000 の所有者としてコントローラ 192.168.110.201 がリストされます。そのコントローラにログインして、VNI 5000 の詳細情報を収集します。

```
192.168.110.201 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled      3
```

192.168.110.201 の出力は、接続数が 3 つであることを示しています。他の VNI を確認します。

```
192.168.110.201 # show control-cluster logical-switches vni 5001
VNI      Controller      BUM-Replication ARP-Proxy Connections
5001     192.168.110.201 Enabled           Enabled      3
```

```
192.168.110.201 # show control-cluster logical-switches vni 5002
VNI      Controller      BUM-Replication ARP-Proxy Connections
5002     192.168.110.201 Enabled           Enabled      3
```


192.168.110.201 が 3 つの VNI 接続を所有しているため、もう一方のコントローラ 192.168.110.203 の接続数はゼロであると予想されます。

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled      0
```

- MAC テーブルと ARP テーブルを確認する前に、一方の仮想マシンからもう一方の仮想マシンへの ping 送信を開始します。

app 仮想マシンから Web 仮想マシン：

```
vmware@vmware-virtual-machine:~$ 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_seq=1 ttl=63 time=2.15 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=63 time=1.60 ms
```

MAC テーブルを確認します。

```
192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI      MAC              VTEP-IP      Connection-ID
5000     00:50:56:a6:23:ae 192.168.250.52 7
```

```
192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI      MAC              VTEP-IP      Connection-ID
5001     00:50:56:a6:8d:72 192.168.250.51 23
```

ARP テーブルを確認します。

```
192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI      IP              MAC              Connection-ID
5000     172.16.20.10   00:50:56:a6:23:ae 7
```

```
192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI      IP              MAC              Connection-ID
5001     172.16.10.10   00:50:56:a6:8d:72 23
```

論理ルーター情報を確認します。各論理ルーター インスタンスは、いずれかのコントローラ ノードによって提供されます。

show control-cluster logical-routers コマンドの **instance** サブコマンドを実行すると、このコントローラに接続されている論理ルーターのリストが表示されます。

interface-summary サブコマンドでは、コントローラが NSX Manager から学習した LIF が表示されます。この情報は、トランスポート ゾーンで管理されているホスト クラスタ内のホストに送信されます。

routes サブコマンドでは、論理ルーターの仮想アプライアンス（制御仮想マシンとも呼ばれます）からこのコントローラに送信されるルーティングテーブルが表示されます。この情報は LIF 設定によって提供されるため、ESXi ホストの場合とは異なり、このルーティング テーブルには、直接接続されているサブネットは含まれません。ESXi ホスト上のルート情報には、直接接続されたサブネットが含まれます。これは、ESXi ホストのデータパスがこれを転送テーブルとして使用するためです。

```
controller # show control-cluster logical-routers instance all
LR-Id      LR-Name      Universal Service-Controller Egress-Locale
0x1388     default+edge-1    false      192.168.110.201    local
```

LR-Id を書き留め、次のコマンドで使します。

```
controller # show control-cluster logical-routers interface-summary 0x1388
Interface                                     Type  Id      IP[]
13880000000b                                vxlan 0x1389  172.16.10.1/24
13880000000a                                vxlan 0x1388  172.16.20.1/24
138800000002                                vxlan 0x138a  192.168.10.2/29
```

```
controller # show control-cluster logical-routers routes 0x1388
Destination      Next-Hop[]      Preference Locale-Id      Source
192.168.100.0/24  192.168.10.1    110          00000000-0000-0000-0000-000000000000
CONTROL_VM
0.0.0.0/0         192.168.10.1    0            00000000-0000-0000-0000-000000000000
CONTROL_VM
```

```
[root@comp02a:~] esxcfg-route -l
VMkernel Routes:
Network      Netmask      Gateway      Interface
10.20.20.0   255.255.255.0 Local Subnet  vmk1
192.168.210.0 255.255.255.0 Local Subnet  vmk0
default      0.0.0.0      192.168.210.1 vmk0
```

- コントローラから特定の VNI への接続を表示します。

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
Host-IP      Port  ID
192.168.110.53 26167 4
192.168.210.52 27645 5
192.168.210.53 40895 6
```

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
Host-IP      Port  ID
192.168.110.53 26167 4
192.168.210.52 27645 5
192.168.210.53 40895 6
```

これらのホスト IP アドレスは vmk0 インターフェイスです。VTEP ではありません。ESXi ホストとコントローラとの接続は、管理ネットワーク上で作成されます。ここに示すポート番号は、ホストがコントローラとの接続を確立するときに ESXi ホスト IP スタックによって割り当てられる短期 TCP ポートです。

- ホスト上では、このポート番号と一致するコントローラ ネットワーク接続が表示されます。

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
tcp      0      0 192.168.110.53:26167      192.168.110.101:1234  ESTABLISHED
96416    newreno  netcpa-worker
```

- ホスト上のアクティブな VNI を表示します。ホスト間での出力の違いを確認してください。すべての VNI がすべてのホストでアクティブになるわけではありません。論理スイッチに接続されている仮想マシンがホストにある場合、そのホストの VNI がアクティブになります。

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --
vds-name Compute_VDS
VXLAN ID Multicast IP Control Plane Controller
Connection Port Count MAC Entry Count ARP Entry Count VTEP Count
-----
5000 N/A (headend replication) Enabled (multicast proxy,ARP proxy) 192.168.110.203
(up) 1 0 0 0
5001 N/A (headend replication) Enabled (multicast proxy,ARP proxy) 192.168.110.202
(up) 1 0 0 0
```

注: vSphere 6 以降で vxlan 名前空間を有効にするには、`/etc/init.d/hostd restart` コマンドを実行します。

ハイブリッドまたはユニキャストモードの論理スイッチの場合、`esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` コマンドの出力は次のようになります。

- [Control Plance (制御プレーン)] が有効になっていることが示されます。
- マルチキャスト プロキシおよび ARP プロキシがリストされます。AARP プロキシは、IP 検出が無効になっていてもリストされます。

- 有効なコントローラ IP アドレスのリストと、接続可能であることが示されます。
- 論理ルーターが ESXi ホストに接続されている場合は、[Port Count (ポート カウント)] が 1 以上になります。これは、論理スイッチに接続されたホストに仮想マシンがない場合も同様です。この 1 つのポートは vdrPort で、ESXi ホストの論理ルーターのカーネル モジュールに接続されている特殊な dvPort です。
- まず、仮想マシンから別のサブネット上の仮想マシンに ping を送信し、MAC テーブルを表示します。[Inner MAC (内側の MAC)] は仮想マシン エントリであり、[Outer MAC (外側の MAC)] と [Outer IP (外側の IP)] は VTEP を指していることに注意してください。

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-  
name=Compute_VDS --vxlan-id=5000
```

Inner MAC	Outer MAC	Outer IP	Flags
00:50:56:a6:23:ae	00:50:56:6a:65:c2	192.168.250.52	00000111

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-  
name=Compute_VDS --vxlan-id=5001
```

Inner MAC	Outer MAC	Outer IP	Flags
02:50:56:56:44:52	00:50:56:6a:65:c2	192.168.250.52	00000101
00:50:56:f0:d7:e4	00:50:56:6a:65:c2	192.168.250.52	00000111

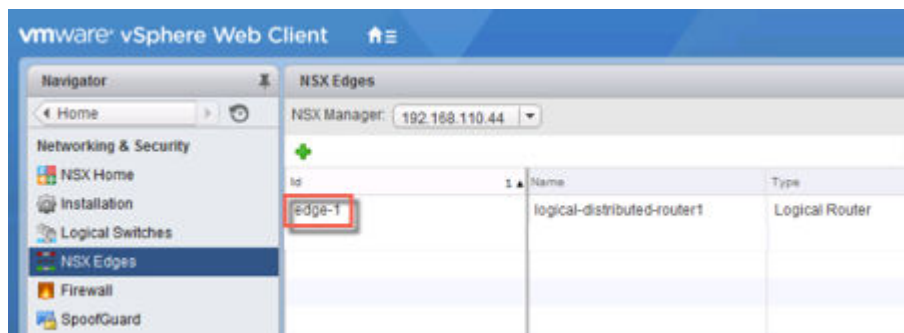
次のステップ

NSX Edge アプライアンスを最初にデプロイしたホストでは、NSX が仮想マシンの自動起動/シャットダウンを有効にします。その後、アプライアンス仮想マシンを別のホストに移行した場合、新しいホストで仮想マシンの自動起動/シャットダウンが有効にならない場合があります。そのため、クラスタ内のすべてのホストをチェックし、仮想マシンの自動起動/シャットダウンが有効になっていることを確認することをお勧めします。

http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html を参照してください。

論理ルーターを展開した後、論理ルーター ID をダブルクリックして、インターフェイス、ルーティング、ファイアウォール、ブリッジ、DHCP リレーなどを設定します。

次はその例です。



Edge Services Gateway の追加

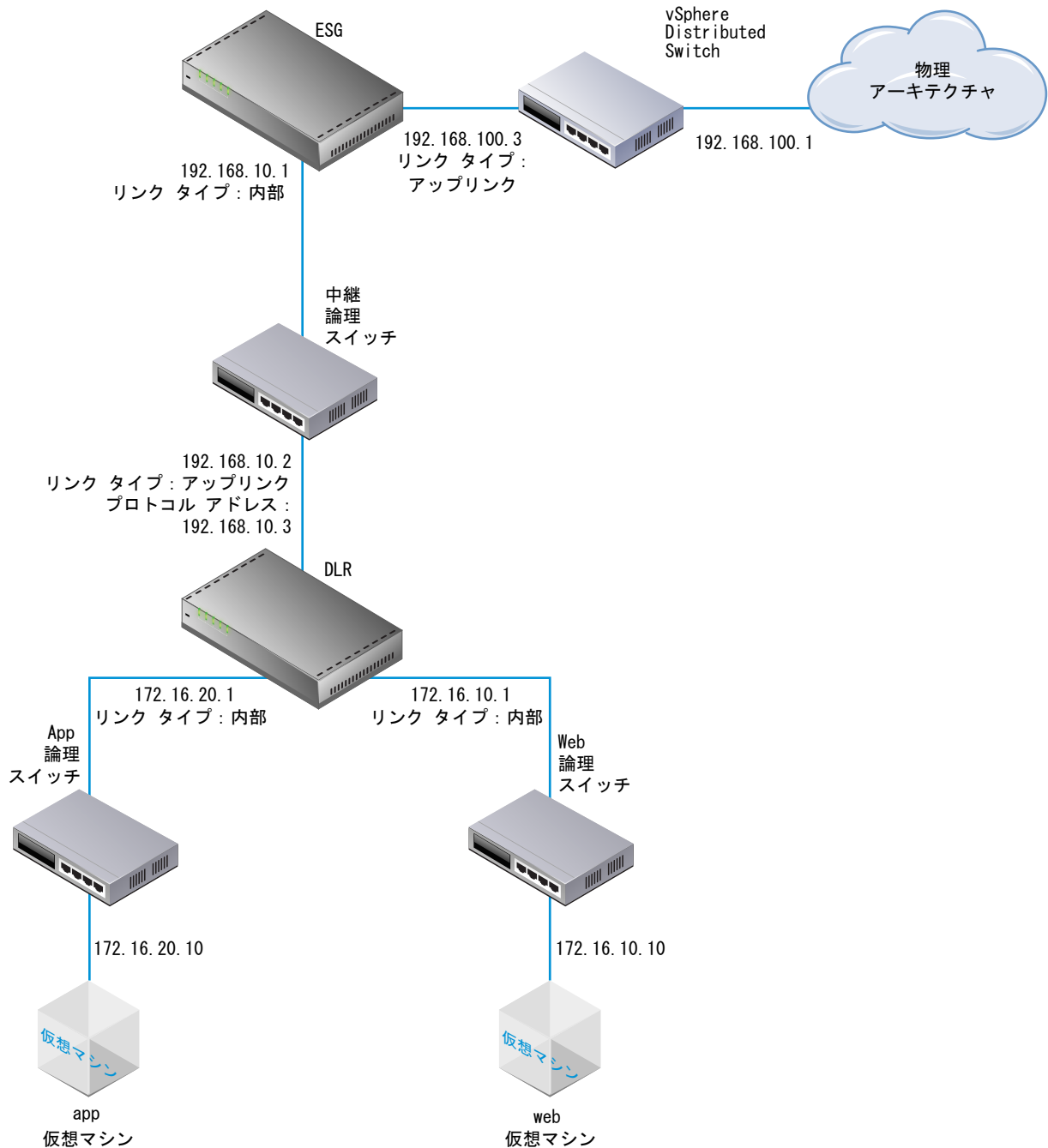
データセンターには、複数の NSX Edge Services Gateway 仮想アプライアンスをインストールできます。各 NSX Edge 仮想アプライアンスには、アップリンクと内部のネットワーク インターフェイスを合計で 10 個指定できます。内部インターフェイスは保護されたポート グループに接続され、そのポート グループ内の保護された仮想マシンすべてのゲートウェイとして機能します。内部インターフェイスに割り当てられたサブネットは、パブリックにルーティングされる IP アドレス空間にも、ネットワーク アドレス変換またはルーティングされる RFC 1918 専用空間にもなります。ファイアウォールルールと他の NSX Edge サービスは、インターフェイス間のトラフィックに適用されます。

ESG のアップリンク インターフェイスは、社内共有ネットワークや、アクセス レイヤー ネットワークを提供するサービスに対するアクセス権を持つアップリンク ポート グループに接続します。

次のリストに、ESG でのインターフェイス タイプ（内部およびアップリンク）ごとの機能のサポートを示します。

- DHCP：アップリンク インターフェイスではサポートされません。
- DNS フォワーダ：アップリンク インターフェイスではサポートされません。
- HA：アップリンク インターフェイスではサポートされていません。少なくとも 1 つの内部インターフェイスが必要です。
- SSL VPN：リスナー IP がアップリンク インターフェイスに属している必要があります。
- IPsec VPN：ローカル サイト IP アドレスがアップリンク インターフェイスに属している必要があります。
- L2 VPN：内部ネットワークのみを拡張できます。

次の図に示すサンプルのトポロジでは、ESG のアップリンク インターフェイスが vSphere Distributed Switch を介して物理インフラストラクチャに接続され、ESG の内部インターフェイスが NSX 論理中継スイッチを介して NSX 論理ルーターに接続されています。




ロード バランシング、サイト間 VPN、および NAT サービス用に複数の外部 IP アドレスを設定できます。

前提条件

Enterprise Administrator または NSX Administrator のロールが割り当てられている必要があります。

Edge Services Gateway (ESG) 仮想アプライアンスをデプロイするのに十分な容量がリソース プールにあることを確認してください。[章 1 「NSX のシステム要件」](#) を参照してください。

手順

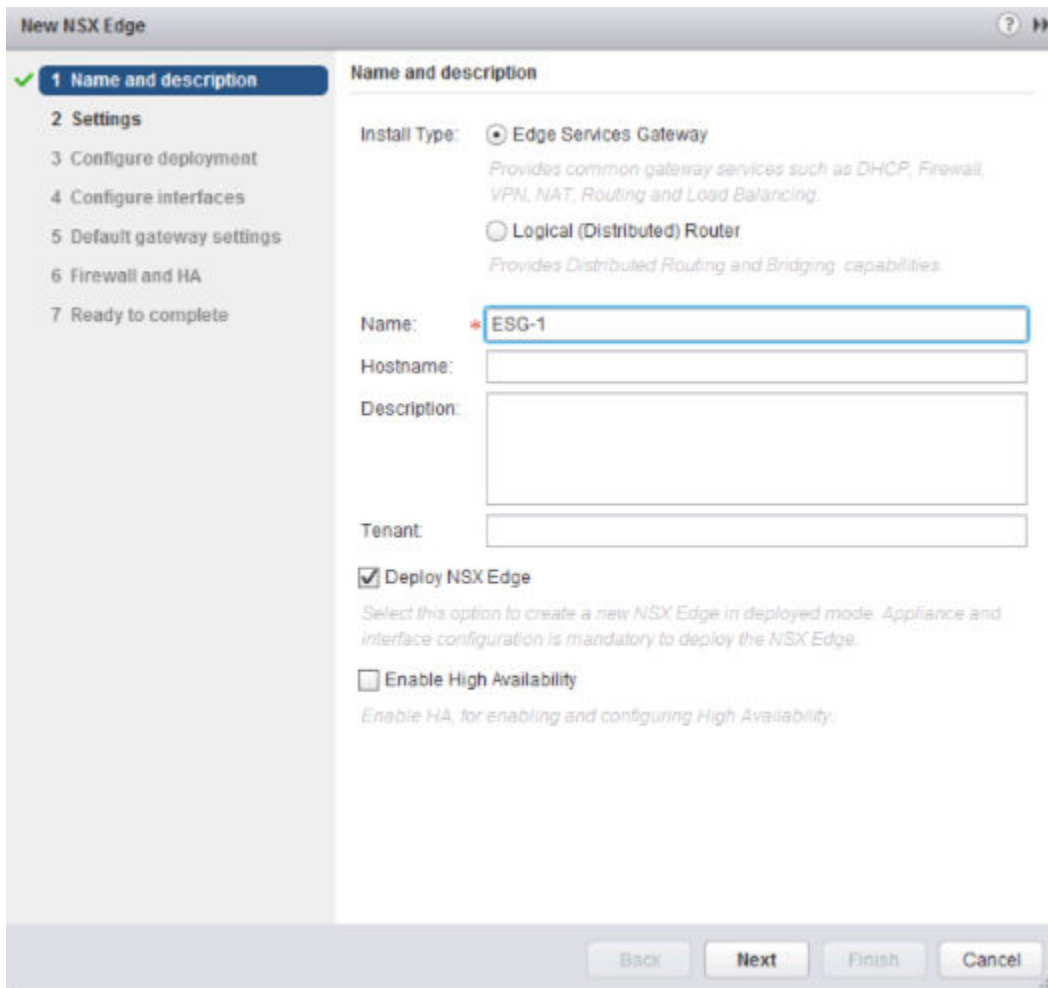
- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [NSX Edges] に移動し、[追加 (Add)] () アイコンをクリックします。
- 2 [Edge Services Gateway] を選択し、デバイスの名前を入力します。

この名前は vCenter インベントリに表示されます。1 つのテナントのすべての ESG の中で一意の名前を付けてください。

必要に応じて、ホスト名を入力することもできます。この名前は CLI に表示されます。ホスト名を指定しない場合は、自動的に作成される Edge ID が CLI に表示されます。

オプションで、説明とテナントを入力し、高可用性を有効にできます。

次はその例です。



New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Name and description

Install Type: ☒ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

Name:

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

Back Next Finish Cancel

- 3 ESG のパスワードを入力し、再入力します。

パスワードは 12 文字以上で、次の 4 つのルールのうち 3 つに従っている必要があります。

- 1 文字以上の大文字
- 1 文字以上の小文字

- 1 文字以上の数字
- 1 文字以上の特殊文字

4 (オプション) SSH、高可用性、および自動ルール生成を有効にして、ログ レベルを設定します。

自動ルール生成を有効にしない場合は、ファイアウォール、NAT、およびルーティングを手動で設定して、ロード バランシングや VPN などの特定の NSX Edge サービスの制御トラフィックを許可する必要があります。自動ルール生成では、データチャネル トラフィックのルールが作成されません。

デフォルトでは、SSH と高可用性が無効になり、自動ルール生成が有効になります。デフォルトでは、ログ レベルが「緊急」に設定されます。

すべての新しい NSX Edge アプライアンスでは、デフォルトでログが有効になっています。デフォルトのログ レベルは「注意」です。

次はその例です。

5 システム リソースに基づいて NSX Edge インスタンスのサイズを選択します。

[Large] NSX Edge は、[Compact] NSX Edge よりも CPU、メモリ、およびディスク容量が多く、より多くの同時 SSL VPN-Plus ユーザーをサポートします。[X-Large] NSX Edge は、百万単位の同時セッションを処理するロード バランサが実装されている環境に適しています。高いスループットが要求される場合は、Quad Large NSX Edge をお勧めします。この NSX Edge では高い接続速度が必要になります。

[章 1 「NSX のシステム要件」](#) を参照してください。

6 Edge Appliance を作成します。

vCenter インベントリに追加する ESG 仮想アプライアンスの設定を入力します。NSX Edge のインストール時にアプライアンスを追加しないと、NSX Edge はアプライアンスが追加されるまでオフライン モードのままになります。

HA を有効にした場合は、アプライアンスを 2 台追加できます。アプライアンスを 1 つ追加すると、NSX Edge はその設定をスタンバイ アプライアンス用にレプリケートします。これにより、DRS や vMotion を実行した後でも、2 台の HA NSX Edge 仮想マシンを手動でホストに移動 (vMotion) しない限り、これらの仮想マシンが同じ ESX ホストに存在することはありません。HA を正しく機能させるには、両方のアプライアンスを共有データストアにデプロイする必要があります。

次はその例です。

- 7 [NSX Edge のデプロイ (Deploy NSX Edge)] を選択し、デプロイ済みモードで Edge を追加します。Edge をデプロイするには、Edge のアプライアンスとインターフェイスを設定する必要があります。

- 8 インターフェイスを設定します。

ESG では、IPv4 および IPv6 アドレスの両方がサポートされます。

HA を有効にするには、内部インターフェイスを少なくとも 1 つ追加する必要があります。

1 つのインターフェイスには、重複しない複数のサブネットを設定できます。

インターフェイスに複数の IP アドレスを入力した場合は、プライマリ IP アドレスを選択できます。1 つのインターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。NSX Edge は、プライマリ IP アドレスをローカルに生成されるトラフィック (リモート Syslog やオペレータが開始した ping など) のソース アドレスと見なします。

何らかの機能に使用する前に、インターフェイスに IP アドレスを追加する必要があります。

オプションで、インターフェイスの MAC アドレスを入力できます。

HA が有効な場合は、オプションとして 2 つの管理 IP アドレスを CIDR 形式で入力できます。2 台の NSX Edge HA 仮想マシンのハートビートは、これらの管理 IP アドレスを介して通信されます。管理 IP アドレスは、同じ L2/サブネットに存在し、相互に通信可能になっている必要があります。

オプションで、MTU を変更することができます。

他のマシンに対する ARP 要求に ESG が応答できるようにする場合は、プロキシ ARP を有効にします。これは、WAN 接続の両側に同じサブネットがある場合などに便利です。

ICMP リダイレクトを有効にして、ルーティング情報が各ホストに伝達されるようにします。

転送するパケット内にあるソース アドレスの到達可能性を確認するには、リバース パス フィルタを有効にします。有効モードでは、ルーターが戻りパケットの転送に使用するインターフェイスで、パケットを受信する必要があります。Loose モードの場合、送信元アドレスがルーティングテーブルに含まれている必要があります。

複数のフェンスされた環境で IP アドレスと MAC アドレスを再使用する場合は、フェンス パラメータを設定します。たとえば、Cloud Management Platform (CMP) では、フェンスを設定することで、同じ IP アドレスと MAC アドレスを完全に分離して、つまり「フェンスして」、複数のクラウドインスタンスを同時に実行できるようになります。

次はその例です。

Edit NSX Edge Interface

vNIC#: 1

Name: * Internal

Type: ☒ Internal ☐ Uplink

Connected To: transit-switch [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

IP Address	Subnet Prefix Length
192.168.10.1*	29

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect Reverse Path Filter [Disable](#) ▼

Fence Parameters:

Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

次の例は 2 つのインターフェイスを示しています。1 つは vSphere Distributed Switch 上のアップリンク ポートグループを介して ESG を外部のネットワークに接続し、もう 1 つは分散論理ルーターが接続されている論理中継スイッチに ESG を接続します。

New NSX Edge

✓ 1 Name and description

✓ 2 Settings

✓ 3 Configure deployment

✓ 4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Configure interfaces

Configure interfaces of this NSX Edge

+

✗

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	uplink	192.168.100.3	24	Mgmt_VDS - HQ_Uplink
1	internal	192.168.10.1	29	transit-switch

Back

Next

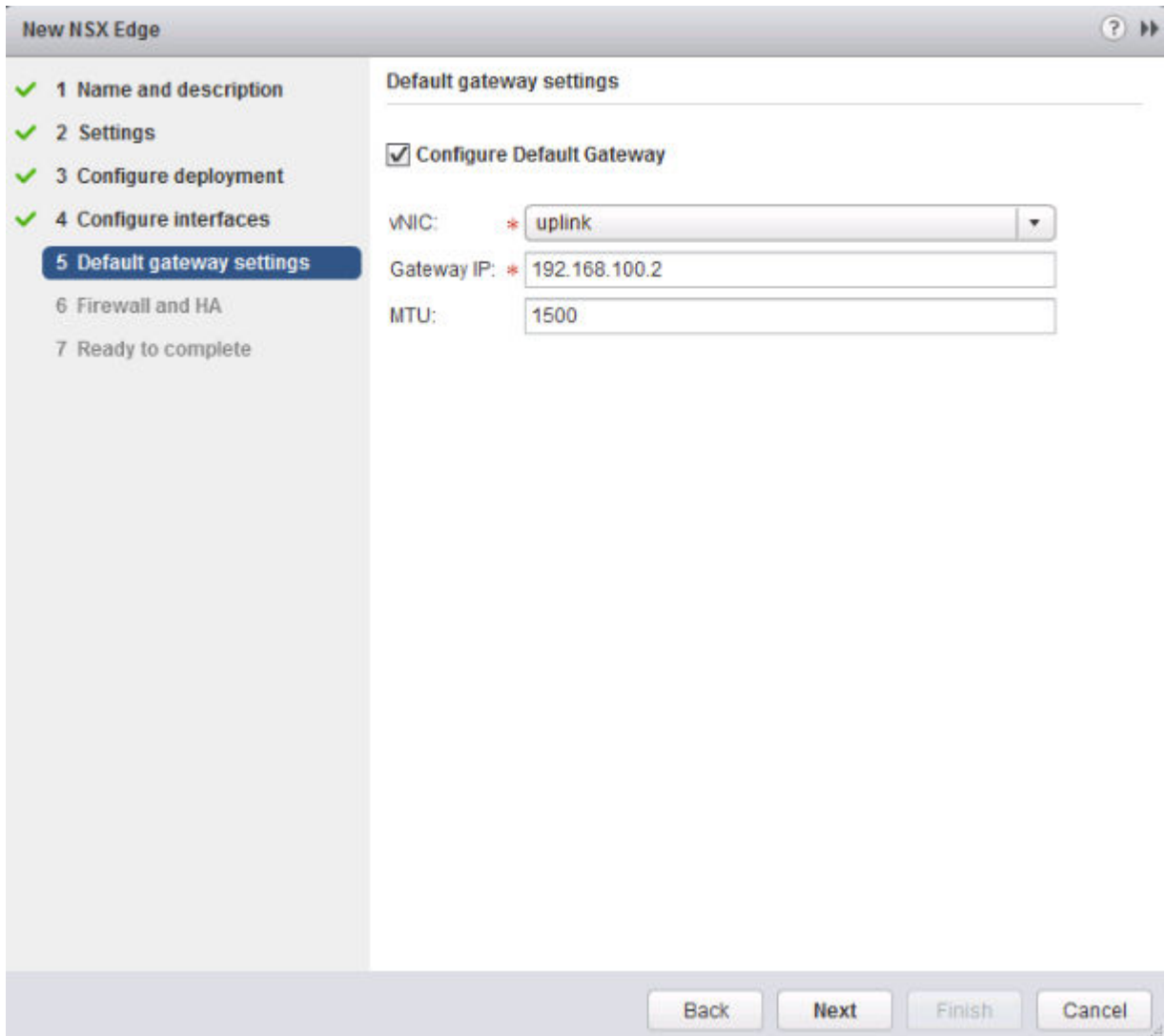
Finish

Cancel

9 デフォルト ゲートウェイを設定します。

MTU 値は編集可能ですが、インターフェイスに設定されている MTU より大きくすることはできません。

次はその例です。



10 ファイアウォール ポリシー、ログ、および HA パラメータを設定します。



警告: ファイアウォール ポリシーを設定しない場合、すべてのトラフィックを拒否するようにデフォルトのポリシーが設定されます。

すべての新しい NSX Edge アプライアンスでは、デフォルトでログが有効になっています。デフォルトのログレベルは「注意」です。ログを ESG 上でローカルに保存する場合にログを有効にすると、ログが大量に生成されて NSX Edge のパフォーマンスに影響する可能性があります。そのため、リモートの Syslog サーバを構成して、すべてのログを統合コレクタに転送し、分析と監視を行うことをお勧めします。

高可用性を有効にした場合は、HA セクションをすべて記入してください。デフォルトでは、HA で内部インターフェイスが自動的に選択され、リンクローカルな IP アドレスが自動的に割り当てられます。NSX Edge は高可用性で 2 台の仮想マシンをサポートし、どちらの仮想マシンのユーザー設定も最新の状態に維持されます。プライマリ仮想マシンでハートビート障害が発生すると、セカンダリ仮想マシンの状態がアクティブに変化します。このようにして、ネットワーク上では常に 1 台の NSX Edge 仮想マシンがアクティブの状態になります。NSX Edge はスタンバイ アプライアンス用にプライマリ アプライアンスの設定をレプリケートし、DRS や vMotion の使用後であっても、2 台の HA NSX Edge 仮想マシンが同じ ESX ホストに存在することのないようにします。2 台の仮想マシンは、構成したアプライアンスと同じリソース プールおよびデータストアにある vCenter Server にデプロイされます。NSX Edge HA の HA 仮想マシンにはローカル リンク IP アドレスが割り当てられるため、それらの仮想マシンは相互に通信できます。HA パラメータを設定する内部インターフェイスを選択します。内部インターフェイスが設定されていない状態でインターフェイスに「任意」を選択した場合、ユーザー インターフェイスではエラーが表示されません。2 台の Edge Appliance が作成されますが、内部インターフェイスが設定されていないため、新しい Edge はスタンバイのままとなり、HA は無効になります。内部インターフェイスを設定すると、Edge Appliance 上で HA が有効になります。バックアップ アプライアンスがプライマリ アプライアンスからハートビート信号を受信しない場合に、プライマリ アプライアンスを非アクティブと見なし、バックアップ アプライアンスで引き継ぐまでの最大期間を秒単位で入力します。デフォルトの間隔は 15 秒です。オプションとして、2 つの管理 IP アドレスを CIDR 形式で入力して、HA 仮想マシンに割り当てられたロー

カル リンク IP アドレスをオーバーライドすることができます。管理 IP アドレスが他のインターフェイスに使用されている IP アドレスと重複しておらず、トラフィックのルーティングを妨げていないことを確認します。ネットワーク上の他の場所に存在する IP アドレス を使用しないでください。これは、そのネットワークが NSX Edge に直接接続されていない場合でも同様です。

次はその例です。

New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 Configure interfaces
- ✓ 5 Default gateway settings
- 6 Firewall and HA**
- 7 Ready to complete

Firewall and HA

☒ **Configure Firewall default policy**

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: * internal

Declare Dead Time: 15 (seconds)

Management IPs:

You can specify pair of IPs (in CIDR format) with /30 subnet. Management IPs must not overlap with any vnic subnets.

Back Next Finish Cancel

ESG がデプロイされたら、[ホストおよびクラスタ] ビューに移動し、Edge 仮想アプライアンスのコンソールを開きます。このコンソールから、接続されたインターフェイスに ping を送信できることを確認します。

次のステップ

NSX Edge アプライアンスを最初にデプロイしたホストでは、NSX が仮想マシンの自動起動/シャットダウンを有効にします。その後、アプライアンス仮想マシンを別のホストに移行した場合、新しいホストで仮想マシンの自動起動/シャットダウンが有効にならない場合があります。そのため、クラスタ内のすべてのホストをチェックし、仮想マシンの自動起動/シャットダウンが有効になっていることを確認することをお勧めします。

http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html を参照してください。

これで、外部デバイスから仮想マシンへの接続を可能にするルーティングを設定できます。

グローバル設定の指定

スタティック ルートに対してデフォルト ゲートウェイを設定でき、Edge Services Gateway または Distributed Router に対して動的なルーティングの詳細を指定できます。

ルーティングを設定するためには、使用できる NSX Edge インスタンスが必要です。NSX Edge のセット アップの詳細については、「[NSX Edge 設定](#)」を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [ルーティング (Routing)] をクリックして、[グローバル設定 (Global Configuration)] をクリックします。
- 5 ECMP (Equal-cost multi-path) ルーティング設定を変更するには、[ルーティング (Routing Configuration)] の横にある [編集 (Edit)] をクリックし、次の操作を実行します。

オプション	説明
Edge Services Gateway の場合	ECMP を編集するには、ECMP の横にある [有効化 (Enable)] または [無効化 (Disable)] をクリックします。
分散論理ルーターの場合	a 有効にする ECMP を選択するか、無効にする ECMP を選択解除します。 b [OK] をクリックします。

ECMP は、単一のターゲットに送られるネクスト ホップ パケットが、複数の最適パス上で行われるようにするためのルーティング戦略です。最適パスは、静的に追加でき、OSPF や BGP などの動的なルーティング プロトコルによるメトリック計算の結果として追加されるようにすることもできます。スタティック ルートに対して複数のパスを追加するには、[スタティック ルート] ダイアログボックスで複数のネクスト ホップをコンマで区切って指定します。詳細については、「[スタティック ルートの追加](#)」を参照してください。

Edge Services Gateway は、Linux ネットワーク スタック実装である、ランダム性コンポーネントを使用するラウンドロビンアルゴリズムを使用します。特定の送信元と宛先の IP アドレス ペアに対してネクスト ホップが選択されると、選択したネクスト ホップをルート キャッシュが格納します。そのフローに対するすべてのパケットは、選択したネクスト ホップに送られます。デフォルト IPv4 ルート キャッシュは、300 秒 (gc_timeout) でタイムアウトします。この間、アクティブでないエントリがあると、ルート キャッシュから削除される対象になります。実際の削除は、ガベージ コレクション タイマーがアクティブになるときに (gc_interval = 60 秒) 行われます。

分散論理ルーターでは、可能な ECMP ネクスト ホップのリストからネクスト ホップを特定するために、XOR アルゴリズムが使用されます。このアルゴリズムでは、送信元および宛先 IP アドレスが、エントロピのソースとして送信パケット上で使用されます。

バージョン 6.1.2 までは、ECMP を有効にすることで、Edge Services Gateway 仮想マシン上の分散ファイアウォールは無効になりました。NAT などのステートフル サービスは、ECMP とは連動しませんでした。NSX for vSphere バージョン 6.1.3 以降、ECMP と分散ファイアウォールとを連動させることができます。

- 6 [ロケール ID (Locale ID)] を分散論理ルーター上で変更するには、[ルーティング (Routing Configuration)] の横にある [編集 (Edit)] をクリックします。ロケール ID を入力し、[OK] をクリックします。

デフォルトでは、ロケール ID は NSX Manager UUID に設定されていますが、ユニバーサル分散論理ルーター作成時に Local Egress (ローカル出力方向) が有効にされている場合、この設定をオーバーライドできます。ロケール ID は、Cross-vCenter NSX または複数サイト環境でルートを選択的に設定するために使用します。詳細については「[Cross-vCenter NSX トポロジ](#)」を参照してください。

ロケール ID は UUID 形式である必要があります。例：XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX。ここで、各 X は 16 進数字 (0 ~ F) で置き換えられます。

- 7 デフォルトゲートウェイを指定するには、[デフォルトゲートウェイ (Edit)] の横にある [編集 (Default Gateway)] をクリックします。
 - a ターゲット ネットワークに向かってネクスト ホップに到達するために経由することができるインターフェイスを選択します。
 - b ゲートウェイ IP アドレスを入力します。
 - c (オプション) ロケール ID を入力します。ロケール ID は、ユニバーサル分散論理ルーター上のみで使用できるオプションです。
 - d (オプション) MTU を編集します。

- e 要求された場合は、[管理ディスタンス (Admin Distance)] を入力します。

1 ~ 255 の値を選択します。特定のネットワークに対して複数のルートがある場合、管理ディスタンスを使用してどのルートを使用するかを選択します。管理ディスタンスが低いほど、ルートの優先順位は高くなります。

表 9-1. デフォルトの管理ディスタンス

ルート ソース	デフォルトの管理ディスタンス
接続済み	0
スタティック	1
外部 BGP	20
OSPF エリア内	30
OSPF エリア間	110
内部 BGP	200

- f (オプション) デフォルト ゲートウェイの説明を入力します。

- g [保存 (Save)] をクリックします。

- 8 動的なルーティングを設定するには、[動的ルーティング (Edit)] の横にある [編集 (Dynamic Routing Configuration)] をクリックします。

- a [ルーター ID (Router ID)] に、動的なルーティングのためにカーネルにルートをプッシュする NSX Edge の最初のアップリンク IP アドレスが表示されます。
- b ここではプロトコルを有効にしないでください。
- c [ログの有効化 (Enable Logging)] を選択してログ情報を保存し、ログ レベルを選択します。

注: 使用する環境内に IPsec VPN が設定されている場合、動的なルーティングは使用しないでください。

- 9 [変更の発行 (Publish Changes)] をクリックします。

次のステップ

ルーティング設定を削除するには、[リセット (Reset)] をクリックします。これにより、すべてのルーティング（デフォルト、固定、OSPF、および BGP の各と、ルート再配分）が削除されます。

NSX Edge 設定

実際に使用できる（つまり、1 つ以上のアプライアンスおよびインターフェイスが追加されていて、デフォルト ゲートウェイ、ファイアウォール ポリシー、高可用性が設定されている）NSX Edge をインストールしたら、NSX Edge サービスの使用を開始できます。

証明書の操作

NSX Edge では、自己署名証明書、認証局 (CA) によって署名された証明書、および CA によって生成および署名された証明書がサポートされます。

CA 署名証明書の設定

証明書署名要求 (CSR) を生成し、CA による署名を取得することができます。グローバル レベルで証明書署名要求を生成すると、お使いのインベントリ内のすべての NSX Edge でそれを利用できます。

手順

- 1 次のいずれかを実行します。

オプション	説明
グローバル証明書を生成する	<ol style="list-style-type: none"> a NSX Manager 仮想アプライアンスにログインします。 b [管理] タブをクリックし、[SSL 証明書] をクリックします。 c [CSR の生成 (Generate CSR)] をクリックします。
NSX Edge 用の証明書を生成する	<ol style="list-style-type: none"> a vSphere Web Client にログインします。 b [Networking and Security (Networking & Security)] をクリックして、[Edge サービス (Edge Services)] をクリックします。 c NSX Edge をダブルクリックします。 d [管理 (Manage)] タブをクリックして、[設定 (Settings)] をクリックします。 e [証明書 (Certificates)] リンクをクリックします。 f [アクション (Actions)] をクリックし、[CSR の生成 (Generate CSR)] を選択します。

- 2 組織のユニットおよび名前を入力します。
- 3 組織の国、都道府県、市町村名などを入力します。
- 4 ホスト間の通信のための暗号化アルゴリズムを選択します。
SSL VPN-Plus がサポートしているのは、RSA 証明書のみです。

- 5 必要に応じてデフォルトの鍵のサイズを編集します。
- 6 グローバル証明書の場合、証明書の説明を入力します。
- 7 [OK] をクリックします。

証明書署名要求が生成され、証明書のリストに表示されます。

- 8 オンライン証明書機関にこの証明書署名要求に署名してもらいます。
- 9 署名付き証明書をインポートします。
 - a 署名付き証明書の内容をコピーします。
 - b 次のいずれかを実行します。
 - 署名付き証明書をグローバル レベルでインポートするには、NSX Manager 仮想アプライアンスで [インポート (Import)] をクリックします。
 - NSX Edge の署名付き証明書をインポートするには、[アクション (Actions)] をクリックし、[証明書 (Certificates)] タブで [証明書のインポート (Import Certificate)] を選択します。


- c [Import CSR] ダイアログ ボックスで、署名付き証明書の内容を貼り付けます。
- d [OK] をクリックします。

CA 署名証明書が証明書リストに表示されます。

CA 証明書の追加

CA 証明書を追加することにより、会社の暫定 CA となることができます。これにより、独自の証明書に署名する権限が得られます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブが開いていることを確認します。
- 5 [証明書 (Certificates)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックし、[CA 証明書 (CA Certificate.)] を選択します。
- 7 [証明書の内容] テキスト ボックスに証明書の内容をコピー アンド ペーストします。
- 8 CA 証明書の説明を入力します。
- 9 [OK] をクリックします。

これで、独自の証明書に署名できるようになります。

自己署名証明書の設定

自己署名したサーバ証明書の作成、インストールおよび管理が可能です。

前提条件

独自の証明書に署名できるように、CA 証明書を持っていることを確認してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブが開いていることを確認します。
- 5 [証明書 (Certificates)] をクリックします。

6 以下の手順に従い、証明書署名要求 (CSR) を生成します。

- a [アクション (Actions)] をクリックし、[CSR の生成 (Generate CSR)] を選択します。
- b [共通名] に NSX Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
- c 組織名およびユニットを入力してください。
- d 組織の国、都道府県、市町村名などを入力します。
- e ホスト間の通信のための暗号化アルゴリズムを選択します。

SSL VPN-Plus がサポートしているのは、RSA 証明書のみです。下位互換性を確保するため、RSA を選択することをお勧めします。

- f 必要に応じてデフォルトの鍵のサイズを編集します。
- g 証明書の説明を入力します。
- h [OK] をクリックします。

証明書署名要求が生成され、証明書のリストに表示されます。

7 生成した証明書が選択されていることを確認します。

8 [アクション (Actions)] をクリックし、[自己署名付き証明書 (Self Sign Certificate)] を選択します。

9 自己署名証明書の有効日数を入力します。

10 [OK] をクリックします。

クライアント証明書の使用

CAI コマンドまたは REST 呼び出しを通じてクライアント証明書を作成できます。その後、この証明書をリモートユーザーに配布し、リモートユーザーが証明書を各自の Web ブラウザにインストールできます。

クライアント証明書の導入の主なメリットは、各リモートユーザーに関する参照クライアント証明書を保存し、リモートユーザーが提示するクライアント証明書に照らして確認できるという点にあります。特定のユーザーからの今後の接続を防ぐために、クライアント証明書のセキュリティ サーバのリストから参照証明書を削除することができます。証明書を削除すると、そのユーザーからの接続が拒否されます。

証明書失効リストの追加


証明書失効リスト (CRL) は、Microsoft によって提供され署名されたサブスクリバとそのステータスのリストです。

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
- 証明書の発行日
- 証明書を発行した機関
- 次のリリースの提案日

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の許可または拒否を行います。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブが開いていることを確認します。
- 5 [証明書 (Certificates)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックして、[CRL] を選択します。
- 7 [証明書の内容 (Certificate contents)] にリストを貼り付けます。
- 8 (オプション) 説明を入力します。
- 9 [OK] をクリックします。

アプライアンスの管理

アプライアンスは、追加、編集、または削除できます。NSX Edge インスタンスは、少なくとも 1 台のアプライアンスが追加されるまで、オフラインのままになります。

アプライアンスの追加

NSX Edge をデプロイする前に、少なくとも 1 台のアプライアンスを追加する必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 [Edge Gateway Appliance (Edge Gateway Appliances)] で、[追加 (Add)] () アイコンをクリックします。
- 6 そのアプライアンスのクラスまたはリソース プール、およびデータストアを選択します。
- 7 (オプション) アプライアンスを追加するホストを選択します。
- 8 (オプション) アプライアンスを追加する vCenter Server フォルダを選択します。
- 9 [追加 (Add)] をクリックします。

アプライアンスの編集

NSX Edge アプライアンスを編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 [Edge Gateway Appliance (Edge Gateway Appliances)] で、変更するアプライアンスを選択します。
- 6 [編集 (Edit)] (✎) アイコンをクリックします。
- 7 [Edge アプライアンスの編集] ダイアログ ボックスで、必要な変更を行います。
- 8 [保存 (Save)] をクリックします。

アプライアンスの削除

NSX Edge アプライアンスを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 [Edge Gateway Appliance (Edge Gateway Appliances)] で、削除するアプライアンスを選択します。
- 6 [削除 (Delete)] (✖) アイコンをクリックします。

インターフェイスの操作

NSX Edge サービス ゲートウェイには、最大 10 個の内部インターフェイス、アップリンク インターフェイス、またはトランク インターフェイスを指定できます。NSX Edge ルーターには、8 個のアップリンク インターフェイスと、最大 1,000 個の内部インターフェイスを指定できます。

NSX Edge をデプロイできるようにするには、内部インターフェイスが少なくとも 1 つ必要です。

インターフェイスの設定

一般に、内部インターフェイスは水平方向トラフィック用であり、アップリンク インターフェイスは垂直方向トラフィック用です。分散論理ルーター (DLR) を Edge Services Gateway (ESG) に接続する場合、ルーターのインターフェイスがアップリンク インターフェイスになり、ESG のインターフェイスが内部インターフェイスになります。NSX トランク インターフェイスは内部ネットワーク用であり、外部ネットワーク用ではありません。トランク インターフェイスを使用すると、複数の内部ネットワーク (VLAN または VXLAN のどちらか) のトランッキングができます。

NSX Edge Services Gateway (ESG) は、内部インターフェイス、アップリンク インターフェイス、またはトランク インターフェイスを最大 10 個持つことができます。この制限は NSX Manager によって適用されます。

NSX デプロイでは、1 つの ESXi ホスト上に最大 1,000 個の分散論理ルーター (DLR) インスタンスを持つことができます。1 つの分散論理ルーターには、最大 8 個のアップリンク インターフェイスと最大 991 個の内部インターフェイスを設定できます。この制限は NSX Manager によって適用されます。NSX デプロイにおけるインターフェイスの拡張については、『VMware® NSX for vSphere Network Virtualization Design Guide』(<https://communities.vmware.com/docs/DOC-27683>) を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[インターフェイス (Interfaces)] タブをクリックします。
- 5 インターフェイスを選択して、[編集 (Edit)] (✎) アイコンをクリックします。
- 6 [Edge インターフェイスの編集] ダイアログ ボックスで、インターフェイスの名前を入力します。
- 7 [内部 (Internal)] または [アップリンク (Uplink)] を選択して、内部と外部のどちらのインターフェイスなのかを指定します。

サブ インターフェイスを作成する場合は、[トランク (Trunk)] を選択します。詳細については、[「サブ インターフェイスの追加」](#) を参照してください。

- 8 このインターフェイスを接続するポート グループまたは論理スイッチを選択します。
 - a [接続先 (Connected To)] フィールドの横の [選択 (Select)] をクリックします。
 - b インターフェイスに接続する内容に応じて、[論理スイッチ (Logical Switch)]、[標準ポートグループ (Standard Portgroup)]、または [分散ポートグループ (Distributed Portgroup)] のタブをクリックします。
 - c 適切な論理スイッチまたはポートグループを選択します。
 - d [選択 (Select)] をクリックします。
- 9 インターフェイスの接続ステータスを選択します。
- 10 [サブネットの (Configure Subnets)] で、[追加 (Add)] (+) アイコンをクリックし、インターフェイスのサブ ネットを追加します。

1 つのインターフェイスには、重複しない複数のサブ ネットを設定できます。

- 11 [サブネットの追加 (Add Subnet)] で、[追加 (Add)] (+) アイコンをクリックし、IP アドレスを追加します。

複数の IP アドレスを入力した場合は、プライマリ IP アドレスを選択できます。1 つのインターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。NSX Edge は、プライマリ IP アドレスをローカルで生成されたトラフィックの送信元のアドレスとして認識します。

何らかの機能に使用する前に、インターフェイスに IP アドレスを追加する必要があります。

- 12 インターフェイスのサブネット マスクを入力し、[保存 (Save)] をクリックします。
- 13 必要に応じてデフォルトの MTU を変更します。
- 14 [オプション (Options)] で、必要なオプションを選択します。

オプション	説明
プロキシ ARP の有効化	異なるインターフェイス間での重複ネットワーク転送をサポートします。
ICMP リダイレクトの送信	ルーティング情報を各ホストに伝達します。
リバース パス フィルタ	転送するパケット内にある送信元のアドレスの到達可能性を確認します。有効な場合は、ルーターが戻りパケットの転送に使用するインターフェイスで、パケットを受信する必要があります。Loose モードの場合、送信元アドレスがルーティングテーブルに含まれている必要があります。

- 15 フェンス パラメータを入力し、[追加 (Add)] をクリックします。
- 16 [OK] をクリックします。

インターフェイスの削除

NSX Edge インターフェイスを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[インターフェイス (Interfaces)] タブをクリックします。
- 5 削除するインターフェイスを選択します。
- 6 [削除 (Delete)] (✖) アイコンをクリックします。

インターフェイスを有効にする

インターフェイス（ポート グループまたは論理スイッチ）内の仮想マシンを隔離するために、NSX Edge に対してそのインターフェイスを有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[インターフェイス (Interfaces)] タブをクリックします。
- 5 有効にするインターフェイスを選択します。

- 6 [有効化 (Enable)] (✓) アイコンをクリックします。

インターフェイスを無効にする

NSX Edge でインターフェイスを無効にすることが可能です。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[インターフェイス (Interfaces)] タブをクリックします。
- 5 無効にするインターフェイスを選択します。
- 6 [無効化 (Disable)] アイコンをクリックします。

トラフィックシェーピングポリシーの変更

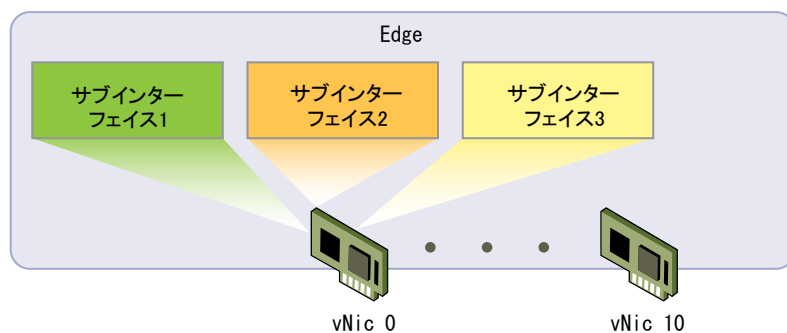
vSphere Distributed Switch で NSX Edge インターフェイスのトラフィックシェーピングポリシーを変更できます。

手順

- 1 NSX Edge をダブルクリックして、[管理 (Manage)] - [設定 (Settings)] - [インターフェイス (Interfaces)] の順に移動します。
- 2 インターフェイスを選択します。
- 3 [アクション (Actions)] - [トラフィックシェーピングポリシーの設定 (Configure Traffic Shaping Policy)] をクリックします。
- 4 適切な変更を加えます。
オプションの詳細については、[トラフィックシェーピングポリシー](#)を参照してください。
- 5 [OK] をクリックします。

サブインターフェイスの追加

トランク vNIC にサブインターフェイスを追加して、NSX Edge サービスで使用できます。



トランク インターフェイスには、次のようなタイプがあります。

- VLAN トランクは、標準的なタイプで、どのバージョンの ESXi でも機能します。これは、タグ付き VLAN トラフィックを Edge に送信するために使用されます。
- VXLAN トランクは、NSX バージョン 6.1 でのみ機能します。これは、VXLAN トラフィックを Edge に送信するために使用されます。

サブインターフェイスは、次の Edge サービスで使用できます。

- DHCP
- ルーティング (BGP のみ)
- ロード バランサ
- IPSEC VPN
- L2 VPN

サブインターフェイスは、高可用性 (HA) または論理ファイアウォールでは使用できません。ただし、ファイアウォール ルールでサブインターフェイスの IP アドレスを使用することはできます。

手順

- 1 NSX Edge の [管理] - [設定] タブで、[インターフェイス] をクリックします。
- 2 インターフェイスを選択して、[編集] (✎) アイコンをクリックします。
- 3 [Edge インターフェイスの編集] ダイアログ ボックスで、インターフェイスの名前を入力します。
- 4 [タイプ] で、[トランク] を選択します。
- 5 このインターフェイスを接続する標準ポートグループまたは分散ポートグループを選択します。
 - a [接続先] フィールドの横の [変更] をクリックします。
 - b インターフェイスに接続する対象に応じて、[標準ポートグループ] または [分散ポートグループ] タブをクリックします。
 - c 適切なポートグループを選択し、[OK] をクリックします。
 - d [選択] をクリックします。
- 6 [サブインターフェイス] で、[追加] アイコンをクリックします。
- 7 [サブインターフェイスの有効化] をクリックし、サブインターフェイスの名前を入力します。
- 8 [トンネル ID] に、1 ~ 4094 の数字を入力します。

トンネル ID は、拡張するネットワークに接続するために使用されます。この値はクライアント サイトとサーバ サイトの両方で同じにする必要があります。

- 9 [バックリング タイプ] で、次のいずれかを選択して、サブ インターフェイスのネットワーク バックリングを指定します。

- VLAN ネットワークの [VLAN]。

サブ インターフェイスで使用する仮想 LAN の VLAN ID を入力します。VLAN ID の範囲は 0 ～ 4094 です。

- VLAN または VXLAN ネットワークの [ネットワーク]。

[選択] をクリックし、分散ポートグループまたは論理スイッチを選択します。NSX Manager は、VLAN ID を抽出し、トランク設定で使用します。

- ネットワークまたは VLAN ID を指定せずにサブ インターフェイスを作成する場合には [なし]。このサブ インターフェイスは、NSX Edge の内部にあり、拡張ネットワークと非拡張（タグなし）ネットワーク間でパケットをルーティングするために使用されます。

- 10 サブネットをサブ インターフェイスに追加するには、[サブネットの] 領域の [追加] アイコンをクリックします。

- 11 [サブネットの追加] で [追加] アイコンをクリックして、IP アドレスを追加します。IP アドレスを入力し、[OK] をクリックします。

複数の IP アドレスを入力した場合は、プライマリ IP アドレスを選択できます。1 つのインターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。NSX Edge は、プライマリ IP アドレスをローカルで生成されたトラフィックのソース アドレスとして認識します。

- 12 サブネット プリフィックスの長さを入力して、[OK] をクリックします。

- 13 必要に応じてサブ インターフェイスのデフォルトの [MTU] 値を編集します。

トランク インターフェイスのデフォルトの MTU は 1600 で、サブ インターフェイスのデフォルトの MTU は 1500 です。サブ インターフェイスの MTU は、NSX Edge のすべてのトランク インターフェイスの中で最も小さい MTU 値以下にする必要があります。

- 14 [リダイレクトの送信の有効化] を選択し、ルーティング情報をホストに伝達します。

- 15 インターフェイスの MAC アドレスを入力します。

サブ インターフェイスでは高可用性がサポートされていないため、1 つの MAC アドレスのみが必要です。

- 16 必要に応じてトランク インターフェイスのデフォルトの MTU を編集します。

- 17 [OK] をクリックします。

これで、Edge サービスでサブインターフェイスを使用できます。

次のステップ

標準ポートグループでバックリングされているトランク vNIC にサブ インターフェイスが追加される場合、VLAN トランクを設定します。[\[VLAN トランクの設定\]](#) を参照してください。

VLAN トランクの設定

分散ポートグループでバックリングされているトランク vNIC にサブ インターフェイスが追加される場合、トランク ポートに VLAN または VXLAN トランクが自動的に設定されます。標準ポートグループでバックリングされているトランク vNIC にサブ インターフェイスが追加される場合、VLAN トランクのみがサポートされます。

前提条件

標準ポートグループでバックアップされているトランク vNIC のサブ インターフェイスが使用できることを確認します。[「サブ インターフェイスの追加」](#) を参照してください。


手順

- 1 vSphere Web Client にログインします。
- 2 [ネットワーク (Networking)] をクリックします。
- 3 標準ポートグループを選択して、[設定の編集 (Edit Settings)] をクリックします。
- 4 [VLAN] タブをクリックします。
- 5 [VLAN タイプ] で、[VLAN トランク] を選択し、トランッキングする VLAN ID を入力します。
- 6 [OK] をクリックします。

自動ルール設定の変更

自動ルール生成が有効になっている場合、NSX Edge は、ファイアウォール、NAT、およびルーティングのルートを追加して、これらのサービスで送信される制御トラフィックを有効にします。自動ルール生成が有効になっていない場合、ファイアウォール、NAT、およびルーティングの設定を手動で追加して、ロード バランシングや VPN などの NSX Edge サービスの制御チャネル トラフィックを許可する必要があります。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 [その他のアクション (More Actions)] () アイコンをクリックし、[自動ルール設定の変更 (Change Auto Rule configuration)] を選択します。
- 6 必要な変更を行い、[OK] をクリックします。

CLI 資格情報の変更

コマンドライン インターフェイス (CLI) へのログインで使用する認証情報を編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[設定 (Settings)] タブをクリックします。

- 5 [その他のアクション (More Actions)] () アイコンをクリックし、[CLI 資格情報の変更 (Change CLI Credentials)] を選択します。
- 6 適切に編集します。
- 7 [OK] をクリックします。

高可用性について

高可用性 (HA) は、ハードウェアまたはソフトウェアに障害が発生して 1 台のアプライアンスが利用できなくなった場合でも、NSX Edge アプライアンスが提供するサービスを利用できることを保証します。NSX Edge の HA は、ダウンタイムが発生しないようにするのではなく、フェイルオーバーによるダウンタイムを最小限に抑えます。アプライアンス間でフェイルオーバーを行う場合、一部のサービスの再起動が必要になる場合があります。

たとえば、NSX Edge HA は、ステートフルなファイアウォールが保持する接続に関する情報、またはロード バランサが保持するステートフルな情報を同期します。すべてのサービスをバックアップにフェイルオーバーするには、多少の時間がかかります。サービスの再起動による影響の例の 1 つは、NSX Edge がルーターとして動作している場合に、動的なルーティングで生じるダウンタイムです。

2 台の NSX Edge HA アプライアンスが通信できなくなった場合、どちらかをアクティブにすることを決定します。この動作は、スタンバイの NSX Edge が利用できない場合に、アクティブの NSX Edge サービスを利用し続けられるようにするためのものです。他方のアプライアンスが存在し続けていて、通信が再度確立された場合は、2 台の NSX Edge 間でアクティブとスタンバイの状態をネゴシエートします。ネゴシエートが終了せず、両方のアプライアンスがアクティブであると宣言した場合、予期しない動作が発生します。この状態は、スプリット ブレインとして知られています。これは、次のような状態の環境で発生します。

- ネットワークのパーティショニングなど、物理ネットワークの接続に問題がある
- NSX Edge で CPU またはメモリの競合が発生している
- ストレージに関する一時的な問題によって、1 台以上の NSX Edge HA 仮想マシンが利用できなくなっている

たとえば、オーバプロビジョニング状態のストレージから仮想マシンを移動させると、NSX Edge HA の安定性とパフォーマンスが改善することが知られています。特に、夜間の大規模なバックアップ中にストレージの遅延が急激に増大すると、NSX Edge HA の安定性に影響が生じます。
- 物理または仮想ネットワーク アダプタで、パケットの交換に関する輻輳が発生している

環境の問題に加えて、HA の構成エンジンが不良状態になったり、HA デーモンが失敗したりした場合にも、スプリット ブレイン状態になることがあります。

ステートフルな高可用性

プライマリ NSX Edge アプライアンスがアクティブ状態であり、セカンダリ アプライアンスがスタンバイ状態です。NSX Edge は、プライマリ アプライアンスの構成をスタンバイ アプライアンスにレプリケートします。または、手動で 2 台のアプライアンスを追加することもできます。VMware は、プライマリ アプライアンスとセカンダリ アプライアンスを別々のリソース プールおよびデータストアに作成することをお勧めしています。プライマリ アプライアンスとセカンダリ アプライアンスを同じデータストアに作成する場合は、HA 構成の対となる 2 台のアプライアンスを異なる ESX ホストにデプロイするため、クラスタ内のすべてのホストがデータストアを共有しなければなりません。データストアがローカル ストレージの場合は、両方の仮想マシンが同じホスト上に展開されます。

すべての NSX Edge サービスは、アクティブなアプライアンス上で動作します。プライマリ アプライアンスは、スタンバイ アプライアンスとともにハートビートを維持し、内部インターフェイスを通じてサービスのアップデートを送信します。

一定時間内（デフォルトは 15 秒）にプライマリ アプライアンスからハートビートが受信されない場合、プライマリ アプライアンスは応答不能と判断されます。スタンバイ アプライアンスがアクティブ状態となり、プライマリ アプライアンスのインターフェイス設定を引き継いで、プライマリ アプライアンスで実行されていた NSX Edge サービスを起動します。切り替えの実行時には、設定およびレポートの [システム イベント (System Events)] タブにシステム イベントが表示されます。ロード バランサおよび VPN サービスでは、NSX Edge との TCP 接続を再確立する必要があるため、サービスが短時間中断されます。論理スイッチ接続およびファイアウォール セッションは、プライマリ アプライアンスとセカンダリ アプライアンス間で同期されているため、切り替え時のサービスの中断はありません。

NSX Edge アプライアンスに障害が発生し、不良状態がレポートされると、HA は失敗したアプライアンスを復活させるために強制的な同期を行います。アプライアンスが復活すると、その時点でアクティブ状態のアプライアンスの設定を引き継ぎ、スタンバイ状態に戻ります。NSX Edge アプライアンスが応答不能の場合、アプライアンスを削除し、新しいアプライアンスを追加する必要があります。

NSX Edge は、DRS および vMotion を使用した後であっても、2 つの HA NSX Edge 仮想マシンが同じ ESX ホスト上に存在することのないようにします（vMotion を使用して手動で同じホストにした場合を除く）。2 台の仮想マシンは、構成したアプライアンスと同じリソース プールおよびデータストアにある vCenter Server にデプロイされます。NSX Edge HA の HA 仮想マシンにはローカル リンク IP アドレスが割り当てられるため、それらの仮想マシン同士は通信できます。管理 IP アドレスを指定してローカル リンクをオーバーライドすることができます。

Syslog サーバが構成されている場合は、アクティブなアプライアンスのログが Syslog サーバに送信されます。

vSphere High Availability

NSX Edge HA は、vSphere High Availability (HA) と互換性があります。NSX Edge インスタンスが動作しているホストの応答がない場合、NSX Edge がスタンバイ ホスト上で再起動され、それにより NSX Edge HA 構成の 2 台の仮想マシンが別のフェイルオーバーに対応できるようになります。

vSphere HA を利用しない場合でも、NSX Edge のアクティブ/スタンバイ構成の仮想マシンは、1 回のフェイルオーバーでは高可用性が問題なく機能します。ただし、障害が発生した仮想マシンがリストアされる前に別のフェイルオーバーが発生した場合は、NSX Edge の可用性が失われる可能性があります。

vSphere 高可用性の詳細については、『vSphere の可用性』を参照してください。

高可用性構成の変更

NSX Edge のインストール時に指定した HA 構成を変更できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブをクリックします。

- 5 [HA 構成 (HA Configuration)] パネルで [変更 (Change)] をクリックします。
- 6 [HA 構成の変更] ダイアログ ボックスで、適宜変更を行います。

注: 高可用性が有効になる前にこの Edge Appliance で L2 VPN が構成されている場合、少なくとも 2 つの内部インターフェイスが設定されている必要があります。L2 VPN ですでに使用されているこの Edge で 1 つのインターフェイスが設定されている場合、Edge Appliance の HA は無効になります。

- 7 [OK] をクリックします。

NSX Edge と NSX Manager の強制同期

NSX Manager から NSX Edge に同期要求を送信できます。

NSX Manager で認識されている Edge 構成をすべてのコンポーネントに同期する必要がある場合、強制同期を使用します。


注: 6.2 以降、強制同期では、水平方向のルーティングトラフィックのデータ損失が回避されますが、垂直方向のルーティングとブリッジで中断が発生する場合があります。

強制同期の結果、以下の操作が実行されます。

- Edge Appliance が再起動され、最新の構成が適用されます。
- ホストとの接続が閉じられます。
- NSX Manager がプライマリまたはスタンドアロンであり、Edge が論理分散ルーターの場合、コントローラ クラスタが同期されます。
- 分散ルーター インスタンスを同期するように、関連するすべてのホストにメッセージが送信されます。

重要: Cross-vCenter NSX 環境では、最初に NSX Edge インスタンスをプライマリ NSX Manager で強制同期し、それが完了した後で、NSX Edge インスタンスをセカンダリ NSX Manager で強制同期する必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge インスタンスを選択します。
- 4 [その他のアクション (More Actions)] () アイコンをクリックし、[強制同期 (Force Sync)] を選択します。

リモート Syslog サーバの設定

1 台または 2 台のリモート Syslog サーバを設定できます。NSX Edge アプライアンスから流れるファイアウォールイベントに関連した NSX Edge のイベントとログは、Syslog サーバに送信されます。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 [詳細 (Details)] パネルで、Syslog サーバの横の [変更 (Change)] をクリックします。
- 6 両方のリモート Syslog サーバの IP アドレスを入力し、プロトコルを選択します。
- 7 [OK] をクリックして構成を保存します。

NSX Edge のステータスの表示

ステータス ページには、選択した NSX Edge のインターフェイスを流れるトラフィックのグラフと、ファイアウォール サービスとロード バランサ サービスの接続統計が表示されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックします。
- 5 ステータスを表示する期間を選択します。

次のステップ

NSX Edge の詳細を表示するには、[管理 (Manage)] をクリックし、[設定 (Settings)] をクリックします。

NSX Edge の再デプロイ

強制同期の後、NSX Edge サービスが期待どおりに動作しない場合は、NSX Edge インスタンスを再デプロイできます。

注: 再デプロイは、停止を伴う操作です。まず強制同期を適用し、問題が解決しない場合に再デプロイを行うことをお勧めします。

NSX Edge インスタンスの再デプロイでは、次のタスクが実行されます。

- Edge Appliance が削除され、最新の構成が適用された状態で、新たにデプロイされます。
- コントローラから論理ルーターが削除された後、最新の構成が適用された状態で、再作成されます。
- ホストの分散論理ルーター インスタンスが削除された後、最新の構成が適用された状態で、再作成されます。

グレースフル リスタートが有効になっていない場合、OSPF の隣接関係は再デプロイ中に取り消されます。

重要: Cross-vCenter 環境では、最初に NSX Edge インスタンスをプライマリ NSX Manager に再デプロイし、それが完了した後で、NSX Edge インスタンスをセカンダリ NSX Manager に再デプロイする必要があります。プライマリとセカンダリの両方の NSX Manager に再デプロイする必要があります。

前提条件

再デプロイ中に NSX Edge Services Gateway アプライアンスを追加でデプロイするために、十分なリソースがホストにあることを確認します。各サイズの NSX Edge で必要とされるリソースについては、[章 1 「NSX のシステム要件」](#) を参照してください。

- 単一の NSX Edge インスタンスの場合、パワーオン状態の NSX Edge アプライアンスが、再デプロイ中に 2 台存在することになります。
- NSX 6.2.3 以降、高可用性構成の 2 台の NSX Edge インスタンスを再デプロイする場合、2 台の新しいアプライアンスがデプロイされてから、古いアプライアンスと置き換えられます。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 4 台存在することになります。NSX Edge が再デプロイが完了すると、どちらかの高可用性アプライアンスがアクティブになります。
- NSX 6.2.3 より前のバージョンで高可用性構成の NSX Edge インスタンスを再デプロイする場合、古いアプライアンスを置き換える際は、新しいアプライアンスを一度に 1 台だけデプロイします。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge の再デプロイ中に 3 台存在することになります。NSX Edge インスタンスが再デプロイされると、通常は高可用性インデックス 0 が割り当てられている NSX Edge アプライアンスがアクティブになります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge インスタンスを選択します。
- 4 [アクション (Actions)] () アイコンをクリックし、[Edge の再デプロイ (Redeploy Edge)] を選択します。

NSX Edge 仮想マシンが新しい仮想マシンで置き換えられ、すべてのサービスがリストアされます。再デプロイしても正常に動作しない場合は、NSX Edge 仮想マシンをパワーオフし、NSX Edge をもう一度再デプロイします。

注: 再デプロイは次の場合に効果が得られないことがあります。


- NSX Edge をインストールしたリソース プールが vCenter インベントリ内に存在しなくなったか、その Mold (管理オブジェクト ID) が変更された。
- NSX Edge をインストールしたデータストアが破損した/アンマウントされたか、アクセス不能になった。
- NSX Edge インターフェイスが接続されている dvportGroups が vCenter インベントリ内に存在しなくなったか、その Mold (vCenter Server 内の識別子) が変更された。

上の条件のいずれかが真の場合は、REST API 呼び出しを使用して、リソース プール、データストア、または dvPortGroup の Mold を更新する必要があります。『NSX API プログラミング ガイド』を参照してください。

NSX Edge のテクニカル サポート ログのダウンロード

テクニカル サポート ログは、NSX Edge インスタンスごとにダウンロードできます。NSX Edge インスタンスで高可用性が有効になっている場合は、両方の NSX Edge 仮想マシンからサポート ログがダウンロードされます。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge インスタンスを選択します。
- 4 [その他のアクション (More Actions)] () アイコンをクリックし、[テクニカル サポート ログのダウンロード (Download Tech Support Logs)] を選択します。
- 5 テクニカル サポート ログが生成されたら、[ダウンロード (Download)] をクリックします。
- 6 [ダウンロード先の選択] ダイアログ ボックスで、ログ ファイルを保存するディレクトリを参照します。
- 7 [保存 (Save)] をクリックします。
- 8 [閉じる (Close)] をクリックします。

スタティック ルートの追加

ターゲット サブネットまたはホストのスタティック ルートを追加できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[ルーティング (Routing)] タブをクリックします。
- 5 左側のパネルから [スタティック ルート (Static Routes)] を選択します。
- 6 [追加 (Add)] () アイコンをクリックします。
- 7 CIDR 表記に [ネットワーク (Network)] を入力します。
- 8 [ネクスト ホップ (Next Hop)] の IP アドレスを入力します。

ルーターは、ネクスト ホップに直接到達する必要があります。

ECMP が有効になっている場合、複数のネクスト ホップを入力できます。
- 9 スタティック ルートを追加する [インターフェイス (Interface)] を選択します。

10 [MTU] では、必要に応じてデータ パケット転送の最大値を編集します。

MTU は、NSX Edge インターフェイスで設定された MTU を超えることはできません。

11 要求された場合は、[アドミニストレーティブ ディスタンス (Admin Distance)] を入力します。

1 ~ 255 の値を選択します。特定のネットワークに対して複数のルートがある場合、管理ディスタンスを使用してどのルートを使用するかを選択します。管理ディスタンスが低いほど、ルートの優先順位は高くなります。

表 9-2. デフォルトの管理ディスタンス

ルート ソース	デフォルトの管理ディスタンス
接続済み	0
スタティック	1
外部 BGP	20
OSPF エリア内	30
OSPF エリア間	110
内部 BGP	200

管理ディスタンスを 255 にすると、スタティック ルートがルーティング テーブル (RIB) とデータ プレーンから除外されるため、ルートが使用されません。

12 (オプション) [ロケール ID (Locale ID)] を入力します。

デフォルトでは、ルートのロケール ID は NSX Manager と同じです。ここでロケール ID を指定すると、ルートがこのロケール ID に関連付けられます。これらのルートは、ロケール ID が一致するホストにのみ送信されます。詳細については「[Cross-vCenter NSX トポロジ](#)」を参照してください。

13 (オプション) スタティック ルートの [説明 (Description)] を入力します。

14 [OK] をクリックします。

論理（分散）ルーター上での OSPF の設定

論理ルーター上に OSPF を設定すると、論理ルーター間での仮想マシンの接続、論理ルーターから Edge Services Gateway (ESG) への仮想マシンの接続が可能になります。

OSPF ルーティング ポリシーでは、コストの等しいルート間でトラフィックのロード バランシングを動的に処理できます。

OSPF ネットワークは、トラフィック フローを最適化し、ルーティング テーブルのサイズを制限するため、ルーティング エリアに分割されます。エリアは、同じエリア ID を持つ OSPF ネットワーク、ルーター、およびリンクの論理コレクションです。

エリアはエリア ID で識別されます。

前提条件

ルーター ID を「例：論理（分散）ルーター上で設定されている OSPF」の説明に従って設定する必要があります。

ルーター ID を有効にすると、フィールドにはデフォルトで、論理ルーターのアップリンク インターフェイスが入力されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 論理ルーターをダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[OSPF] をクリックします。
- 5 OSPF を有効にします。
 - a ウィンドウの右上にある [編集 (Edit)] をクリックして、[OSPF の有効化 (Enable OSPF)] をクリックします。
 - b [転送アドレス (Forwarding Address)] に、データパス パケットを転送するために、ホスト内のルーターのデータパス モジュールで使用する IP アドレスを入力します。
 - c [プロトコル アドレス (Protocol Address)] に、[転送アドレス (Forwarding Address)] と同じサブネット内の一意の IP アドレスを入力します。プロトコル アドレスは、ピアと隣接するために、プロトコルによって使用されます。
- 6 OSPF エリアを設定します。
 - a オプションで、デフォルトで設定されている Not-So-Stubby Area (NSSA) 51 を削除します。
 - b [エリア定義 (Area Definitions)] で、[追加 (Add)] アイコンをクリックします。
 - c エリア ID を入力します。NSX Edge では、IP アドレスまたは 10 進数形式のエリア ID を使用できます。
 - d [タイプ (Type)] で、[標準 (Normal)] または [NSSA] を選択します。

NSSA は、AS 外部の Link State Advertisement (LSA) の NSSA へのフラッディングを防止し、外部の宛先に対するデフォルト ルーティングを使用します。したがって、NSSA は OSPF ルーティング ドメインのエッジに配置する必要があります。NSSA は外部ルートを OSPF ルーティング ドメインにインポートできるため、OSPF ルーティング ドメインに属さない小規模なルーティング ドメインに中継サービスを提供できます。
- 7 (オプション) [認証 (Authentication)] のタイプを選択します。OSPF では、エリア レベルで認証が実行されます。

エリア内のすべてのルーターに、同じ認証と対応するパスワードが設定されている必要があります。MD5 認証が機能するためには、受信ルーターと送信ルーターの両方に同じ MD5 鍵が必要です。

 - a [なし (None)] : 認証は要求されません (デフォルト値)。
 - b [パスワード (Password)] : この認証方法では、パスワードは送信パケットに含まれます。
 - c [MD5] : この認証方法では、MD5 (メッセージダイジェスト タイプ 5) 暗号化が使用されます。MD5 チェックサムは送信パケットに含まれます。
 - d [パスワード (Password)] または [MD5] タイプの認証の場合、パスワードまたは MD5 鍵を入力します。
- 8 エリアにインターフェイスをマッピングします。
 - a [インターフェイス マッピングのエリア (Area to Interface Mapping)] で、[追加 (Add)] アイコンをクリックし、OSPF エリアに属するインターフェイスをマッピングします。
 - b マッピングするインターフェイスとマッピング先の OSPF エリアを選択します。

9 (オプション) 必要に応じて、デフォルトの OSPF 設定を編集します。

通常、デフォルト OSPF 設定を維持することをお勧めします。設定を変更する場合は、OSPF ピアで同じ設定が使用されていることを確認してください。

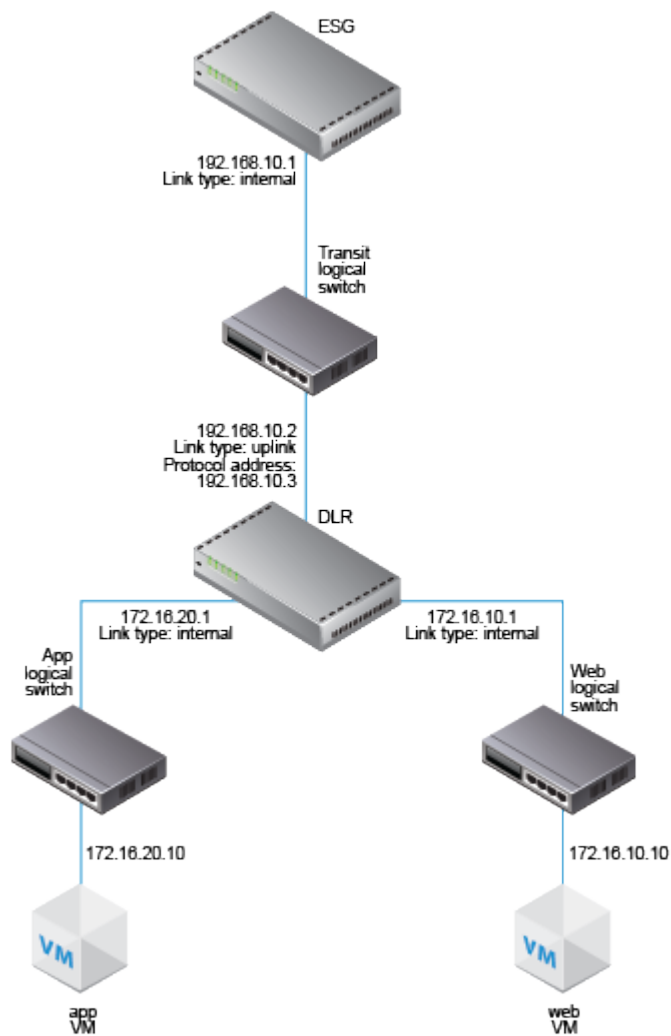
- a [Hello 間隔 (Hello Interval)] には、インターフェイスで送信されるハロー パケット間のデフォルト間隔が表示されます。
- b [Dead 間隔 (Dead Interval)] には、1 つ以上のハロー パケットをネイバーから受信しないとルーターでネイバーの停止が宣言されるデフォルト間隔が表示されます。
- c [優先順位 (Priority)] には、インターフェイスのデフォルトの優先順位が表示されます。優先順位の最も高いインターフェイスが指定ルーターになります。
- d インターフェイスの [コスト (Cost)] には、そのインターフェイスを通じてパケットを送信するのに必要なデフォルトのオーバーヘッドが表示されます。インターフェイスのコストとバンド幅は反比例します。バンド幅が大きくなれば、コストは小さくなります。

10 [変更の発行 (Publish Changes)] をクリックします。

例：論理（分散）ルーター上で設定されている OSPF

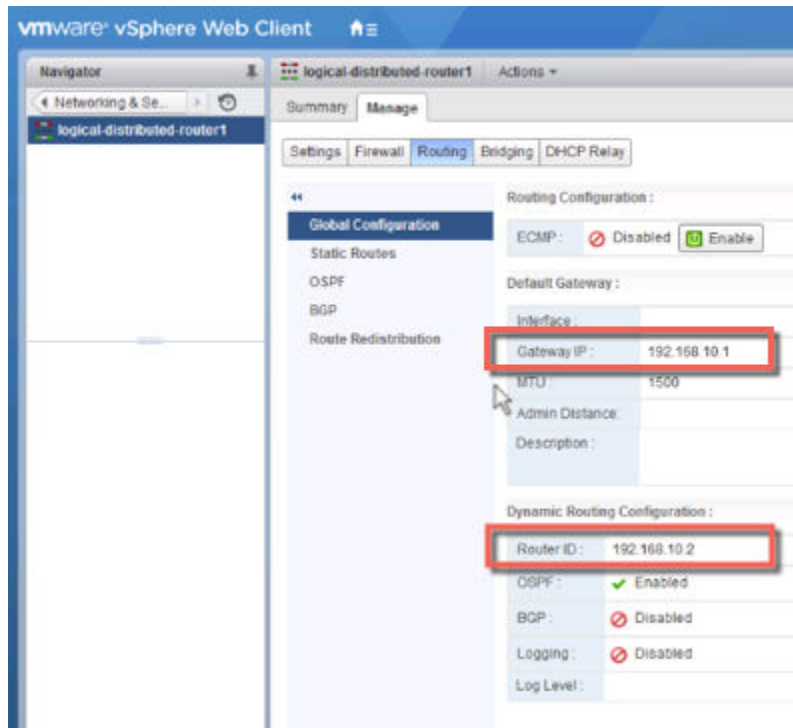
次に示す、OSPF を使用する単純な NSX シナリオでは、論理ルーター (DLR) と Edge Services Gateway (ESG) が OSPF のネイバー関係になっています。

図 9-1. NSX トポロジ



次の画面では、論理ルーターのデフォルト ゲートウェイは ESG の内部インターフェイスの IP アドレス (192.168.10.1) です。

ルーター ID は論理ルーターのアップリンク インターフェイス、つまり ESG (192.168.10.2) と接する IP アドレスです。



論理ルーター設定では、転送アドレスとして 192.168.10.2 が使用されます。プロトコルアドレスには、同じサブセット内にあり、他の場所では使用されない、任意の IP アドレスを指定できます。この例では、192.168.10.3 が指定されています。指定されたエリア ID は 0 で、アップリンク インターフェイス（ESG に接するインターフェイス）がそのエリアにマッピングされます。

The screenshot shows the NSX Manager interface for configuring a logical distributed router. The left sidebar contains a tree view with 'Global Configuration', 'Static Routes', 'OSPF' (selected), 'BGP', and 'Route Redistribution'. The main panel is titled 'logical distributed-router1' and has an 'Actions' dropdown. Below the title are tabs for 'Summary' and 'Manage'. Under 'Manage', there are sub-tabs for 'Settings', 'Firewall', 'Routing' (selected), 'Bridging', and 'DHCP Relay'. The 'Routing' tab displays the 'OSPF Configuration' section, which includes fields for 'Status' (Enabled), 'Protocol Address' (192.168.10.3), 'Forwarding Address' (192.168.10.2), 'Graceful Restart' (Enabled), and 'Default Originate' (Disabled). Below this is the 'Area Definitions' section, which shows a table with columns for 'Area ID', 'Type', and 'Authentication'. The table contains one entry: Area ID 0, Type Normal, Authentication None. At the bottom is the 'Area to Interface Mapping' section, which shows a table with columns for 'Interface', 'Area ID', 'Hello Interval (seconds)', 'Dead Interval (seconds)', 'Priority', and 'Cost'. The table contains one entry: Interface to-ESG, Area ID 0, Hello Interval 10, Dead Interval 40, Priority 128, Cost 1.

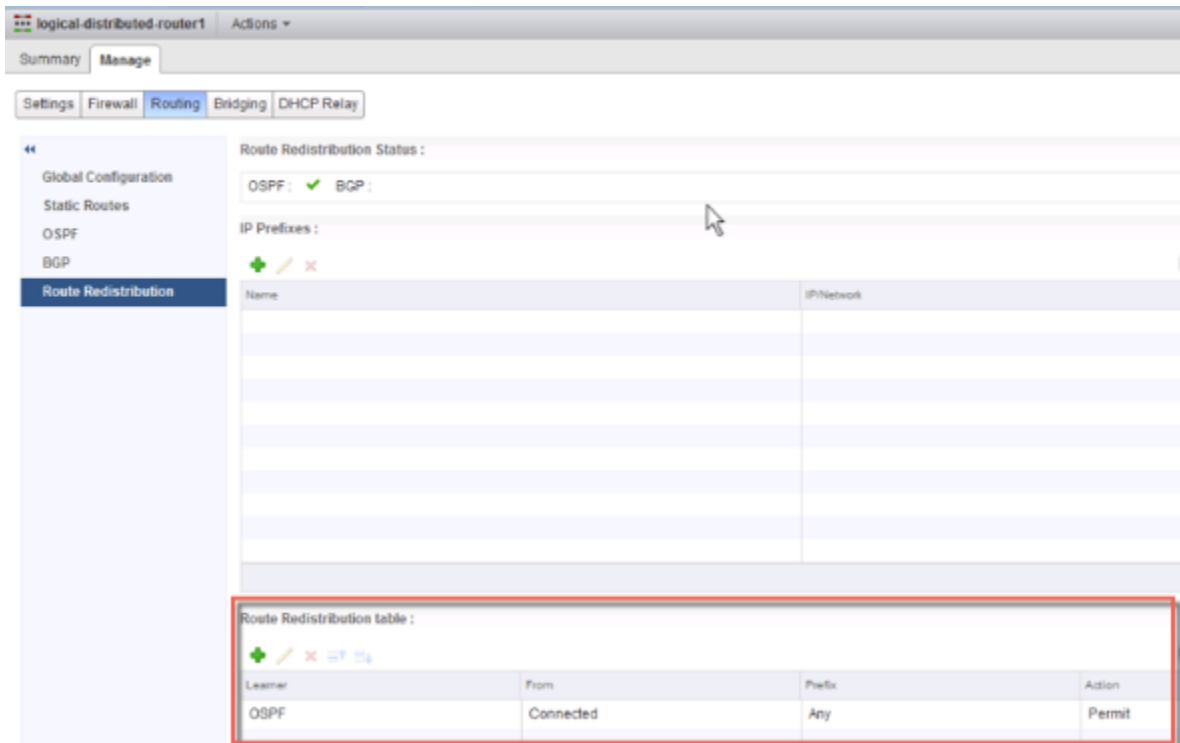
Area ID	Type	Authentication
0	Normal	None

Interface	Area ID	Hello Interval (seconds)	Dead Interval (seconds)	Priority	Cost
to-ESG	0	10	40	128	1

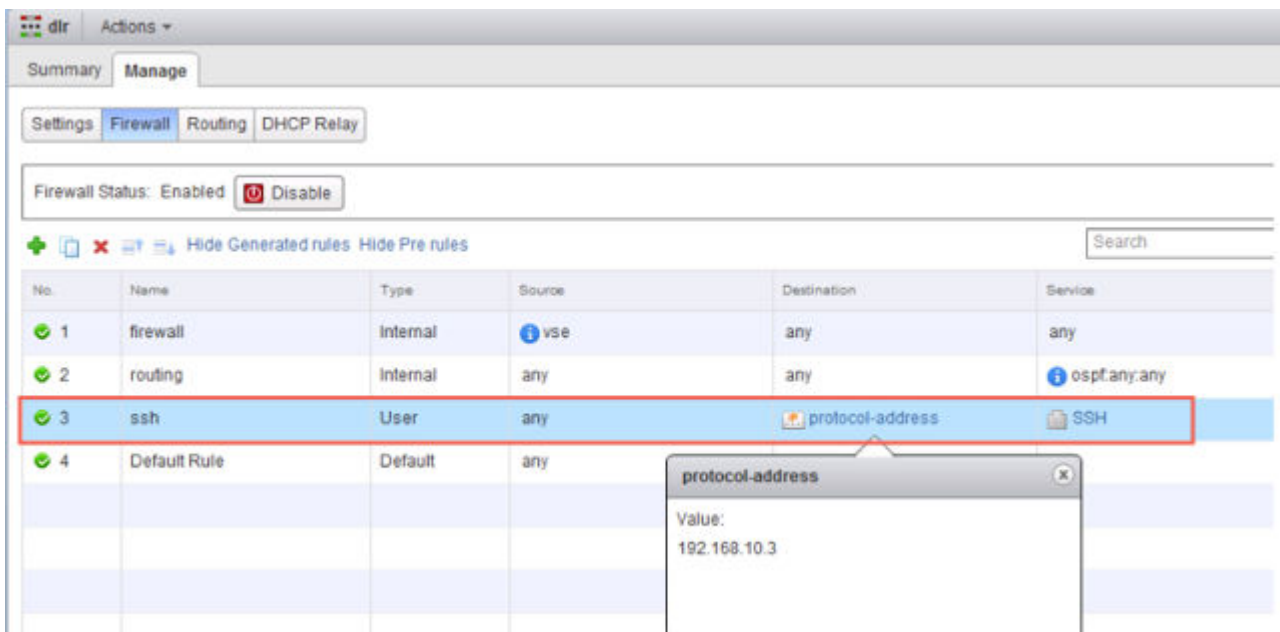
次のステップ

ルート再配分とファイアウォールの設定により、正しいルートがアドバタイズされることを確認します。

この例では、論理ルーターの接続ルート（172.16.10.0/24 と 172.16.20.0/24）が OSPF にアドバタイズされます。



論理ルーターを作成したときに SSH を有効にした場合は、論理ルーターのプロトコル アドレスへの SSH を許可するファイアウォール フィルタの設定も必要になります。次はその例です。



Edge Services Gateway 上での OSPF の設定

Edge Services Gateway (ESG) 上で OSPF を構成すると、ESG がルートを学習してアドバタイズできるようになります。ESG 上で OSPF を最も一般的に利用する場所は、ESG と論理（分散）ルーターとの間のリンク上です。このため、ESG は、論理ルーターに接続している論理インターフェイス (LIFS) について学習できます。これは、OSPF、IS-IS、BGP、または固定ルーティングを使用することで実現できます。

OSPF ルーティング ポリシーでは、コストの等しいルート間でトラフィックのロード バランシングを動的に処理できます。

OSPF ネットワークは、トラフィック フローを最適化し、ルーティング テーブルのサイズを制限するため、ルーティング エリアに分割されます。エリアは、同じエリア ID を持つ OSPF ネットワーク、ルーター、およびリンクの論理コレクションです。

エリアはエリア ID で識別されます。

前提条件

ルーター ID を「例：Edge Services Gateway 上で設定されている OSPF」の説明に従って設定する必要があります。

ルーター ID を有効にすると、フィールドにはデフォルトで、ESG のアップリンク インターフェイスの IP アドレスが入力されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 ESG をダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[OSPF] をクリックします。
- 5 OSPF を有効にします。
 - a ウィンドウの右上にある [編集 (Edit)] をクリックして、[OSPF の有効化 (Enable OSPF)] をクリックします。
 - b (オプション) OSPF サービスの再起動時にパケット転送が中断されないようにするには、[グレースフル リスタートの有効化 (Enable Graceful Restart)] をクリックします。
 - c (オプション) ESG が自身をデフォルト ゲートウェイとしてピアにアドバタイズできるようにするには、[デフォルトの発信元の有効化 (Enable Default Originate)] をクリックします。
- 6 OSPF エリアを設定します。
 - a (オプション) デフォルトで設定されている Not-So-Stubby Area (NSSA) 51 を削除します。
 - b [エリア定義 (Area Definitions)] で、[追加 (Add)] アイコンをクリックします。

- c エリア ID を入力します。NSX Edge では、IP アドレスまたは 10 進数形式のエリア ID を使用できます。
- d [タイプ (Type)] で、[標準 (Normal)] または [NSSA] を選択します。

NSSA は、AS 外部の Link State Advertisement (LSA) の NSSA へのフラッドिंगを防止し、外部の宛先に対するデフォルト ルーティングを使用します。したがって、NSSA は OSPF ルーティング ドメインのエッジに配置する必要があります。NSSA は外部ルートを OSPF ルーティング ドメインにインポートできるため、OSPF ルーティング ドメインに属さない小規模なルーティング ドメインに中継サービスを提供できます。

7 (オプション) [認証 (Authentication)] のタイプを選択します。OSPF では、エリア レベルで認証が実行されます。

エリア内のすべてのルーターに、同じ認証と対応するパスワードが設定されている必要があります。MD5 認証が機能するためには、受信ルーターと送信ルーターの両方に同じ MD5 鍵が必要です。

- a [なし (None)] : 認証は要求されません (デフォルト値)。
- b [パスワード (Password)] : この認証方法では、パスワードは送信パケットに含まれます。
- c [MD5] : この認証方法では、MD5 (メッセージ ダイジェスト タイプ 5) 暗号化が使用されます。MD5 チェックサムは送信パケットに含まれます。
- d [パスワード (Password)] または [MD5] タイプの認証の場合、パスワードまたは MD5 鍵を入力します。

8 エリアにインターフェイスをマッピングします。

- a [インターフェイス マッピングのエリア (Area to Interface Mapping)] で、[追加 (Add)] アイコンをクリックし、OSPF エリアに属するインターフェイスをマッピングします。
- b マッピングするインターフェイスとマッピング先の OSPF エリアを選択します。

9 (オプション) デフォルトの OSPF 設定を編集します。

通常、デフォルト OSPF 設定を維持することをお勧めします。設定を変更する場合は、OSPF ピアで同じ設定が使用されていることを確認してください。

- a [Hello 間隔 (Hello Interval)] には、インターフェイスで送信されるハロー パケット間のデフォルト間隔が表示されます。
- b [Dead 間隔 (Dead Interval)] には、1 つ以上のハロー パケットをネイバーから受信しないとルーターでネイバーの停止が宣言されるデフォルト間隔が表示されます。
- c [優先順位 (Priority)] には、インターフェイスのデフォルトの優先順位が表示されます。優先順位の最も高いインターフェイスが指定ルーターになります。
- d インターフェイスの [コスト (Cost)] には、そのインターフェイスを通じてパケットを送信するのに必要なデフォルトのオーバーヘッドが表示されます。インターフェイスのコストとバンド幅は反比例します。バンド幅が大きくなれば、コストは小さくなります。

10 [変更の発行 (Publish Changes)] をクリックします。

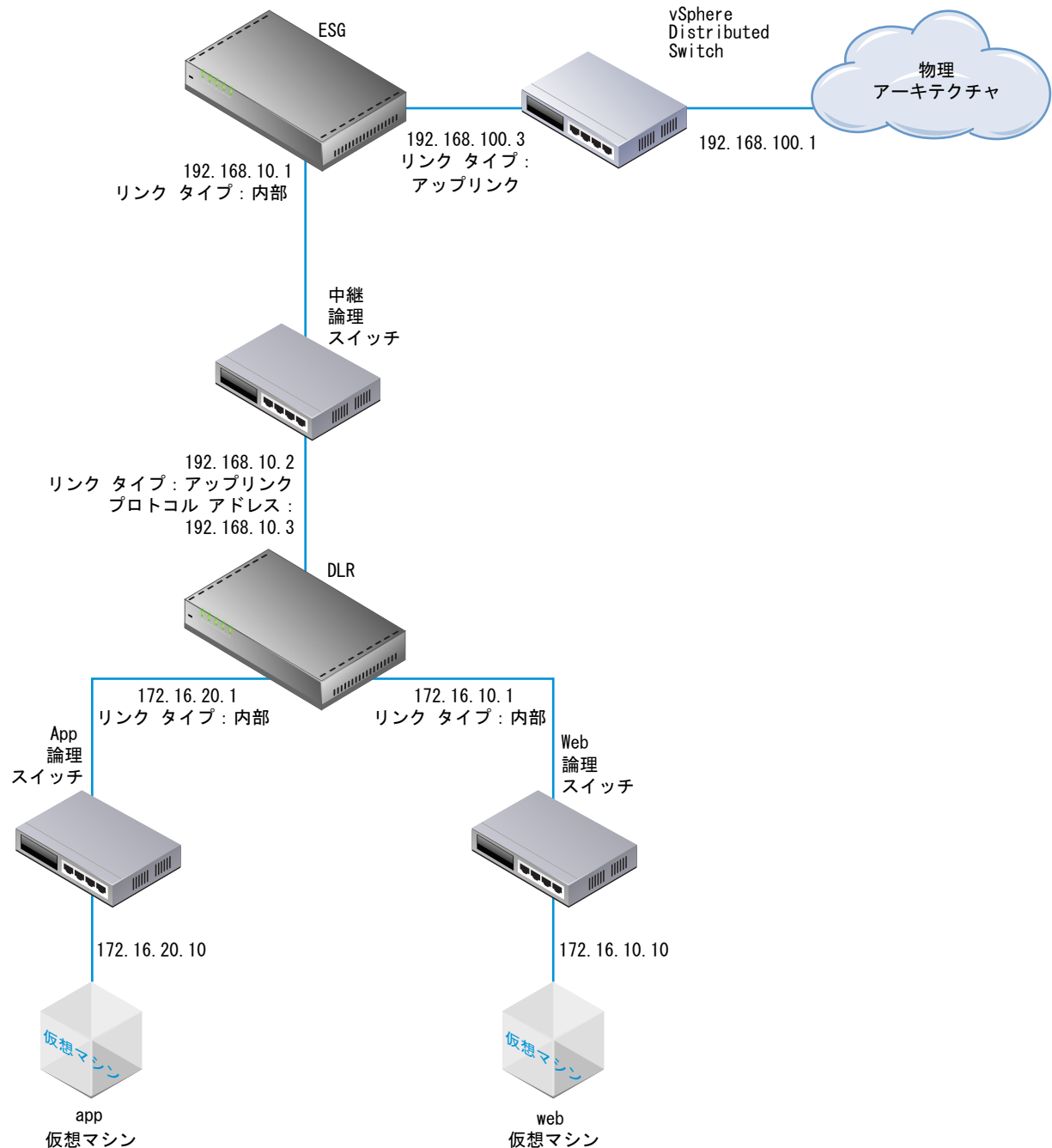
11 ルート再配分とファイアウォールの設定により、正しいルートがアドバタイズされることを確認します。

例：Edge Services Gateway 上で設定されている OSPF

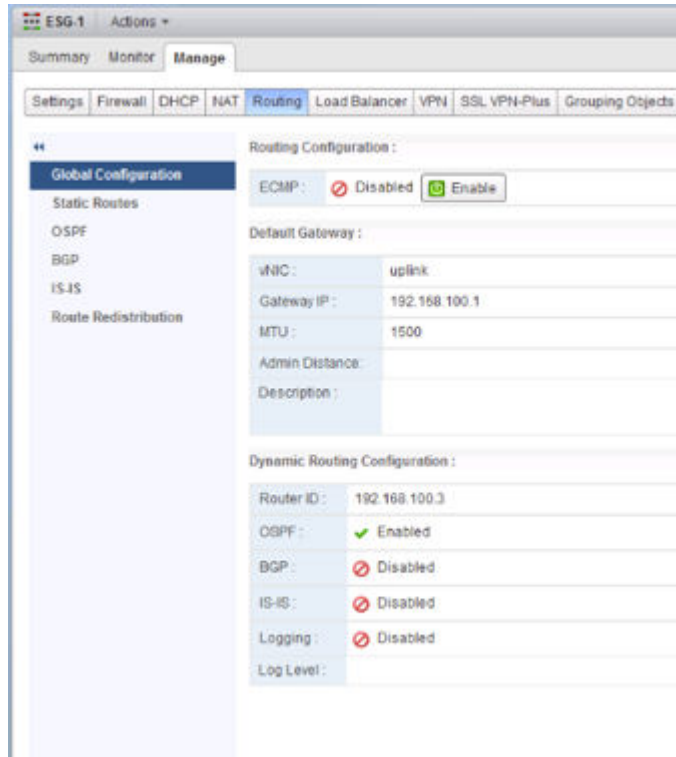
OSPF を使用する単純な NSX シナリオの 1 つとして、論理ルーターと Edge Services Gateway が OSPF のネイバー関係になっている例をここに示します。

ESG は、ブリッジ、物理ルーター、またはここで示すように vSphere Distributed Switch 上のアップリンク ポートグループを介して外部に接続できます。

図 9-2. NSX トポロジ



次の画面では、ESG のデフォルト ゲートウェイは外部ピアに対する ESG のアップリンク インターフェイスです。
ルーター ID は ESG のアップリンク インターフェイス IP アドレス、つまり外部ピアに接する IP アドレスです。



指定されたエリア ID は 0 で、内部インターフェイス（論理ルーターに接するインターフェイス）がそのエリアにマッピングされます。

ESG-1 Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration
Static Routes
OSPF
BGP
IS-IS
Route Redistribution

OSPF Configuration : Edit

Status : ✓ Enabled
Graceful Restart : ✓ Enabled
Default Originate : ✗ Disabled

Area Definitions :

Area ID	Type	Authentication
0	Normal	None

Area to Interface Mapping :

vNIC	Area ID	Hello Interval (seconds)	Dead Interval (seconds)	Priority	Cost
internal	0	10	40	128	1

接続ルートは OSPF に再配分されるため、OSPF のネイバー（論理ルーター）は ESG のアップリンク ネットワークを学習できます。

Summary Monitor **Manage**

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration
Static Routes
OSPF
BGP
IS-IS
Route Redistribution

Route Redistribution Status:

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes:

+ - ✎ ✖

Name	IP Network

Route Redistribution table:

+ - ✎ ✖

Learned	From	Prefix	Action
OSPF	Connected	Any	Permit

注: さらに、ESG とその外部ピア ルーター間に OSPF を設定できますが、通常このリンクは、ルートのアドバタイズに BGP を使用します。

ESG が論理ルーターから OSPF 外部ルートを学習していることを確認します。

```
NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 5

S      0.0.0.0/0          [0/0]          via 192.168.100.1
0 E2  172.16.10.0/24      [110/1]        via 192.168.10.2
0 E2  172.16.20.0/24      [110/1]        via 192.168.10.2
C      192.168.10.0/29    [0/0]          via 192.168.10.1
C      192.168.100.0/24   [0/0]          via 192.168.100.3
```

接続を検証するには、物理アーキテクチャ内の外部デバイスが仮想マシンに ping を実行できることを確認します。

次はその例です。

```
PS C:\Users\Administrator> ping 172.16.10.10
```

```
Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.10.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10
```

```
Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.20.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

BGP の設定

ボーダー ゲートウェイ プロトコル (BGP) によって、主要なルーティングの決定が行われます。BGP には、複数の自律システム間のネットワーク到達可能性を示す IP ネットワークまたはプリフィックスのテーブルがあります。

ルーティング情報の交換前に 2 つの BGP スピーカ間に基になる接続が確立されます。この関係を維持するために、BGP スピーカからキープ アライブ メッセージが送信されます。接続が確立されると、各 BGP スピーカでルートを交換し、それらのテーブルを同期します。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[BGP] をクリックします。
- 5 [編集 (Edit)] をクリックします。
- 6 [BGP 構成の編集] ダイアログ ボックスで、[BGP の有効化 (Enable BGP)] をクリックします。
- 7 BGP サービスの再起動時にパケット転送が中断されないようにするには、[グレースフル リスタートの有効化 (Enable Graceful Restart)] をクリックします。
- 8 NSX Edge が自身をデフォルト ゲートウェイとしてピアにアドバタイズできるようにするには、[デフォルトの発信元の有効化 (Enable Default Originate)] をクリックします。
- 9 [ローカル AS (Local AS)] にルーター ID を入力します。ローカル AS を入力します。これは、BGP が他の自律システム (AS) のルーターとピアを形成する場合にアドバタイズされます。ルーターがトラバースする AS のパスは、ターゲットへの最適パスを選択するときのメトリックの 1 つとして使用されます。
- 10 [OK] をクリックします。
- 11 [ネイバー (Neighbors)] で、[追加 (Add)] アイコンをクリックします。
- 12 ネイバーの IP アドレスを入力します。

Edge Services Gateway (ESG) と論理ルーターの間に BGP ピアリングを設定する場合は、ESG の BGP ネイバー アドレスとして、論理ルーターのプロトコル IP を使用します。
- 13 (論理ルーターのみ) 転送アドレスを入力します。

転送アドレスは、BGP ネイバー (アップリンク インターフェイス) に接する分散論理ルーターのインターフェイスに割り当てた IP アドレスです。
- 14 (論理ルーターのみ) プロトコル アドレスを入力します。

プロトコル アドレスは、BGP ネイバー関係を確立するために論理ルーターが使用する IP アドレスです。プロトコル アドレスには、転送アドレスと同じサブネット内の (他の場所では使用されない) IP アドレスを指定できます。Edge Services Gateway (ESG) と論理ルーターの間に BGP ピアリングを設定する場合は、ESG ネイバーの IP アドレスとして、論理ルーターのプロトコル IP を使用します。
- 15 リモート AS を入力します。
- 16 必要に応じてネイバー接続のデフォルトの重みを編集します。
- 17 [ホールド ダウン タイマー (Hold Down Timer)] には、ソフトウェアでピアの停止が宣言される、キープ アライブ メッセージを受信しなくなったからの期間 (180 秒) が表示されます。必要に応じて編集します。

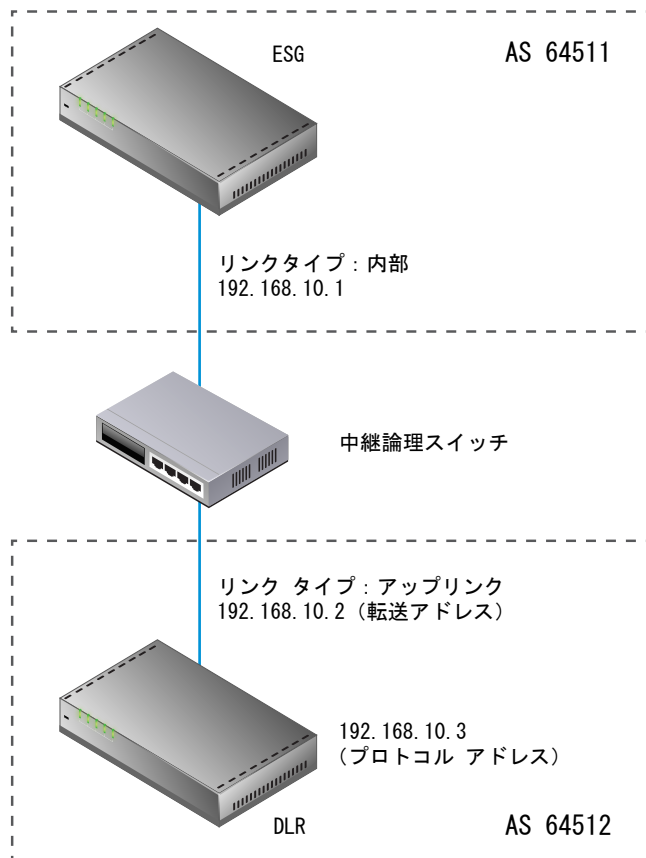
- 18 [キープ アライブ タイマー (Keep Alive Timer)] には、ソフトウェアがそのピアにキープ アライブ メッセージを送信するデフォルトの頻度 (60 秒) が表示されます。必要に応じて編集します。
- 19 認証が必要な場合は、認証パスワードを入力します。ネイバー間の接続で送信される各セグメントが検証されます。MD5 認証は、両方の BGP ネイバーで同じパスワードを使用して設定する必要があります。同じでないと、これらのネイバー間の接続が作成されません。
- 20 ネイバーからルート フィルタリングを指定するには、[BGP フィルタ (BGP Filters)] 領域の [追加 (Add)] アイコンをクリックします。



警告: フィルタの最後で、「すべてブロックする」ルールが適用されます。

- 21 ネイバーからのトラフィックをフィルタリングするのか、ネイバーへのトラフィックをフィルタリングするのかを示す方向を選択します。
- 22 トラフィックの許可または拒否を示すアクションを選択します。
- 23 ネイバーへのフィルタリング/ネイバーからのフィルタリングを行うネットワークを CIDR 形式で入力します。
- 24 フィルタリングする IP 接頭辞を入力し、[OK] をクリックします。
- 25 [変更の発行 (Publish Changes)] をクリックします。

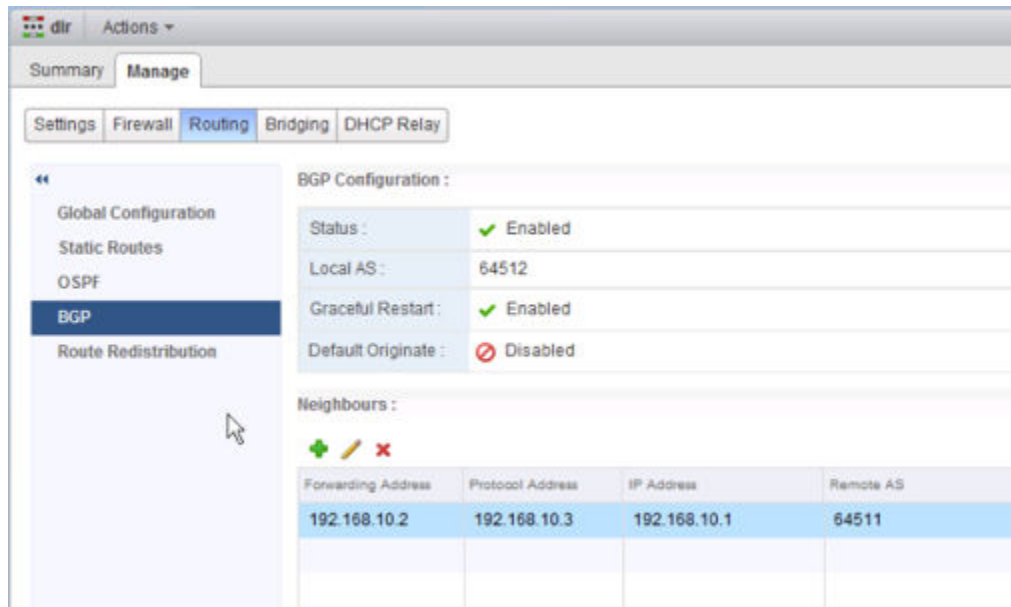
例：ESG と論理ルーター間での BGP の構成



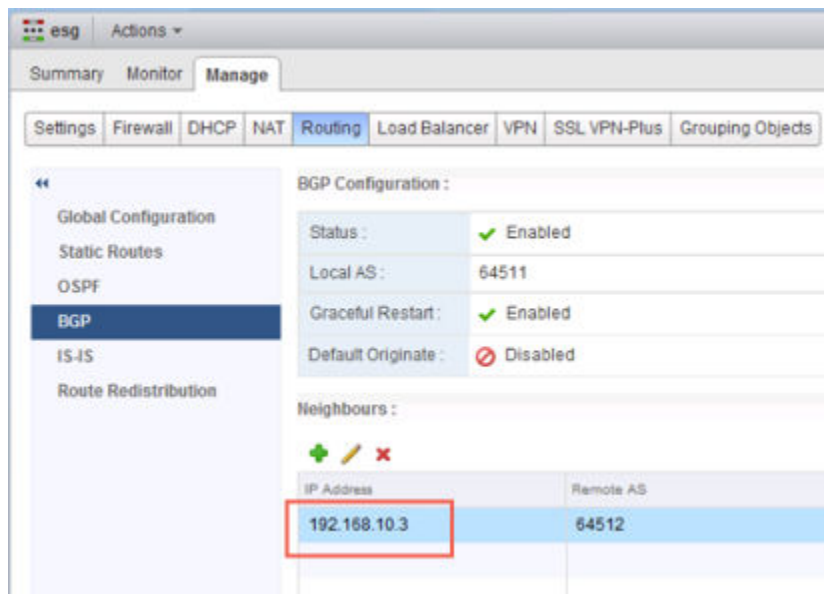
このトポロジでは、ESG は AS 64511 内にあります。論理ルーター (DLR) は AS 64512 内にあります。

論理ルーターの転送アドレスは、192.168.10.2 です。これは、論理ルーターのアップリンク インターフェイス上で設定されたアドレスです。論理ルーターのプロトコル アドレスは、192.168.10.3 です。これは、論理ルーターと BGP とのピアリング関係を構築するために ESG が使用するアドレスです。

論理ルーター上で、次のように BGP を設定します。



ESG 上で、次のように BGP を構成します。



ESG のネイバー アドレスは 192.168.10.3 です。これは、論理ルーターのプロトコル アドレスです。

論理ルーターで `show ip bgp neighbors` コマンドを実行して、BGP state が Established になっていることを確認します。

```

NSX-edge-6-0> show ip bgp neighbors

BGP neighbor is 192.168.10.1,    remote AS 64511,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 120 messages, Sent 125 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x9aa20f3c
  Route refresh request:received 0 sent 0
  Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 5
Local host: 192.168.10.3, Local port: 179
Remote host: 192.168.10.1, Remote port: 43846

```

ESG で `show ip bgp neighbors` コマンドを実行して、BGP state が Established になっていることを確認します。

```

NSX-edge-7-0> show ip bgp neighbors

BGP neighbor is 192.168.10.3,    remote AS 64512,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 121 messages, Sent 120 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 3 Identifier 0x40212c6c
  Route refresh request:received 0 sent 0
  Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 1
Local host: 192.168.10.1, Local port: 43846
Remote host: 192.168.10.3, Remote port: 179

```

IS-IS プロトコルの設定

Intermediate System to Intermediate System (IS-IS) は、パケットスイッチ型ネットワークを経由したデータグラムの最適なルートを決定的することによって情報を移動するように設計されたルーティング プロトコルです。

大規模なルーティング ドメインをサポートするため、2 レベルの階層が使用されます。大規模なドメインは、複数のエリアに分割されます。1 つのエリア内のルーティングは、レベル 1 ルーティングと呼ばれます。エリア間のルーティングは、レベル 2 ルーティングと呼ばれます。レベル 2 の中間システム (IS) では、送信先エリアへのパスが追跡されます。レベル 1 の IS では、そのエリア内でのルーティングが追跡されます。別のエリアに送信されるパケットでは、送信先エリアに関係なく、レベル 1 の IS からそのエリア内で最も近いレベル 2 の IS にパケットが送信されます。パケットはレベル 2 ルーティングを経由して送信先エリアに送信されます。この場合、レベル 1 ルーティングを経由して送信先に送信されることもあります。レベル 1 およびレベル 2 両方の IS は、レベル 1-2 と呼ばれます。

注: IS-IS プロトコルは NSX で試験的にサポートされています。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[IS-IS] をクリックします。
- 5 [編集 (Edit)] をクリックし、[IS-IS の有効化 (Enable IS-IS)] をクリックします。
- 6 [システム ID] に値を入力し、IS-IS タイプを選択します。

レベル 1 はエリア内、レベル 2 はエリア間、レベル 1-2 はこの両方です。レベル 2 ルーターは、他のレベル 2 ルーターのみとやりとりできるエリア間ルータです。ルーティング情報はレベル 1 ルーターと他のレベル 1 ルーターとの間で交換されます。同様に、レベル 2 ルーターは他のレベル 2 ルーターのみと情報を交換します。レベル 1-2 ルーターは、両方のレベルで情報を交換し、エリア内ルーターとエリア間ルーターを接続するのに使用されます。
- 7 [ドメイン パスワード (Domain Password)] と [エリア パスワード (Area Password)] に値を入力します。エリアパスワードが挿入されてレベル 1 リンク状態パケットがチェックされ、レベル 2 リンク状態パケットのドメインパスワードがチェックされます。
- 8 IS-IS エリアを定義します。
 - a [エリア (Areas)] で [追加 (Add)] アイコンをクリックします。
 - b エリアの IP アドレスを 3 個まで入力します。
 - c [保存 (Save)] をクリックします。
- 9 インターフェイス マッピングを設定します。
 - a [インターフェイス マッピング (Interface Mapping)] で [追加 (Add)] アイコンをクリックします。
 - b レベル 1、レベル 2、レベル 1-2 隣接のどのインターフェイスを構成しているかを示す [回路タイプ] を選択します。
 - c [Hello 間隔 (Hello Interval)] には、インターフェイスで送信された Hello パケット間のデフォルト間隔（ミリ秒単位）が表示されます。必要に応じてデフォルト値を編集します。

- d [Hello 乗数 (Hello Multiplier)] には、ネイバーの IS-IS Hello パケットがいくつ失敗するとそのネイバーがダウンしていると判断されるかを決定するデフォルトの数が表示されます。必要に応じてデフォルト値を編集します。
- e [LSP 間隔 (LSP Interval)] には、連続的な IS-IS リンク状態パケット (LSP) 転送間の遅延時間（ミリ秒単位）が表示されます。必要に応じてデフォルト値を編集します。
- f [メトリック (Metric)] に、インターフェイスのデフォルトメトリックが表示されます。これは、ネットワーク内でリンクを経由して各インターフェイスから他の場所へ送信される場合のコストを計算するために使用されます。必要に応じてデフォルト値を編集します。
- g [優先順位 (Priority)] に、インターフェイスの優先順位が表示されます。優先順位が最も高いインターフェイスが、指定ルーターになります。必要に応じてデフォルト値を編集します。
- h [メッシュ グループ] に、このインターフェイスが属すメッシュ グループを識別する数値を入力します。必要に応じてデフォルト値を編集します。
- i インターフェイスの認証パスワードを入力し、[OK] をクリックします。必要に応じてデフォルト値を編集します。

10 [変更の発行 (Publish Changes)] をクリックします。

ルート再配分の設定

デフォルトで、ルーターは同じプロトコルが稼働している他のルーターと経路を共有します。マルチプロトコル環境では、プロトコル間で経路を共有するために、ルート再配分を設定する必要があります。

そのネットワークの拒否基準を追加することで、インターフェイスをルート再配分から除外できます。NSX 6.2 では、分散論理ルーターの高可用性（管理）インターフェイスは自動的にルート再配分から除外されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[ルート再配分 (Route Redistribution)] をクリックします。
- 5 [ルート再配分ステータス (Route Redistribution Status)] の横にある [編集 (Edit)] をクリックします。
- 6 ルート再配分を有効にするプロトコルを選択し、[OK] をクリックします。

7 IP プリフィックスを追加します。

IP プリフィックス リストのエントリは、順番に処理されます。

a [IP プリフィックス (IP Prefixes)] で [追加 (Add)] アイコンをクリックします。

b ネットワークの名前と IP アドレスを入力します。

「以下」(LE) 修飾子または「以上」(GE) 修飾子を含めている場合を除き、入力した IP プリフィックスは正確に一致します。

c [OK] をクリックします。

8 IP プリフィックスの再配分基準を指定します。

a [ルート再配分テーブル (Route Redistribution table)] で [追加 (Add)] アイコンをクリックします。

b [ラーナー プロトコル (Learner Protocol)] で、他のプロトコルからルートを学習するプロトコルを選択します。

c [次のものからの学習を許可 (Allow Learning from)] で、ルートの学習元となるプロトコルを選択します。

d [OK] をクリックします。

9 [変更の発行 (Publish Changes)] をクリックします。

NSX Manager ロケール ID の表示

NSX Manager ごとに、ロケール ID があります。デフォルトでは、この ID は NSX Manager UUID に設定されています。この設定は、ユニバーサル分散論理ルーター、クラスタ、またはホスト レベルで上書きできます。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] に移動し、[ネットワークとセキュリティのインベントリ (Networking & Security Inventory)] の下で NSX Manager をクリックします。
- 2 [サマリ (Summary)] タブをクリックします。[ID] フィールドに、その NSX Manager の UUID が格納されています。

ユニバーサル分散論理ルーター上でのロケール ID の設定

ユニバーサル分散論理ルーターの作成時に Local Egress (ローカル出力方向) が有効になっている場合、ホストのロケール ID がルートに関連付けられたロケール ID と一致する場合に限り、ルートがホストに送信されます。ルーター上のロケール ID は変更でき、この更新されたロケール ID は、このルーター上のすべてのルート (固定および動的) に関連付けられます。ルートは、ロケール ID が一致するホストとクラスタに送信されます。

Cross-vCenter NSX 環境のルーティング設定の詳細については、[「Cross-vCenter NSX トポロジ」](#) を参照してください。

前提条件

ユニバーサル分散論理ルーターは、Local Egress (ローカル出力方向) を有効にした状態で作成されている必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 ユニバーサル分散論理ルーターをダブルクリックします。
- 4 [ルーティング (Routing)] タブをクリックして、[グローバル設定 (Global Configuration)] をクリックします。
- 5 [ルーティング設定 (Routing Configuration)] の横にある [編集 (Edit)] をクリックします。
- 6 新しいロケール ID を入力します。

重要: ロケール ID は UUID 形式である必要があります。例: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX。ここで、各 X は 16 進数字 (0 ~ F) で置き換えられます。

ホストまたはクラスタ上でのロケール ID の設定

ユニバーサル分散論理ルーターの作成時に Local Egress (ローカル出力方向) が有効になっている場合、ホストのロケール ID がルートに関連付けられたロケール ID と一致する場合に限り、ルートがホストに送信されます。ホストのクラスタまたはホスト上にロケール ID を設定することで、ルートを選択的にホストに送信できます。

前提条件

ホストまたはクラスタに対してルーティングを実行するユニバーサル分散論理ルーターは、Local Egress (ローカル出力方向) を有効にした状態で作成されている必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [ホストの準備 (Host Preparation)] タブをクリックします。
- 4 設定する必要があるホストまたはクラスタを管理する NSX Manager を選択します。
- 5 変更するホストまたはクラスタを選択します。必要に応じて、クラスタを展開してホストを表示します。
- 6 [設定 (Settings)] アイコン (⚙️) をクリックして、[ロケール ID の変更 (Change Locale ID)] をクリックします。
- 7 新しいロケール ID を入力して、[OK (OK.)] をクリックします。

注: ロケール ID は UUID 形式である必要があります。例: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX。ここで、各 X は 16 進数字 (0 ~ F) で置き換えられます。

ユニバーサル コントローラ クラスタは、この新しいロケール ID に一致するルートのみをホストに送信します。

次のステップ

ロケール ID が指定されたスタティック ルートを設定します。

論理ファイアウォール

論理ファイアウォールは、動的仮想データセンターにセキュリティ メカニズムを提供します。論理ファイアウォールは、それぞれ異なる展開方法に対処する 2 つのコンポーネントから構成されます。分散ファイアウォールではテナントまたはデータセンターの境界における水平方向のアクセス コントロール、Edge ファイアウォールでは垂直方向のトラフィック適用に重点が置かれています。これらのコンポーネントを共に利用することで、仮想データセンターにおけるエンドツーエンドのファイアウォールのニーズに対応できます。この 2 つのテクノロジーは、個別にデプロイすることも、両方をデプロイすることも可能です。

この章には、次のトピックが含まれています。

- [Distributed Firewall](#)
- [Edge ファイアウォール](#)
- [ファイアウォール ルール セクションの操作](#)
- [ファイアウォール ルールの使用](#)
- [ファイアウォールによる保護からの仮想マシンの除外](#)
- [仮想マシンの IP 検出](#)
- [ファイアウォール CPU イベントおよびメモリしきい値イベントの表示](#)
- [ファイアウォール ログ](#)
- [NSX Edge ファイアウォール ルールの使用](#)

Distributed Firewall

Distributed Firewall は、ハイパーバイザー カーネルが組み込まれたファイアウォールで、仮想化されたワークロードとネットワークを表示および制御できます。VMware vCenter Server オブジェクト（データセンターやクラスターなど）、仮想マシンの名前、ネットワーク構造（IP アドレスまたは IPSet アドレス）、VLAN（DVS ポートグループ）、VXLAN（論理スイッチ）、セキュリティ グループ、Active Directory のユーザー グループ ID に基づいてアクセス コントロール ポリシーを作成できます。ファイアウォール ルールは、各仮想マシンの vNIC レベルで適用されます。これは、仮想マシンで vMotion が実行された場合でも一貫したアクセス コントロールが行われるようにするためです。ファイアウォールにハイパーバイザーが組み込まれているという特徴により、ライン レートに近いスループットが実現され、物理サーバにおけるワークロード統合を強化できます。このファイアウォールの分散特性により、ホストをデータセンターに追加すると自動的にファイアウォール容量が拡張されるスケール アウト アーキテクチャを実現できます。

Distributed Firewall は、パフォーマンス向上のために、L2 パケットに対してキャッシュを作成します。L3 パケットは次の順序で処理されます。

- 1 すべてのパケットが、既存の状態を確認されます。これは、既存セッションで偽の SYN や再転送された SYN を検出できるようにするために、SYN に対しても実行されます。
- 2 状態の一致が見つかった場合、パケットは処理されます。
- 3 状態の一致が見つからない場合は、一致が見つかるまで各ルールに対してパケットが処理されます。
 - TCP パケットの場合、状態は、SYN フラグの付いたパケットに対してのみ設定されます。ただし、プロトコルを指定しないルール（サービス ANY）は、任意の組み合わせのフラグを持つ TCP パケットと一致する可能性があります。
 - UDP パケットの場合は、5 タプルの詳細がパケットから抽出されます。状態テーブル内に状態がない場合は、抽出された 5 タプルの詳細を使用して新しい状態が作成されます。それ以降に受信したパケットに対しては、作成した状態に対するマッチングが行われます。
 - ICMP パケットの場合は、状態を作成するのに、ICMP タイプ、コード、およびパケットの方向が使用されます。

Distributed Firewall は、ID ベースのルールの作成にも役立ちます。管理者は、企業の Active Directory で定義されたユーザーのグループメンバーシップに基づいてアクセスをコントロールできます。ID ベースのファイアウォール ルールの使用が想定されるシナリオを次に示します。

- ユーザー認証に Active Directory (AD) を用いるラップトップやモバイル デバイスを使用して、ユーザーが仮想アプリケーションにアクセスする
- 仮想マシンが Microsoft Windows ベースである VDI インフラストラクチャを使用して、ユーザーが仮想アプリケーションにアクセスする

環境にサードパーティ ベンダーのファイアウォール ソリューションがデプロイされている場合は、[「論理ファイアウォールを使用したベンダー ソリューションへのトラフィックのリダイレクト」](#)を参照してください。

Distributed Firewall では、ゲスト仮想マシンまたはワークロード仮想マシン上でオープンソースの VMware Tools を実行する操作は検証されていません。

Distributed Firewall のリソース使用率の ESXi しきい値パラメータ

各 ESXi ホストには、CPU、RAM、1 秒あたりの接続 (CPS) という Distributed Firewall リソース使用率の 3 つのしきい値パラメータが設定されます。200 秒の間に 20 回連続でそれぞれのしきい値を超えた場合、アラームが表示されます。サンプルは 10 秒ごとに取得されます。

100 パーセントの CPU は、ホストで使用可能な合計 CPU に相当します。

100 パーセントの RAM は、Distributed Firewall に割り当てられたメモリ（「合計最大サイズ」）に相当し、これはホストにインストールされた RAM の合計量によって決まります。

表 10-1. 合計最大サイズ

物理メモリ	合計最大サイズ (MB)
0 ~ 8 GB	160
8 GB ~ 32 GB	608

表 10-1. 合計最大サイズ (続き)

物理メモリ	合計最大サイズ (MB)
32GB ~ 64GB	992
64GB ~ 96GB	1920
96GB ~ 128GB	2944
128 GB	4222

メモリは、フィルタ、ルール、コンテナ、接続状態、検出された IP、ドロップフローを含む Distributed Firewall の内部データ構造によって使用されます。これらのパラメータは、次の API 呼び出しを使用して操作できます。

`https://NSX-MGR-IP/api/4.0/firewall/stats/eventthresholds`

Request body:

```
<eventThresholds>
  <cpu>
    <percentValue>100</percentValue>
  </cpu>
  <memory>
    <percentValue>100</percentValue>
  </memory>
  <connectionsPerSecond>
    <value>100000</value>
  </connectionsPerSecond>
</eventThresholds>
```

Edge ファイアウォール

Edge ファイアウォールは、垂直方向のトラフィックを監視して、ファイアウォール、ネットワーク アドレス変換 (NAT)、サイト間 IPSec VPN、SSL VPN などの境界セキュリティ機能を提供します。このソリューションは仮想マシンで利用でき、高可用性モードでデプロイできます。

Edge ファイアウォールのサポートは、分散論理ルーターに制限されます。管理インターフェイスおよびアップリンク インターフェイス、またはそのいずれかのルールのみが機能しますが、内部インターフェイスのルールは機能しません。

注: NSX-V Edge は、攻撃者が SYN パケットのフラッディングによって、ファイアウォールのステートトラッキングテーブルをいっぱいにする SYN フラッド攻撃に対して脆弱性があります。この DOS/DDOS 攻撃によって、ユーザーへのサービスが中断されてしまいます。Edge は、ファイアウォールのステートトラッキングリソースを使用せずに、偽の TCP 接続を検出して終了させるロジックを実装して、SYN フラッド攻撃に対して防御する必要があります。この機能はデフォルトで無効になっています。リスクの高い環境でこの機能を有効にするには、ファイアウォールのグローバル設定の中で、REST API `enableSynFloodProtection` の値を「true」に設定します。

ファイアウォール ルール セクションの操作

セクションを追加して、ファイアウォール ルールを分離できます。たとえば、販売部門とエンジニア部門用のルールを別のセクションに置くことができます。

複数のセクションを L2 ルールおよび L3 ルール用に作成できます。

Cross-vCenter NSX 環境には、1 つのユニバーサル L2 ルール セクションと 1 つのユニバーサル L3 ルール セクションを設けることができます。プライマリ NSX Manager 上ではユニバーサル ルールを管理する必要があり、ユニバーサル ルールを追加するには、その前にユニバーサル セクションを作成する必要があります。

ユニバーサル セクション外部のルールは、ルールが追加されるプライマリまたはセカンダリの NSX Manager のローカル ルールになります。

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 テーブルに新しいセクションを追加して、ルールを整理したり、Cross-vCenter NSX 環境で使用するユニバーサル セクションを作成したりできます。

前提条件

変更を加える適切な NSX Manager を決定します。


- スタンドアロン環境や単一の vCenter NSX の環境では、NSX Manager は 1 つしか存在しないため、NSX Manager を選択する必要はありません。
- ユニバーサル オブジェクトはプライマリ NSX Manager から管理する必要があります。
- NSX Manager に対してローカルなオブジェクトは、NSX Manager から管理する必要があります。
- 拡張リンク モードが有効になっていない Cross-vCenter NSX 環境で設定の変更を行うには、変更する NSX Manager にリンクされた vCenter Server から変更を行う必要があります。
- 拡張リンク モードの Cross-vCenter NSX 環境では、リンクされた任意の vCenter Server から、任意の NSX Manager の設定を変更できます。NSX Manager ドロップダウン メニューから、適切な NSX Manager を選択します。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 複数の NSX Manager が使用可能な場合は、いずれかの NSX Manager を選択します。ユニバーサル セクションを追加するプライマリ NSX Manager を選択する必要があります。
- 3 [全般 (General)] タブが開かれていることを確認し、L3 ルール用のセクションを追加します。[イーサネット (Ethernet)] タブをクリックして、L2 ルール用のセクションを追加します。
- 4 [セクションの追加 (Add Section)] () アイコンをクリックします。
- 5 セクションの名前を入力して、新しいセクションの位置を指定します。セクションの名前は、NSX Manager 内で一意の名前である必要があります。

- 6 (オプション) ユニバーサル セクションを作成するには、[このセクションをユニバーサル同期の対象としてマーク (Mark this section for Universal Synchronization)] を選択します。
- 7 [OK] をクリックして、[変更の発行 (Publish Changes)] をクリックします。

次のステップ

セクションにルールを追加します。セクションの名前を編集するには、そのセクションの [セクションの編集 (Edit section)] () アイコンをクリックします。

ファイアウォール ルール セクションのマージ

セクションをマージして、そのセクション内のルールを統合できます。セクションを Service Composer セクションやデフォルト セクションとマージすることはできない点に注意してください。Cross-vCenter NSX 環境では、セクションをユニバーサル セクションとマージすることはできません。

複雑なファイアウォールの設定をマージして統合すると、メンテナンスがしやすくなり、わかりやすくなります。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 マージするセクションで、[マージ (Merge)] () アイコンをクリックし、このセクションを上のセクションとマージするか、下のセクションとマージするかを指定します。


両セクションのルールがマージされます。新しいセクションには、他のセクションをマージしたセクションの名前が維持されます。
- 3 [変更の発行 (Publish Changes)] をクリックします。

ファイアウォール ルール セクションの削除

ファイアウォール ルール セクションを削除できます。そのセクション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 vSphere Web Client で、[Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 L3 ルールのセクションを削除する場合は、[全般 (General)] タブを開いていることを確認します。L2 ルールのセクションを削除する場合は、[イーサネット (Ethernet)] タブをクリックします。
- 3 削除するセクションの [セクションを削除します (Delete section)] () アイコンをクリックします。
- 4 [OK] をクリックして、[変更の発行 (Publish Changes)] をクリックします。

そのセクションおよびそのセクションのすべてのルールが削除されます。

ファイアウォール ルールの使用

分散ファイアウォール ルールおよび Edge ファイアウォール ルールは、[ファイアウォール] タブで集中管理できます。マルチテナント環境で、プロバイダは統合ファイアウォール ユーザー インターフェイスを使用して高レベルのトラフィック フロー ルールを定義できます。

各トラフィック セッションがファイアウォール 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。ルールは次の順序で表示されます。

- 1 ユーザーがファイアウォール ユーザー インターフェイスで定義したルールの優先順位が最も高くなり、仮想 NIC レベル単位の優先順位で上位から下位に向かって適用されます。
- 2 自動組み込みルール (Edge サービス用に制御トラフィック フローを有効にするルール)。
- 3 ユーザーが NSX Edge インターフェイスで定義したルール。
- 4 Service Composer ルール - ポリシーごとに別々のセクション。ファイアウォール テーブル内のこれらのルールは編集できませんが、セキュリティ ポリシー ファイアウォール ルール セクションの先頭にルールを追加することは可能です。この操作を行う場合は、Service Composer でそれらのルールを再同期する必要があります。詳細については、[章 17 「Service Composer」](#) を参照してください。
- 5 デフォルトの分散ファイアウォール ルール

ファイアウォール ルールが適用されるのは、ファイアウォールを有効にしているクラスタ上のみであることに注意してください。クラスタの準備の詳細については、『NSX インストール ガイド』を参照してください。

デフォルトの分散ファイアウォール ルールの編集

デフォルトのファイアウォール設定は、どのユーザー定義ファイアウォール ルールにも一致しないトラフィックに適用されます。分散ファイアウォールのデフォルト ルールは、統合ファイアウォール ユーザー インターフェイスに表示され、各 NSX Edge のデフォルト ルールが NSX Edge レベルで表示されます。

デフォルトの分散ファイアウォール 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の準備済み全クラスタを通過します。デフォルト ルールは常に、ルール テーブルの下部に表示され、削除や追加はできません。ただし、ルールの操作要素を [許可] から [ブロック] または [却下] に変更したり、ルールにコメントを追加したり、そのルールのトラフィックをログ記録するかどうかを指定したりすることは可能です。

Cross-vCenter NSX 環境では、デフォルト ルールはユニバーサル ルールではありません。デフォルト ルールへの変更は、すべて対応する各 NSX Manager で実施する必要があります。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 デフォルト セクションを展開して、必要な変更を行います。
[操作 (Action)] および [ログ (Log)] の編集や、デフォルト ルールへのコメントの追加のみ実行できます。

ファイアウォール ルールの追加

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

次の vCenter オブジェクトをファイアウォール ルールのソースまたはターゲットとして指定できます。

表 10-2. ファイアウォール ルールでサポートされるオブジェクト

ソースまたはターゲット	適用先
<ul style="list-style-type: none"> ■ クラスタ ■ データセンター ■ 分散ポート グループ ■ IP セット ■ レガシー ポート グループ ■ 論理スイッチ ■ リソース プール ■ Security Group ■ vApp ■ 仮想マシン ■ vNIC ■ IP アドレス (IPv4 または IPv6) 	<ul style="list-style-type: none"> ■ Distributed Firewall がインストールされているすべてのクラスタ (つまり、ネットワーク仮想化の準備ができていないすべてのクラスタ) ■ 準備ができていないクラスタにインストールされているすべての Edge Gateway ■ クラスタ ■ データセンター ■ 分散ポート グループ ■ Edge ■ レガシー ポート グループ ■ 論理スイッチ ■ Security Group ■ 仮想マシン ■ vNIC

前提条件

NSX 分散ファイアウォールの状態が後方互換性モードになっていないことを確認してください。現在の状態を確認するには、REST API 呼び出し GET `https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state` を使用します。現在の状態が後方互換性モードになっている場合、REST API 呼び出し PUT `https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state` を使用して状態を前方互換性モードに変更できます。分散ファイアウォールが後方互換性モードになっているときに、分散ファイアウォール ルールを発行しないでください。


ユニバーサル ファイアウォール ルールを追加する場合は、[「ユニバーサル ファイアウォール ルールの追加」](#) を参照してください。

ID ベースのファイアウォール ルールを追加する場合は、次のことを確認します。


- 1 つ以上のドメインが NSX Manager に登録されている。NSX Manager は、グループ、ユーザー情報、およびこれらの間の関係を登録先の各ドメインから取得します。[「NSX Manager への Windows ドメインの登録」](#) を参照してください。
- ルールのソースまたはターゲットとして使用できる、Active Directory オブジェクトに基づいた Security Group が作成されている。[「Security Group の作成」](#) を参照してください。

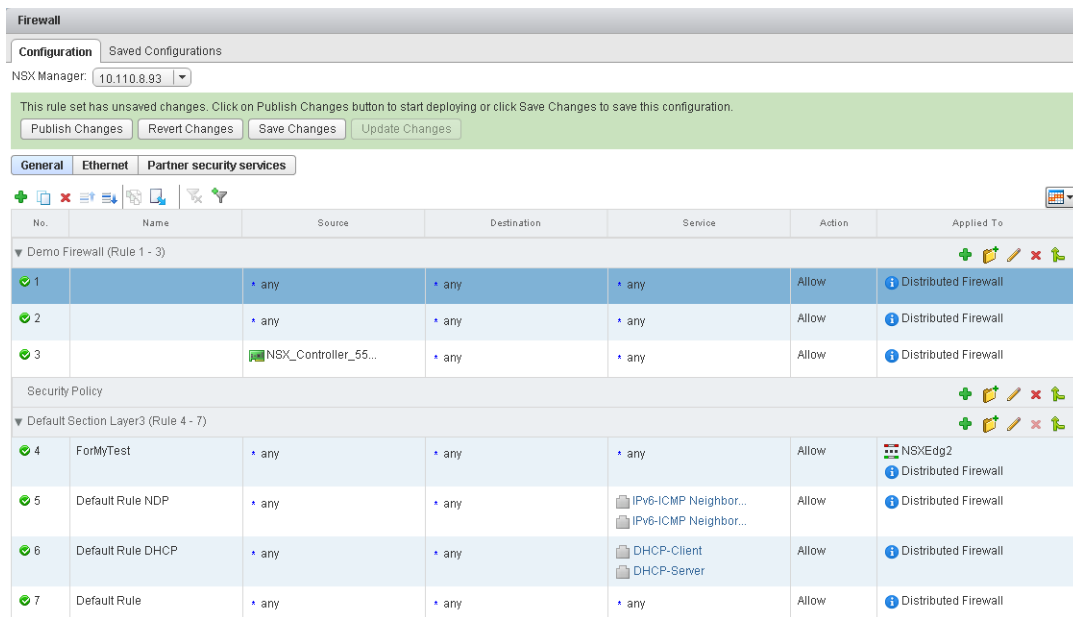
VMware vCenter オブジェクトに基づいてルールを追加する場合、VMware Tools が仮想マシンにインストールされていることを確認します。NSX インストール ガイド を参照してください。

手順


- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 [全般 (General)] タブが開かれていることを確認し、L3 ルールを追加します。[イーサネット (Ethernet)] タブをクリックし、L2 ルールを追加します。
- 3 ルールを追加するセクションで、[ルールの追加 (Add rule)] () アイコンをクリックします。
- 4 [変更の発行 (Publish Changes)] をクリックします。

セクションの一番上に新しい許可ルールが追加されます。セクションにシステム定義のルールしかない場合は、新しいルールはデフォルトのルールの上に追加されます。

セクション内の特定の場所にルールを追加する場合は、ルールを選択します。[番号]列で、  をクリックし、[上に追加 (Add Above)] または [下に追加 (Add Below)] を選択します。



No.	Name	Source	Destination	Service	Action	Applied To
▼ Demo Firewall (Rule 1 - 3)						
1		* any	* any	* any	Allow	Distributed Firewall
2		* any	* any	* any	Allow	Distributed Firewall
3		NSX_Controller_55...	* any	* any	Allow	Distributed Firewall
Security Policy						
▼ Default Section Layer3 (Rule 4 - 7)						
4	ForMyTest	* any	* any	* any	Allow	NSXEdg2 Distributed Firewall
5	Default Rule NDP	* any	* any	IPv6-ICMP Neighbor...	Allow	Distributed Firewall
6	Default Rule DHCP	* any	* any	DHCP-Client	Allow	Distributed Firewall
7	Default Rule	* any	* any	DHCP-Server	Allow	Distributed Firewall

- 5 新しいルールの [名前 (Name)] セルをポイントし、  をクリックします。
- 6 新しいルールの名前を入力します。




- 7 新しいルールの [ソース (Source)] セルをポイントします。次の表で説明されている追加のアイコンが表示されます。

オプション	説明
 をクリック	<p>ソースを IP アドレスとして指定するには：</p> <ol style="list-style-type: none"> IP アドレス形式を選択します。 <p>ファイアウォールでは、IPv4 形式と IPv6 形式の両方がサポートされています。</p> <ol style="list-style-type: none"> IP アドレスを入力します。 <p>複数の IP 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。</p>
 をクリックします。	<p>ソースを特定の IP アドレス以外のオブジェクトとして指定するには：</p> <ol style="list-style-type: none"> [表示 (View)] で、通信の発生元のコンテナを選択します。 <p>選択したコンテナのオブジェクトが表示されます。</p> <ol style="list-style-type: none"> 1 つ以上のオブジェクトを選択し、 をクリックします。 <p>新しい Security Group または IPSet を作成できます。新しいオブジェクトを作成すると、デフォルトでソースの列に追加されます。新しい Security Group または IPSet の作成については、章 22 「ネットワークおよびセキュリティ オブジェクト」 を参照してください。</p> <ol style="list-style-type: none"> ソースをルールから除外するには、[詳細オプション (Advanced options)] をクリックします。 [ソースの無効化 (Negate Source)] を選択し、このソースをルールから除外します。 <p>[ソースの無効化 (Negate Source)] を選択すると、前の手順で指定したソースを除くすべてのソースから受信するトラフィックにルールが適用されます。</p> <p>[ソースの無効化 (Negate Source)] を選択しないと、前の手順で指定したソースから受信するトラフィックにルールが適用されます。</p> <ol style="list-style-type: none"> [OK] をクリックします。


- 8 新しいルールの [ターゲット (Destination)] セルをポイントします。次の表で説明されている追加のアイコンが表示されます。

オプション	説明
 をクリック	<p>ターゲットを IP アドレスとして指定するには：</p> <ol style="list-style-type: none"> IP アドレス形式を選択します。 <p>ファイアウォールでは、IPv4 形式と IPv6 形式の両方がサポートされています。</p> <ol style="list-style-type: none"> IP アドレスを入力します。 <p>複数の IP 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。</p>
 をクリックします。	<p>ターゲットを特定の IP アドレス以外のオブジェクトとして指定するには：</p> <ol style="list-style-type: none"> [表示 (View)] で、通信のターゲットのコンテナを選択します。 <p>選択したコンテナのオブジェクトが表示されます。</p> <ol style="list-style-type: none"> 1 つ以上のオブジェクトを選択し、 をクリックします。 <p>新しい Security Group または IPSet を作成できます。新しいオブジェクトを作成すると、デフォルトで [ターゲット] 列に追加されます。新しい Security Group または IPSet の作成については、章 22 「ネットワークおよびセキュリティ オブジェクト」 を参照してください。</p> <ol style="list-style-type: none"> ターゲット ポートを除外するには、[詳細オプション (Advanced options)] をクリックします。 [ターゲットの無効化 (Negate Destination)] を選択し、このターゲットをルールから除外します。 <p>[ターゲットの無効化 (Negate Destination)] を選択すると、前の手順で指定したターゲットを除くすべてのターゲットに送信するトラフィックにルールが適用されます。</p> <p>[ターゲットの無効化 (Negate Destination)] を選択しないと、前の手順で指定したターゲットに送信するトラフィックにルールが適用されます。</p> <ol style="list-style-type: none"> [OK] をクリックします。

- 9 新しいルールの [サービス (Service)] セルをポイントします。次の表で説明されている追加のアイコンが表示されます。

オプション	説明
 をクリック	<p>サービスをポートとプロトコルの組み合わせで指定するには：</p> <p>a サービス プロトコルを選択します。</p> <p>Distributed Firewall では、FTP、CIFS、ORACLE TNS、MS-RPC、SUN-RPC のプロトコルの ALG（アプリケーション レベル ゲートウェイ）がサポートされています。</p> <p>Edge では、FTP の ALG のみがサポートされています。</p> <p>b ポート番号を入力し、[OK] をクリックします。</p>
 をクリックします。	<p>事前定義されたサービス/サービス グループを選択するか、新しいサービス/サービス グループを定義するには：</p> <p>a</p> <p>1 つ以上のオブジェクトを選択し、 をクリックします。</p> <p>新しいサービスまたはサービス グループを作成できます。新しいオブジェクトを作成すると、デフォルトで [選択したオブジェクト] 列に追加されます。</p> <p>b [OK] をクリックします。</p>

ACK または SYN フラッドからネットワークを保護するために、デフォルト ルールでサービスを TCP-all_ports または UDP-all_ports に設定し、アクションをブロックに設定できます。デフォルト ルールの変更については、[「デフォルトの分散ファイアウォール ルールの編集」](#)を参照してください。

- 10 新しいルール of [アクション (Action)] セルをポイントし、 をクリックします。次の表の説明に従って適切な選択を行い、[OK] をクリックします。

アクション	結果
許可	指定したソース、ターゲット、サービスの送受信トラフィックを許可します。
ブロック	指定したソース、ターゲット、サービスの送受信トラフィックをブロックします。
拒否	<p>受け入れられないパケットに対する拒否メッセージを送信します。</p> <p>TCP 接続では、RST パケットが送信されます。</p> <p>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。</p>
ログに記録	このルールと一致するすべてのセッションのログを記録します。ログを有効にするとパフォーマンスに影響が出る場合があります。
ログに記録しない	セッションのログを記録しません。

- 11 [適用先 (Applied To)] で、このルールが適用可能なスコープを定義します。次の表の説明に従って適切な選択を行い、[OK] をクリックします。

ルールの適用先	操作
環境内の準備ができていないすべてのクラスター	[Distributed Firewall] がインストールされているすべてのクラスターにこのルールを適用します (Apply this rule on all clusters on which Distributed Firewall is enabled)] を選択します。[OK] をクリックすると、このルールの [適用先] 列に [Distributed Firewall] が表示されます。
環境内のすべての NSX Edge Gateway	[すべての Edge ゲートウェイにこのルールを適用します (Apply this rule on all Edge gateways)] を選択します。[OK] をクリックすると、このルールの [適用先] 列に [すべての Edge (All Edges)] が表示されます。 上記の両方のオプションが選択されている場合、[適用先] 列には [任意 (Any)] が表示されます。
1 つ以上のクラスター、データセンター、分散仮想ポート グループ、NSX Edge、ネットワーク、仮想マシン、vNIC、または論理スイッチ	1 [コンテナタイプ (Container type)] で、適切なオブジェクトを選択します。 2 [使用可能] リストで、1 つ以上のオブジェクトを選択し、  をクリックします。




ルールのソースおよびターゲット フィールドに仮想マシンまたは vNIC が含まれる場合、ルールを正常に動作させるには [適用先 (Applied To)] にソースおよびターゲットの両方の仮想マシンまたは vNIC を追加する必要があります。


- 12 [変更の発行 (Publish Changes)] をクリックします。

数秒後、発行操作に成功したかどうかを示すメッセージが表示されます。失敗した場合、ルールが適用されなかったホストがリストされます。失敗した発行の詳細を確認するには、[NSX Manager (NSX Managers)] - [<NSX_Manager_IP_Address>] - [監視 (Monitor)] - [システム イベント (System Events)] の順に移動します。

[変更の発行 (Publish Changes)] をクリックすると、ファイアウォール設定が自動的に保存されます。以前の設定に戻す方法については、「[ファイアウォール設定の読み込み](#)」を参照してください。

次のステップ

-  をクリックしてルールを無効にするか、 をクリックしてルールを有効にします。
- ルール テーブル内の追加の列を表示するには、 をクリックし、適切な列を選択します。

カラム名	表示される情報
ルール ID	各ルールに対してシステムが生成した一意の ID
ログに記録	このルールのトラフィックがログ記録されるかどうか
統計	 をクリックし、このルールに関連するトラフィック（トラフィック パケットおよびサイズ）を表示
コメント	ルールのコメント


- 検索フィールドにテキストを入力し、ルールを検索します。
- ファイアウォール テーブル内で、ルールの位置を上下に移動します。

- [セクションをマージします (Merge section)] アイコンをクリックし、[上のセクションとマージ (Merge with above section)] または [下のセクションとマージ (Merge with below section)] を選択してセクションをマージします。

ファイアウォール設定の読み込み

自動保存またはインポートされたファイアウォール設定を読み込みめます。現在の設定に Service Composer によって管理されるルールが含まれる場合、そのルールはインポート後にオーバーライドされます。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 L3 ファイアウォール設定を読み込むには、[全般 (General)] タブが開かれていることを確認します。L2 ファイアウォール設定を読み込むには、[イーサネット (Ethernet)] タブをクリックします。
- 3 [設定のロード (Load configuration)] () アイコンをクリックします。
- 4 読み込む設定を選択して、[OK] をクリックします。

現在の設定が選択された設定に置き換わります。

次のステップ

設定に含まれる Service Composer のルールが、読み込まれた設定によってオーバーライドされた場合は、Service Composer の [セキュリティ ポリシー] タブで、[アクション (Actions)] - [ファイアウォールのルールの同期 (Synchronize Firewall Rules)] をクリックします。

ユニバーサル ファイアウォール ルールの追加

Cross-vCenter NSX 環境の場合、ユニバーサル ルールは、プライマリ NSX Manager のユニバーサル ルール セクションで定義された Distributed Firewall ルールを参照します。これらのルールは、環境内のすべてのセカンダリ NSX Manager でレプリケートされるため、vCenter の境界を越えて一貫したファイアウォール ポリシーを維持できます。複数の vCenter Server 間の vMotion では、Edge ファイアウォール ルールはサポートされていません。

プライマリ NSX Manager には、ユニバーサル L2 ルール用のユニバーサル セクションとユニバーサル L3 ルール用のユニバーサル セクションをそれぞれ 1 つずつ含めることができます。セカンダリ NSX Manager では、ユニバーサル セクションやユニバーサル ルールを表示できますが、編集することはできません。ローカル セクションに対するユニバーサル セクションの配置は、ルールの優先順位に影響しません。

表 10-3. ユニバーサル ファイアウォール ルールでサポートされるオブジェクト

ソースとターゲット	適用先	サービス
<ul style="list-style-type: none"> ■ ユニバーサル MAC セット ■ ユニバーサル IP セット ■ IP セット、MAC セット、またはユニバーサル セキュリティ グループを含めることができるユニバーサル セキュリティ グループ ■ ユニバーサル論理スイッチ 	<ul style="list-style-type: none"> ■ ユニバーサル論理スイッチ ■ Distributed Firewall - Distributed Firewall がインストールされているすべてのクラスタにルールを適用 	<ul style="list-style-type: none"> ■ 事前に作成されたユニバーサル サービスおよびサービス グループ ■ ユーザーが作成したユニバーサル サービスおよびサービス グループ

ユニバーサル ルールでは、他の vCenter オブジェクトはサポートされていません。

前提条件

ユニバーサル ルールを作成する前に、ユニバーサル ルール セクションを作成する必要があります。[「ファイアウォール ルール セクションの追加」](#)を参照してください。

手順




- 1 vSphere Web Client で、[Networking and Security] - [ファイアウォール] の順に移動します。
- 2 NSX Manager で、プライマリ NSX Manager が選択されていることを確認します。
プライマリ NSX Manager でのみユニバーサル ルールを追加できます。
- 3 [全般] タブが開かれていることを確認し、L3 ユニバーサル ルールを追加します。[イーサネット] タブをクリックし、L2 ユニバーサル ルールを追加します。
- 4 ユニバーサル セクションで、[ルールの追加] () アイコンをクリックし、[変更の発行] をクリックします。
ユニバーサル セクションの一番上に新しい許可ルールが追加されます。
- 5 新しいルールの [名前] セルをポイントし、 をクリックします。ルールの名前を入力します。
- 6 新しいルールの [ソース] セルをポイントします。次の表で説明されている追加のアイコンが表示されます。

オプション	説明
 をクリック	<p>ソースを IP アドレスとして指定するには：</p> <ol style="list-style-type: none"> a IP アドレス形式を選択します。 ファイアウォールでは、IPv4 形式と IPv6 形式の両方がサポートされています。 b IP アドレスを入力します。
 をクリックします。	<p>ソースとしてユニバーサル IPSet、MACSet、またはセキュリティ グループを指定するには：</p> <ol style="list-style-type: none"> a [オブジェクト タイプ] で、通信の発生元のコンテナを選択します。 選択したコンテナのオブジェクトが表示されます。 b 1 つ以上のオブジェクトを選択し、 をクリックします。 新しいセキュリティ グループまたは IPSet を作成できます。新しいオブジェクトを作成すると、デフォルトでソースの列に追加されます。新しいセキュリティ グループまたは IPSet の作成については、章 22 「ネットワークおよびセキュリティ オブジェクト」を参照してください。 c ソースをルールから除外するには、[詳細オプション] をクリックします。 d [ソースの無効化] を選択し、このソースをルールから除外します。 [ソースの無効化] を選択すると、前の手順で指定したソースを除くすべてのソースから受信するトラフィックにルールが適用されます。 [ソースの無効化] を選択しないと、前の手順で指定したソースから受信するトラフィックにルールが適用されます。 e [OK] をクリックします。

7 新しいルールの [ターゲット] セルをポイントします。次の表で説明されている追加のアイコンが表示されます。

オプション	説明
 をクリック	<p>ターゲットを IP アドレスとして指定するには：</p> <ol style="list-style-type: none"> IP アドレス形式を選択します。 <p>ファイアウォールでは、IPv4 形式と IPv6 形式の両方がサポートされています。</p> <ol style="list-style-type: none"> IP アドレスを入力します。
 をクリックします。	<p>ターゲットとしてユニバーサル IPSet、MACSet、またはセキュリティ グループを指定するには：</p> <ol style="list-style-type: none"> [オブジェクト タイプ] で、通信のターゲットのコンテナを選択します。 <p>選択したコンテナのオブジェクトが表示されます。</p> <ol style="list-style-type: none"> 1 つ以上のオブジェクトを選択し、 をクリックします。 <p>新しいセキュリティ グループまたは IPSet を作成できます。新しいオブジェクトを作成すると、デフォルトで [ターゲット] 列に追加されます。新しいセキュリティ グループまたは IPSet の作成については、章 22 「ネットワークおよびセキュリティ オブジェクト」 を参照してください。</p> <ol style="list-style-type: none"> ターゲットをルールから除外するには、[詳細オプション] をクリックします。 [ターゲットの無効化] を選択し、このターゲットをルールから除外します。 <p>[ターゲットの無効化] を選択すると、前の手順で指定したターゲットを除くすべてのターゲットに送信するトラフィックにルールが適用されます。</p> <p>[ターゲットの無効化] を選択しないと、前の手順で指定したターゲットに送信するトラフィックにルールが適用されます。</p> <ol style="list-style-type: none"> [OK] をクリックします。

8 新しいルールの [サービス] セルをポイントします。次の表で説明されている追加のアイコンが表示されます。

オプション	説明
 をクリック	<p>サービスをポートとプロトコルの組み合わせで指定するには：</p> <ol style="list-style-type: none"> サービス プロトコルを選択します。 <p>Distributed Firewall では、FTP、CIFS、ORACLE TNS、MS-RPC、SUN-RPC のプロトコルの ALG（アプリケーション レベル ゲートウェイ）がサポートされています。</p> <ol style="list-style-type: none"> ポート番号を入力し、[OK] をクリックします。
 をクリックします。	<p>事前定義されたユニバーサル サービス/ユニバーサル サービス グループを選択するか、新しいユニバーサル サービス/ユニバーサル サービス グループを定義するには：</p> <ol style="list-style-type: none"> 1 つ以上のオブジェクトを選択し、 をクリックします。 <p>新しいサービスまたはサービス グループを作成できます。新しいオブジェクトを作成すると、デフォルトで [選択したオブジェクト] 列に追加されます。</p> <ol style="list-style-type: none"> [OK] をクリックします。


ACK または SYN フラッドからネットワークを保護するために、デフォルト ルールでサービスを TCP-all_ports または UDP-all_ports に設定し、アクションをブロックに設定できます。デフォルト ルールの変更については、[「デフォルトの分散ファイアウォール ルールの編集」](#) を参照してください。

- 9 新しいルールの [アクション] セルをポイントし、 をクリックします。次の表の説明に従って適切な選択を行い、[OK] をクリックします。

アクション	結果
許可	指定したソース、ターゲット、サービスの送受信トラフィックを許可します。
ブロック	指定したソース、ターゲット、サービスの送受信トラフィックをブロックします。
拒否	受け入れられないパケットに対する拒否メッセージを送信します。 TCP 接続では、RST パケットが送信されます。 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。
ログに記録	このルールと一致するすべてのセッションのログを記録します。ログを有効にするとパフォーマンスに影響が出る場合があります。
ログに記録しない	セッションのログを記録しません。

- 10 [適用先] セルで、デフォルト設定の [Distributed Firewall] を受け入れて、Distributed Firewall が有効になっているすべてのクラスタにルールを適用するか、編集アイコン をクリックして、ルールを適用するユニバーサル論理スイッチを選択します。

- 11 [変更の発行] をクリックします。



ユニバーサル ルールがすべてのセカンダリ NSX Manager でレプリケートされます。ルール ID はすべての NSX インスタンスで同じままです。ルール ID を表示するには、 をクリックし、ルール ID を選択します。


ユニバーサル ルールは、プライマリ NSX Manager でのみ編集でき、セカンダリ NSX Manager では読み取り専用になります。


ユニバーサル セクション レイヤー 3 とデフォルトのセクション レイヤー 3 のあるファイアウォール ルール：

No.	Name	Source	Destination	Service	Action	Applied To
▼ Universal Section Layer3 (Rule 1 - 2)						
1	Web Micro-Segmentation	Web USG	Web USG	any	Block	Distributed Firewall
2	Allow Web Access	any	Web USG	HTTPS SSH	Allow	Distributed Firewall
▼ Default Section Layer3 (Rule 3 - 7)						
3	Web Micro-Segmentation	Web SG	Web SG	any	Allow	Distributed Firewall
4	Allow Web Access	any	Web SG	HTTPS SSH	Allow	Distributed Firewall
5	Default Rule NDP	any	any	IPv6-ICMP Neighbor ... IPv6-ICMP Neighbor ...	Allow	Distributed Firewall
6	Default Rule DHCP	any	any	DHCP-Client DHCP-Server	Allow	Distributed Firewall
7	Default Rule	any	any	any	Block	Distributed Firewall

次のステップ

- [番号] 列で  をクリックしてルールを無効にするか、 をクリックしてルールを有効にします。

- ルール テーブル内の追加の列を表示するには、 をクリックし、適切な列を選択します。

カラム名	表示される情報
ルール ID	各ルールに対してシステムが生成した一意の ID
ログに記録	このルールのトラフィックがログ記録されるかどうか
統計	 をクリックし、このルールに関連するトラフィック（トラフィック パケットおよびサイズ）を表示
コメント	ルールのコメント

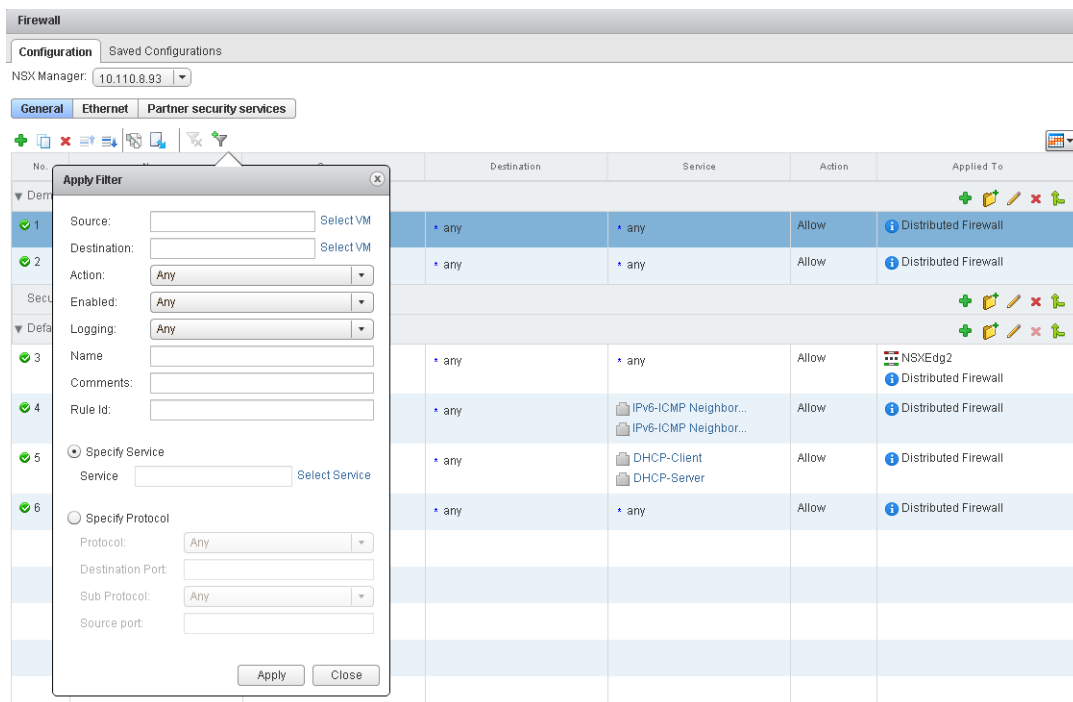
- 検索フィールドにテキストを入力し、ルールを検索します。
- ファイアウォール テーブル内で、ルールの位置を上下に移動します。

ファイアウォール ルールのフィルタ

さまざまな基準を使用してルールセットをフィルタできます。これにより、ルールの変更が簡略化されます。送信元仮想マシン、宛先仮想マシン、送信元 IP アドレス、宛先 IP アドレス、ルール アクション、ログ、ルール名、コメント、およびルール ID を基準にして、ルールをフィルタできます。


手順

- 1 [ファイアウォール] タブで、[フィルタの適用 (Apply Filter)] () アイコンをクリックします。



- 2 該当するフィルタ基準を入力または選択します。
- 3 [適用 (Apply)] をクリックします。
指定したフィルタ基準に一致するルールが表示されます。

次のステップ

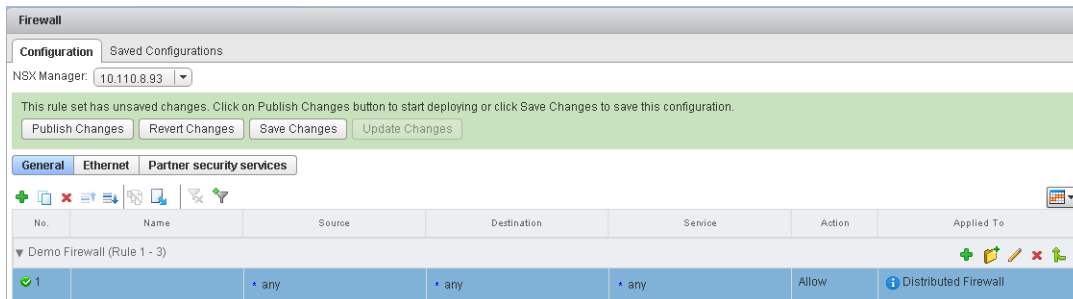
再びすべてのルールを表示するには、[適用したフィルタの削除 (Remove applied filter)] () アイコンをクリックします。

ルールの追加とその後の発行

ルールを追加し、そのルールを発行しないまま設定を保存できます。保存した設定は後でロードして発行できます。

手順

- 1 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 ルールの追加」](#)を参照してください。
- 2 [変更の保存] をクリックします。



- 3 の名前と説明を入力し、[OK] をクリックします。
- 4 [設定の保持] をクリックして、この変更内容を保持します。
NSX では、最大で 100 個のを保存できます。この制限を超えると、保存される設定 ([設定の保持] とマークされた設定) は保持されますが、保持されなかった古い設定は、容量を空けるために削除されます。
- 5 次のいずれかを実行します。
 - [変更を元に戻す] をクリックし、ルールを追加する前の設定に戻します。追加したばかりのルールを発行する場合は、[設定のロード] アイコンをクリックし、ステップ 3 で保存したルールを選択し、[OK] をクリックします。
 - [変更の更新] をクリックし、ルールの追加を続行します。

ファイアウォール ルールの順序の変更

ファイアウォール ルールは、ルール テーブルに記載されている順序で適用されます。

ルールは次の順序で表示 (および適用) されます。



- 1 ユーザー定義の事前ルールに最も高い優先順位が与えられます。このルールは、各仮想 NIC レベルの優先順位に沿って、上から順に適用されます。
- 2 自動配置されたルール。
- 3 NSX Edge レベルで定義されたローカル ルール。

- 4 Service Composer ルール - ポリシーごとに別々のセクション。ファイアウォール テーブル内のこれらのルールは編集できませんが、セキュリティ ポリシー ファイアウォール ルール セクションの先頭にルールを追加することは可能です。この操作を行う場合は、Service Composer でそれらのルールを再同期する必要があります。詳細については、[章 17 「Service Composer」](#) を参照してください。

5 デフォルトの分散ファイアウォール ルール

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 [ファイアウォール (Firewall)] タブで、移動するルールを選択します。
- 2 [ルールを上へ移動 (Move rule up)] () または [ルールを下へ移動 (Move rule down)] () アイコンをクリックします。
- 3 [変更の発行 (Publish Changes)] をクリックします。

ファイアウォール ルールの削除

作成済みのファイアウォール ルールを削除できます。デフォルト ルールまたは Service Composer で管理されるルールは削除できません。

手順

- 1 [ファイアウォール (Firewall)] タブで、ルールを 1 つ選択します。
- 2 ファイアウォール テーブルの上にある [選択したルールの削除 (Delete selected rule)] () アイコンをクリックします。
- 3 [変更の発行 (Publish Changes)] をクリックします。

ファイアウォールによる保護からの仮想マシンの除外

NSX Distributed Firewall 保護から一連の仮想マシンを除外することができます。

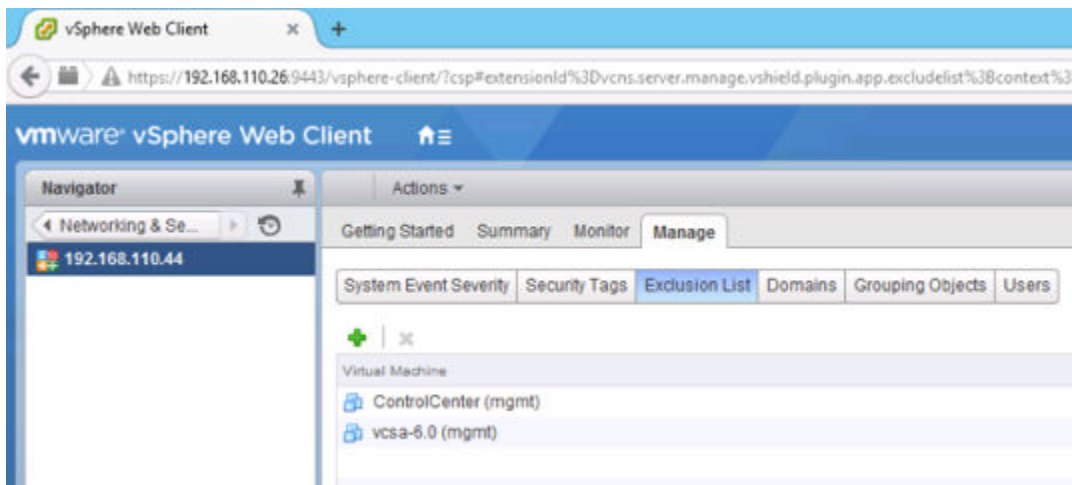
NSX Manager、NSX コントローラ、および NSX Edge 仮想マシンは、NSX Distributed Firewall 保護から自動的に除外されます。また、除外リストに以下のサービス仮想マシンを含めて、トラフィックの自由なフローを可能にすることをお勧めします。

- vCenter Server。vCenter Server は Firewall によって保護されているクラスタに移動できますが、これを前もって除外リストに追加しておき、接続の問題を防止する必要があります。
- パートナーのサービス仮想マシン。
- 無差別モードを必要とする仮想マシン。この仮想マシンを NSX Distributed Firewall で保護した場合、仮想マシンのパフォーマンスに悪影響が及ぶ可能性があります。
- Windows ベースの vCenter Server で使用する SQL Server。
- vCenter Web サーバ (個別に実行している場合)。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] をクリックします。
- 2 [ネットワークとセキュリティのインベントリ (Networking & Security Inventory)] で、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で、NSX Manager をクリックします。
- 4 [管理 (Manage)] タブをクリックして、[除外リスト (Exclusion List)] タブをクリックします。
- 5 [追加 (Add)] (+) アイコンをクリックします。
- 6 除外する仮想マシンの名前を入力し、[追加 (Add)] をクリックします。

次はその例です。



- 7 [OK] をクリックします。

1 台の仮想マシンに複数の vNIC がある場合は、そのすべてが保護から除外されます。仮想マシンを除外リストに追加した後に vNIC を仮想マシンに追加した場合、新しく追加した vNIC に Firewall が自動的にデプロイされます。この vNIC を Firewall 保護から除外するには、仮想マシンを除外リストから削除した後、除外リストに再度追加する必要があります。代替の回避策は仮想マシンの電源を入れ直す（パワーオフした後にパワーオンする）ことです。問題が少ないのは最初のオプションです。

仮想マシンの IP 検出

VMware Tools は仮想マシンで実行され、いくつかのサービスを提供します。Distributed Firewall に欠かせないサービスの 1 つは、仮想マシンおよびその vNIC と IP アドレスとの関連付けです。NSX 6.2 より前のバージョンでは、VMware Tools が仮想マシンにインストールされていないと、その IP アドレスを検出できませんでした。NSX 6.2 では、DHCP スヌーピングか ARP スヌーピングのいずれか、またはその両方で仮想マシンの IP アドレスを検出するようにクラスタを設定できます。これにより、NSX は VMware Tools が仮想マシンにインストールされていない場合でも IP アドレスを検出できます。VMware Tools がインストールされている場合、DHCP および ARP のスヌーピングと組み合わせて使用できます。

VMware では、VMware Tools を環境内のすべての仮想マシンにインストールすることをお勧めします。vCenter に仮想マシンの IP アドレスを提供するだけでなく、他にも多くの機能があります。

- 仮想マシンとホストまたはクライアント デスクトップの間でのコピー アンド ペーストを可能にする
- ホスト オペレーティング システムと時刻を同期する
- vCenter からの仮想マシンのシャットダウンまたは再起動を可能にする
- 仮想マシンからネットワーク、ディスク、メモリの使用量を収集し、ホストに送信する
- ハートビートを送信して収集することで仮想マシンの可用性を判断する

VMware Tools がインストールされていない仮想マシンでは、仮想マシンのクラスタで ARP および DHCP のスヌーピングが有効になっている場合、NSX は ARP または DHCP のスヌーピングを使用して IP アドレスを検出します。

IP アドレス検出タイプの変更

仮想マシンの IP アドレスは、仮想マシンにインストールされる VMware Tools によって、またはホスト クラスタで有効にされる DHCP スヌーピングおよび ARP スヌーピングによって検出できます。これらの IP 検出方法は、同じ NSX インストール環境で同時に使用できます。

手順

- 1 vSphere Web Client で、[Networking and Security] - [インストール手順] - [ホストの準備] の順に移動します。
- 2 変更するクラスタをクリックし、[アクション (⚙️)] - [IP アドレス検出タイプの変更] をクリックします。
- 3 目的の検出タイプを選択して [OK] をクリックします。

次のステップ

SpoofGuard を設定します。

デフォルトのファイアウォール ルールを設定します。

ファイアウォール CPU イベントおよびメモリしきい値イベントの表示

クラスタがネットワークの仮想化用に準備されるときに、ファイアウォール モジュールがそのクラスタのすべてのホスト上にインストールされます。このモジュールが割り当てる 3 つのヒープは、モジュール パラメータ用モジュール ヒープ、ルール、コンテナ、フィルタ用ルール ヒープ、およびトラフィック フロー用状態ヒープです。ヒープ サイズ割り当ては、有効なホスト物理メモリによって決まります。ルール数、コンテナ セット数、接続数に応じて、ヒープ サイズは時間の経過とともに拡大または縮小される可能性があります。ハイパーバイザー上で実行されているファイアウォール モジュールは、パケット処理のためにホスト CPU も使用します。

指定した任意の時間のホスト リソース使用率を知ること、サーバ使用率およびネットワーク設計をよりよく整理できます。

デフォルトの CPU しきい値は 100 であり、メモリしきい値は 100 です。デフォルトのしきい値は、REST API 呼び出しを使用して変更できます。メモリおよび CPU 使用率がしきい値に達すると、ファイアウォール モジュールでシステム イベントが生成されます。デフォルトのしきい値の設定の詳細については、『NSX API ガイド』の「Memory and CPU Thresholds」を参照してください。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 2 [名前 (Name)] 列で、該当する NSX Manager の IP アドレスをクリックします。
- 3 [監視 (Monitor)] タブをクリックして、[システム イベント (System Events)] をクリックします。

ファイアウォール ログ

ファイアウォールは、監査ログ、ルール メッセージ ログ、システム イベント ログなどのログ ファイルを生成して保存します。

ファイアウォールは 3 種類のログを生成します。

- ルール メッセージ ログには、各ルールで許可されるトラフィックや拒否されるトラフィックなどの、すべてのアクセスに関する決定事項が含まれています（そのルールで、ログが有効になっている場合）。これらのログは、各ホストの `/var/log/dfwpktlogs.log` に保存されます。

次の例では、

- 1002 は分散ファイアウォールのルール ID です。
- domain-c7 は vCenter 管理対象オブジェクト ブラウザ (MOB) のクラスタ ID です。
- 192.168.110.10/138 はソース IP アドレスです。
- 192.168.110.255/138 はターゲット IP アドレスです。

```
~ # more /var/log/dfwpktlogs.log
```

```
2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138->192.168.110.255/138
```

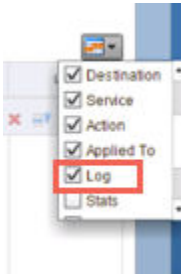
次の例は、192.168.110.10 を 172.16.10.12 に ping した結果を示しています。

```
~ # tail -f /var/log/dfwpktlogs.log | grep 192.168.110.10
```

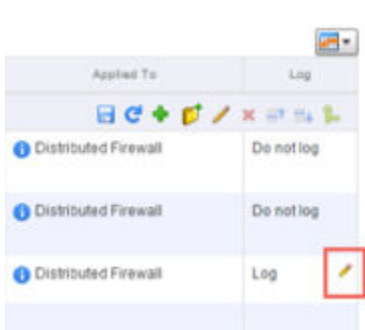
```
2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
```

vSphere Web Client 6.0 でルール メッセージ ロギングを有効にするには、次の手順を実行します (vSphere 5.5 ではユーザー インターフェイスが少し異なる可能性があります、手順は同じです)。

- a [Networking and Security] > [ファイアウォール (Firewall)] ページで [ログ (Log)] 列を有効にします。

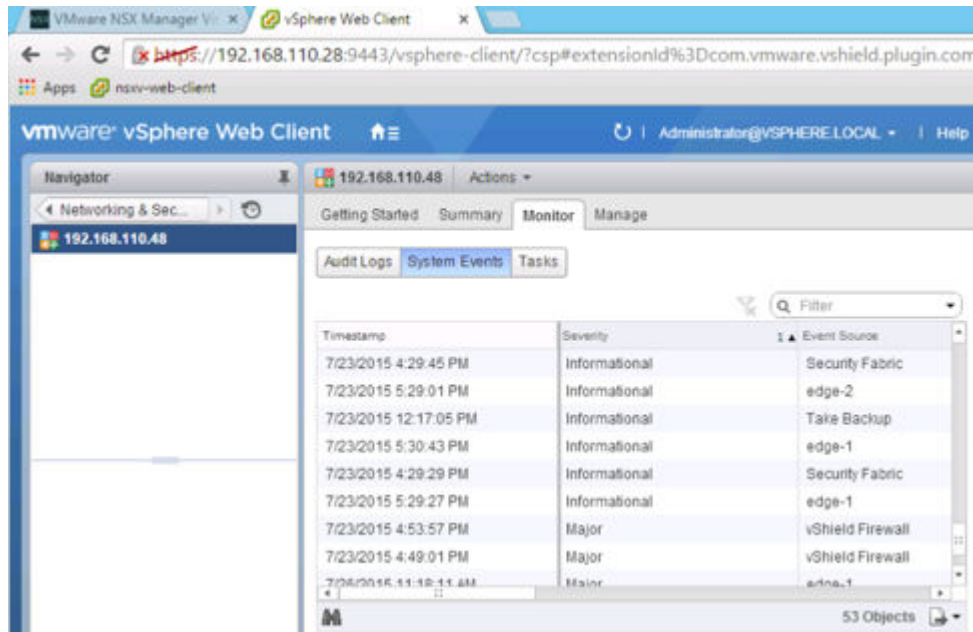


- b [ログ] テーブル セルにマウスを合わせて鉛筆アイコンをクリックし、ルールのロギングを有効にします。



- 監査ログには、管理ログと分散ファイアウォールの設定の変更が含まれています。これらのログは、`/home/secureall/secureall/logs/vsm.log` に保存されます。
- システム イベント ログには、適用された分散ファイアウォールの設定のほか、作成、削除、または失敗したフィルタ、セキュリティ グループに追加された仮想マシンなどの情報が含まれます。これらのログは、`/home/secureall/secureall/logs/vsm.log` に保存されます。

ユーザー インターフェイスで監査およびシステム イベント ログを表示するには、[Networking and Security] > [インストール手順 (Installation)] > [管理 (Management)] の順に移動して NSX Manager の IP アドレスをダブルクリックします。次に [監視 (Monitor)] タブを選択します。



詳細については、[章 23 「操作と管理」](#) を参照してください。

NSX Edge ファイアウォール ルールの使用

NSX Edge に移動し、それに適用されるファイアウォール ルールを確認できます。

分散論理ルーターに適用されるファイアウォール ルールは、分散論理ルーター制御仮想マシンで送受信される制御プレーントラフィックのみを保護します。これらのルールによって、何らかのデータ プレーン保護が強制的に適用されることはありません。データ プレーントラフィックを保護するには、論理ファイアウォール ルールを作成して水平方向を保護するか、または NSX Edge Services Gateway レベルのルールを作成して垂直方向を保護します。

この NSX Edge に適用できる Firewall ユーザー インターフェイス上で作成されたルールは、読み取り専用モードで表示されます。ルールは次の順序で表示および適用されます。


- 1 ユーザーがファイアウォール ユーザー インターフェイスで定義したルール（読み取り専用）。
- 2 自動組み込みルール（Edge サービス用に制御トラフィック フローを有効にするルール）。
- 3 NSX Edge ファイアウォール ユーザー インターフェイスのユーザー定義のルール。
- 4 デフォルトルール。

デフォルトの NSX Edge ファイアウォール ルールの編集

デフォルトのファイアウォール設定は、どのユーザー定義ファイアウォール ルールにも一致しないトラフィックに適用されます。デフォルトの Edge ファイアウォール ポリシーでは、すべての受信トラフィックがブロックされます。デフォルトのアクション設定とログ設定を変更できます。

手順

- 1 vSphere Web Client で、[ネットワークとセキュリティ (Networking & Security)] - [NSX Edge (NSX Edges)] の順に移動します。

- 2 NSX Edge をダブルクリックします。
- 3 [管理 (Manage)] タブをクリックして、[ファイアウォール (Firewall)] をクリックします。
- 4 ファイアウォール テーブルで最後のルールになっている [デフォルト ルール (Default Rule)] を選択します。
- 5 新しいルールの [アクション (Action)] セルをポイントし、 をクリックします。
 - a [承諾 (Accept)] をクリックして、指定した送信元と宛先で送受信されるトラフィックを許可します。
 - b [ログ (Log)] をクリックし、このルールと一致するすべてのセッションのログを記録します。
ログを有効にするとパフォーマンスに影響が出る場合があります。
 - c 必要に応じてコメントを入力します。
 - d [OK] をクリックします。
- 6 [変更の発行 (Publish Changes)] をクリックします。

NSX Edge ファイアウォール ルールの追加

[Edge ファイアウォール] タブには、[集中管理ファイアウォール] タブで作成されたルールが読み取り専用モードで表示されます。ここで追加したルールは、[集中管理ファイアウォール] タブには表示されません。

複数の NSX Edge インターフェイスや IP アドレス グループをファイアウォール ルールの送信元および送信先として追加できます。

図 10-1. NSX Edge インターフェイスから HTTP サーバへ向かうトラフィックのためのファイアウォール ルール

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	vnic-index-0:any	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

HTTP Address Group
Value:
10.20.222.34

For HTTP server
Value:
TCP:8080

図 10-2. NSX Edge のすべての内部インターフェイス（内部インターフェイスに接続されているポートグループ上のサブネット）から HTTP サーバへ向かうトラフィックのためのファイアウォール ルール

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	internal	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

HTTP Address Group
Value:
10.20.222.34

For HTTP server
Value:
TCP:8080

注: 送信元として [内部 (internal)] を選択すると、追加の内部インターフェイスを設定するときにルールが自動的に更新されます。

図 10-3. 内部ネットワーク内の m/c への SSH を許可するトラフィックのためのファイアウォール ルール





No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to internal network	User	any	VM in internal netw...	Internal VM	Accept
3	Default Rule	Default	any			Deny

VM in internal network
 Value:
 192.168.0.10


Internal VM
 Value:
 TCP:22



手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [NSX Edge] の順に移動します。
- 2 NSX Edge をダブルクリックします。
- 3 [管理 (Manage)] タブをクリックして、[ファイアウォール (Firewall)] タブをクリックします。
- 4 次のいずれかを実行します。

オプション	説明
ファイアウォールテーブル中の特定の場所にルールを追加する	<p>a ルールを選択します。</p> <p>b [番号] 列で  をクリックし、[上に追加 (Add Above)] または [下に追加 (Add Below)] を選択します。</p> <p>選択したルールの下に新しい許可ルールが追加されます。ファイアウォール テーブルにシステム定義のルールしかない場合は、新しいルールはデフォルトのルールの上に追加されます。</p>
ルールをコピーしてルールを追加する	<p>a ルールを選択します。</p> <p>b [コピー] () アイコンをクリックします。</p> <p>c ルールを選択します。</p> <p>d [番号] 列で、 をクリックし、[上に貼り付け (Paste Above)] または [下に貼り付け (Paste Below)] を選択します。</p>
ファイアウォールテーブル中の任意の場所にルールを追加する	<p>a [追加 (Add)] () アイコンをクリックします。</p> <p>選択したルールの下に新しい許可ルールが追加されます。ファイアウォール テーブルにシステム定義のルールしかない場合は、新しいルールはデフォルトのルールの上に追加されます。</p>

新しいルールはデフォルトで有効になっています。

- 5 新しいルールの [名前 (Name)] セルをポイントし、 をクリックします。
- 6 新しいルールの名前を入力します。

- 7 新しいルールの [ソース (Source)] セルをポイントし、 または  をクリックします。

 をクリックした場合は、IP アドレスを入力します。

- a ドロップダウン リストからオブジェクトを選択し、適切な選択を行います。

[vNIC グループ (vNIC Group)] を選択してから [vse] を選択すると、ルールは NSX Edge によって生成されたトラフィックに適用されます。[内部 (internal)] または [外部 (external)] を選択すると、ルールは、選択した NSX Edge インスタンス の内部またはアップリンク インターフェイスから流れるトラフィックに適用されます。ルールは、追加のインターフェイスの設定時に自動的に更新されます。内部インターフェイスのファイアウォール ルールは、論理ルーターでは機能しません。

[IP セット (IP Sets)] を選択すると、新しい IP アドレス グループを作成できます。新しいグループを作成すると、自動的に送信元の列に追加されます。IP セットの作成の詳細については、[「IP アドレス グループの作成」](#)を参照してください。

- b [OK] をクリックします。

- 8 新しいルールの [ターゲット (Destination)] セルをポイントし、 または  をクリックします。



- a ドロップダウン リストからオブジェクトを選択し、適切な選択を行います。

[vNIC グループ (vNIC Group)] を選択してから [vse] を選択すると、ルールは NSX Edge によって生成されたトラフィックに適用されます。[内部 (internal)] または [外部 (external)] を選択すると、ルールは、選択した NSX Edge インスタンス の内部またはアップリンク インターフェイスへ流れるトラフィックに適用されます。ルールは、追加のインターフェイスの設定時に自動的に更新されます。内部インターフェイスのファイアウォール ルールは、論理ルーターでは機能しません。


[IP セット (IP Sets)] を選択すると、新しい IP アドレス グループを作成できます。新しいグループを作成すると、自動的に送信元の列に追加されます。IP セットの作成の詳細については、[「IP アドレス グループの作成」](#)を参照してください。

- b [OK] をクリックします。

- 9 新しいルールの [サービス (Service)] セルをポイントし、 または  をクリックします。

-  をクリックした場合は、サービスを選択します。新しいサービスまたはサービス グループを作成するには、[新規 (New)] をクリックします。新しいサービスを作成すると、自動的にサービスの列に追加されます。新規サービスの作成の詳細については、[「サービスの作成」](#)を参照してください。
-  をクリックした場合は、プロトコルを選択します。[詳細オプション] の横にある矢印をクリックして、ソース ポートを指定できます。VMware は、リリース 5.1 以降のソース ポートを指定しないことを推奨しています。そのかわり、プロトコルとポートの組み合わせについてサービスを作成できます。



注: NSX Edge では、L3 プロトコルで定義されたサービスのみがサポートされます。


- 10 新しいルール of [アクション (Action)] セルをポイントし、 をクリックします。次の表の説明に従って適切な選択を行い、[OK] をクリックします。

選択したアクション	結果
許可	指定した送信元と送信先で送受信されるトラフィックを許可します。
ブロック	指定した送信元と送信先で送受信されるトラフィックをブロックします。
拒否	受け入れられないパケットに対する拒否メッセージを送信します。 TCP パケットでは、RST パケットが送信されます。 他のパケットでは、ICMP 到達不能（管理上制限されている）パケットが送信されます。
ログに記録	このルールと一致するすべてのセッションのログを記録します。ログを有効にするとパフォーマンスに影響が出る場合があります。
ログに記録しない	セッションのログを記録しません。
コメント	必要に応じてコメントを入力します。
[詳細オプション] > [一致] > [変換された IP]	変換された IP アドレスおよび NAT ルールに関するサービスにルールを適用します。
ルールの方向の有効化	ルールの方向（受信または送信）を示します。 VMware は、ファイアウォール ルールの方向を指定することはお勧めしていません。

- 11 [変更の発行 (Publish Changes)] をクリックして、新しいルールを NSX Edge インスタンスに適用します。

次のステップ

- ルールを無効にするには、[番号 (No.)] 列のルール番号の横の  をクリックします。
- 生成されたルールまたは事前ルール（[集中管理ファイアウォール] タブで追加されたルール）を非表示にするには、[生成されたルールを非表示にする (Hide Generated rules)] または [事前ルールを非表示にする (Hide Pre rules)] をクリックします。
- ルール テーブル内の追加の列を表示するには、 をクリックし、適切な列を選択します。

カラム名	表示される情報
ルール タグ	各ルールに対してシステムが生成した一意の ID
ログに記録	このルールのトラフィックがログ記録されるかどうか
統計	 をクリックすると、このルール（セッション数、トラフィック パケットおよびサイズ）の影響を受けるトラフィックが表示されます
コメント	ルールのコメント

- 検索フィールドにテキストを入力し、ルールを検索します。

NSX Edge ファイアウォール ルールの編集

[Edge ファイアウォール] タブで追加された、ユーザー定義のファイアウォール ルールのみを編集できます。[統合ファイアウォール] タブで追加されたルールを [Edge ファイアウォール] タブで編集することはできません。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [NSX Edge (NSX Edges)] の順に移動します。
- 2 NSX Edge をダブルクリックします。
- 3 [監視 (Monitor)] タブをクリックして、[ファイアウォール (Firewall)] タブをクリックします。
- 4 編集するルールを選択します。

注: 自動生成のルールやデフォルト ルールは変更できません。

- 5 必要な変更を行い、[OK] をクリックします。
- 6 [変更の発行 (Publish Changes)] をクリックします。



NSX Edge ファイアウォール ルールの優先順位の変更

[Edge ファイアウォール] タブで追加されたユーザー定義のファイアウォール ルールの順序を変更し、NSX Edge を通過するトラフィックをカスタマイズできます。たとえば、ロード バランサのトラフィックを許可するルールを設定しているとします。ここで、特定の IP アドレス グループからのロード バランサのトラフィックを拒否するルールを追加し、このルールをロード バランサを許可するトラフィック ルールの上に置くことができます。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [NSX Edge (NSX Edges)] の順に移動します。
- 2 NSX Edge をダブルクリックします。
- 3 [監視 (Monitor)] タブをクリックして、[ファイアウォール (Firewall)] タブをクリックします。
- 4 優先順位を変更するルールを選択します。

注: 自動生成されたルールまたはデフォルト ルールの優先順位は変更できません。

- 5 [上へ移動 (Move Up)] () または [下へ移動 (Move Down)] () アイコンをクリックします。
- 6 [OK] をクリックします。
- 7 [変更の発行 (Publish Changes)] をクリックします。

NSX Edge ファイアウォール ルールの削除

NSX Edge の [ファイアウォール] タブで追加された、ユーザー定義のファイアウォール ルールを削除できます。[統合ファイアウォール] タブで追加されたルールは、ここでは削除できません。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [NSX Edge (NSX Edges)] の順に移動します。
- 2 NSX Edge をダブルクリックします。

- 3 [監視 (Monitor)] タブをクリックして、[ファイアウォール (Firewall)] タブをクリックします。
- 4 削除するルールを選択します。

注: 自動生成されたルールまたはデフォルト ルールは削除できません。

- 5 [削除 (Delete)] (✖) アイコンをクリックします。

NAT ルールの管理

NSX Edge は、ネットワーク アドレス変換 (NAT) サービスを提供して、パブリック アドレスをプライベート ネットワーク内のコンピュータ（またはコンピュータ グループ）に割り当てます。このテクノロジーを使用すると、組織または企業が使用するパブリック IP アドレスの数が制限されるため、コストおよびセキュリティの面で利点があります。プライベートにアドレスが割り当てられた仮想マシン上で稼働しているサービスにアクセスするには、NAT ルールを設定する必要があります。

NAT サービスの設定は、送信元の NAT (SNAT) ルールと宛先の NAT (DNAT) ルールに分けられます。

SNAT ルールの追加

ソース IP アドレスをパブリックからプライベートの IP アドレスまたはその逆に変更するソース NAT (SNAT) ルールを作成できます。

前提条件

- 変換された（パブリック）IP アドレスを、ルールを追加する NSX Edge インターフェイスに追加しておく必要があります。
- SNAT ルールはサブインターフェイスではサポートされません。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [NSX Edge]] の順に移動します。
- 2 NSX Edge をダブルクリックします。
- 3 [管理 (Manage)] タブをクリックして、[NAT] タブをクリックします。
- 4 [追加 (Add)] (✚) アイコンをクリックし、[SNAT ルールの追加 (Add SNAT Rule)] を選択します。
- 5 ルールを追加するインターフェイスを選択します。

SNAT ルールはサブインターフェイスではサポートされません。

- 6 元の送信元 IP アドレスを次のいずれかのフォーマットで入力します。

フォーマット	例
IP アドレス	192.0.2.0
IP アドレス範囲	192.0.2.0 ~ 192.0.2.24
IP アドレス/サブネット	192.0.2.0/24
any	

- 7 変換された（公開の）送信元 IP アドレスを次のいずれかのフォーマットで入力します。

フォーマット	例
IP アドレス	192.0.2.0
IP アドレス範囲	192.0.2.0 ~ 192.0.2.24
IP アドレス/サブネット	192.0.2.0/24
any	

- 8 [有効 (Enabled)] を選択してルールを有効にします。
- 9 [ログの有効化 (Enable logging)] をクリックし、アドレス変換のログを記録します。
- 10 [OK] をクリックしてルールを追加します。
- 11 [変更の発行 (Publish Changes)] をクリックします。


DNAT ルールの追加

ターゲット IP アドレスをパブリックからプライベートの IP アドレスまたはその逆に変更するターゲット NAT (DNAT) ルールを作成できます。

前提条件

元の（パブリック）IP アドレスを、ルールを追加する NSX Edge インターフェイスに追加しておく必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[NAT] タブをクリックします。
- 5 [追加 (Add)]（）アイコンをクリックし、[DNAT ルールの追加 (Add DNAT Rule)] を選択します。
- 6 DNAT ルールを適用するインターフェイスを選択します。
- 7 オリジナル（パブリック）IP アドレスを次のいずれかのフォーマットで入力します。

フォーマット	例
IP アドレス	192.0.2.0
IP アドレス範囲	192.0.2.0 ~ 192.0.2.24
IP アドレス/サブネット	192.0.2.0/24
any	

- 8 プロトコルを入力します。

- 9 オリジナルのポートまたはポート範囲を入力します。

フォーマット	例
ポート番号	80
ポート範囲	80-85
any	

- 10 変換された IP アドレスを次のいずれかのフォーマットで入力します。

フォーマット	例
IP アドレス	192.0.2.0
IP アドレス範囲	192.0.2.0 ~ 192.0.2.24
IP アドレス/サブネット	192.0.2.0 /24
any	

- 11 変換されたポートまたはポート範囲を入力します。

フォーマット	例
ポート番号	80
ポート範囲	80-85
any	

- 12 [有効 (Enabled)] を選択してルールを有効にします。
- 13 [ログの有効化 (Enable logging)] を選択し、アドレス変換のログを記録します。
- 14 [追加 (Add)] をクリックしてルールを保存します。

Identity Firewall の概要

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 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。準備段階では、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、分散ファイアウォール 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。IDFW がログインを検出する方法は、ゲスト イントロスペクションおよび Active Directory イベント ログ スクレイパの 2 種類です。ゲスト イントロスペクションは、IDFW 仮想マシンを実行する ESXi クラスタに展開します。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、仮想マシンにインストールされたゲスト エージェントは、ゲスト イントロスペクションフレームワークを介して NSX Manager に情報を転送します。第 2 のオプションは、Active Directory イベント ログ スクレイパです。NSX Manager で、Active Directory ドメイン コントローラのインスタンスにポイントするように Active Directory イベント ログ スクレイパを設定します。これにより、NSX Manager は Active Directory セキュリティ イベント ログからイベントを取得できるようになります。これらの方法のいずれか、または両方を使用できます。Active Directory イベント ログ スクレイパとゲスト イントロスペクション の両方を使用する場合は、これらが排他的に動作することに注意してください。つまり、片方が動作を停止しても、他方がバックアップとして動作を開始することはありません。

インフラストラクチャを準備したら、管理者は NSX セキュリティ グループを作成し、新しく使用可能になった Active Directory (ディレクトリ グループと呼ばれます) を追加します。続いて管理者は、ファイアウォール ルールが関連付けられたセキュリティ ポリシーを作成して、これらのポリシーを新規に作成したセキュリティ グループに適用します。この操作によって、ユーザーがデスクトップにログインすると、システムはイベントおよび使用されている IP アドレスを検出し、そのユーザーに関連付けられているファイアウォール ポリシーを検索して、これらのルールを適用します。これは、物理および仮想の両方のデスクトップで機能します。物理デスクトップについては、ユーザーが物理デスクトップにログインしたことを検出する目的でも、Active Directory イベント ログ スクレイパが必要となります。

Identity Firewall がサポートする OS

Active Directory をサポートするサーバ

- Windows 2012
- Windows 2008

- Windows 2008 R2

サポートされるゲスト OS

- Windows 2012
- Windows 2008
- Windows 2008 R2
- Windows 10
- Windows 8 (32 ビットまたは 64 ビット)
- Windows 7 (32 ビットまたは 64 ビット)

Identity Firewall のワークフロー

Identity Firewall (IDFW) によって、ユーザー ベースの Distributed Firewall (DFW) ルールが利用できるようになります。

ユーザー ベースの Distributed Firewall (DFW) 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 (IDFW) は、Active Directory ユーザーのログイン先を監視し、ファイアウォール ルールを適用するために Distributed Firewall によって使用される IP アドレスに対して、ログインをマッピングします。Identity Firewall では、ゲスト イントロスペクション フレームワークまたは Active Directory イベント ログ スクレイピングのいずれかが必要です。

手順

- 1 NSX で Active Directory の同期を設定します。[「Windows ドメインと Active Directory の同期」](#)を参照してください。この操作は、Service Composer で Active Directory グループを使用するために必要とされます。
- 2 Distributed Firewall 用に ESXi クラスタを準備します。『NSX インストール ガイド』の「NSX 用ホスト クラスタの準備」を参照してください。
- 3 Identity Firewall ログイン検出オプションを設定します。これらのオプションのいずれか 1 つまたは両方を設定する必要があります。
 - Active Directory イベント ログ アクセスを設定します。[「NSX Manager への Windows ドメインの登録」](#)を参照してください。
 - ゲスト エージェントがインストールされている Windows ゲスト OS。これは、VMware Tools™ の完全なインストールに含まれます。保護されているクラスタに対して、ゲスト イントロスペクション サービスをデプロイします。[「ゲスト イントロスペクション のインストール」](#)を参照してください。ゲスト イントロスペクションのトラブルシューティングについては、[「ゲスト イントロスペクションのトラブルシューティング データの収集」](#)を参照してください。

Active Directory ドメインの操作

1 つ以上の Windows ドメインを NSX Manager および関連する vCenter Server に登録できます。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先の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。

NSX Manager が Active Directory 認証情報を取得すると、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 ルールを作成し、アクティビティ モニタリング レポートを実行できるようになります。

この章には、次のトピックが含まれています。

- [NSX Manager への Windows ドメインの登録](#)
- [Windows ドメインと Active Directory の同期](#)
- [Windows ドメインの編集](#)
- [Windows 2008 で読み取り専用セキュリティ ログ アクセスを有効にする](#)
- [ディレクトリ権限の確認](#)

NSX Manager への Windows ドメインの登録

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。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 [ドメイン (Domain)] タブをクリックして、[ドメインの追加 (Add domain)] () アイコンをクリックします。

- 5 [ドメインの追加 (Add Domain)] ダイアログ ボックスで、完全修飾ドメイン名 (**eng.vmware.com** など) とドメインの netBIOS 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。

- 6 同期する際に、有効なアカウントを持っていないユーザーを除外するには、[無効なユーザーを無視 (Ignore disabled users)] をクリックします。
- 7 [次へ (Next)] をクリックします。
- 8 [LDAP オプション] ページで、ドメインと同期するドメイン コントローラを指定し、プロトコルを選択します。
- 9 必要に応じてポート番号を編集します。
- 10 ドメイン アカウントのユーザー認証情報を入力します。このユーザーは、ディレクトリ ツリー構造にアクセスできる必要があります。
- 11 [次へ (Next)] をクリックします。
- 12 (オプション) [セキュリティ イベント ログ アクセス] ページで、指定した Active Directory サーバのセキュリティ イベント ログにアクセスするための接続方法として、[CIFS] または [WMI] を選択します。必要に応じてポート番号を変更します。この手順は、Active Directory イベント ログ スクレイパによって使用されます。[「Identity Firewall のワークフロー」](#) を参照してください。

注: イベント ログリーダーは、Active Directory のイベント ログから、「Windows 2008/2012: 4624, Windows 2003: 540」という ID を持つイベントを探します。イベント ログ サーバには 128 MB という制限があります。この制限に到達すると、セキュリティ ログリーダーにイベント ID 1104 が表示されます。詳細については <https://technet.microsoft.com/en-us/library/dd315518> を参照してください。

- 13 LDAP サーバのユーザー認証情報を使用する場合は、[ドメイン認証情報を使用 (Use Domain Credentials)] を選択します。ログ アクセス用の代替ドメイン アカウントを指定する場合は、[ドメイン認証情報を使用 (Use Domain Credentials)] の選択を解除し、ユーザー名とパスワードを指定します。

指定したアカウントは、手順 10 で指定したドメイン コントローラのセキュリティ イベント ログを読み取る必要があります。

- 14 [次へ (Next)] をクリックします。
- 15 [設定の確認] ページで、入力した設定を確認します。
- 16 [終了 (Finish)] をクリックします。



注目: ドメインの競合によって、エンティティに対するドメインの追加処理が失敗したというエラー メッセージが表示された場合は、回避策として [自動マージ] を選択します。

ドメインが作成され、その設定がドメイン リストの下に表示されます。

次のステップ

イベント ログ サーバのログイン イベントが有効であることを確認します。

LDAP サーバを追加、編集、削除、有効、または無効にするには、ドメイン リストの下のパネルで [LDAP サーバ (LDAP Servers)] タブを選択します。イベント ログ サーバに対して同様のタスクを実行するには、ドメイン リストの下のパネルで [イベント ログ サーバ (Event Log Servers)] タブを選択します。複数の Windows サーバ（ドメイン コントローラ、Exchange サーバ、またはファイル サーバ）をイベント ログ サーバとして追加すると、ユーザー ID との関連付けが強化されます。

注: Identity Firewall を使用している場合、Active Directory サーバのみがサポートされます。

Windows ドメインと Active Directory の同期

デフォルトでは、登録されているすべてのドメインが Active Directory と 3 時間ごとに自動的に同期します。必要に応じて、オンデマンドで同期することもできます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 同期するドメインを選択します。
- 5 次のいずれかをクリックします。

クリック対象	宛先
	最後の同期イベント以降に変更されたローカル Active Directory オブジェクトが更新される差分同期を実行します。
	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。

Windows ドメインの編集

名前、netBIOS 名、プライマリ LDAP サーバ、およびドメインのアカウント認証情報を編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 ドメインを選択して、[ドメインの編集 (Edit domain)] アイコンをクリックします。
- 5 必要な変更を行い、[終了 (Finish)] をクリックします。

Windows 2008 で読み取り専用セキュリティ ログ アクセスを有効にする

読み取り専用セキュリティ ログ アクセスは、IDFW のイベント ログ スクレイパにより使用されます。

新しいユーザー アカウントを作成した後、ユーザーに読み取り専用アクセス権限を付与するために、Windows 2008 サーバベースのドメイン セクションで読み取り専用セキュリティ ログ アクセスを有効にする必要があります。

注: この手順は、ドメイン、ツリー、またはフォレストの 1 つのドメイン コントローラで実行する必要があります。

手順

- 1 [スタート(Start)] > [管理ツール(Administrative Tools)] > [Active Directory Users and Computers] の順に移動します。
- 2 ナビゲーション ツリーで、セキュリティ ログ アクセスを有効にするドメインに対応するノードを展開します。
- 3 展開したノードの下で、[Builtin] ノードを選択します。
- 4 グループのリストで [Event Log Readers] をダブルクリックします。
- 5 [Event Log Readers Properties] ダイアログ ボックスで、[Members] を選択します。
- 6 [Add...] ボタンをクリックします。
[Select Users, Contacts, Computers, or Groups] ダイアログが表示されます。
- 7 すでに「Active Directory リーダー」ユーザーのグループを作成した場合は、[Select Users, Contacts, Computers, or Groups] ダイアログでそのグループを選択します。ユーザーだけを作成し、グループを作成しなかった場合は、[Select Users, Contacts, Computers, or Groups] ダイアログでそのユーザーを選択します。
- 8 [OK] をクリックして、[Select Users, Contacts, Computers, or Groups] ダイアログを閉じます。
- 9 [OK] をクリックして、[Event Log Readers Properties] ダイアログを閉じます。
- 10 [Active Directory Users and Computers] ウィンドウを閉じます。

次のステップ

セキュリティ ログ アクセスを有効にした後で、[「ディレクトリ権限の確認」](#)の手順に従ってディレクトリ権限を確認します。

ディレクトリ権限の確認

ユーザー アカウントがセキュリティ ログの読み取りに必要な権限を持っていることを確認します。

新しいアカウントを作成してセキュリティ ログ アクセスを有効にした後で、セキュリティ ログを読み取り可能であることを確認する必要があります。

前提条件

セキュリティ ログ アクセスを有効にします。[「Windows 2008 で読み取り専用セキュリティ ログ アクセスを有効にする」](#)を参照してください。

手順

- 1 ドメインに属するワークステーションから、管理者としてドメインにログインします。
- 2 [スタート(Start)] > [管理ツール(Administrative Tools)] > [イベント ビューアー(Event Viewer)] の順に移動します。
- 3 [Action] メニューから [Connect to Another Computer...] を選択します。[Select Computer] ダイアログが表示されます。(イベント ログを表示するマシンにすでにログインしている場合でも、この操作を実行する必要があります。)
- 4 [Another computer] ラジオ ボタンがすでに選択されていない場合は、選択します。
- 5 [Another computer] ラジオボタンの隣のテキスト フィールドに、ドメイン コントローラの名前を入力します。または、[参照... (Browse...)] ボタンをクリックして、ドメイン コントローラを選択します。
- 6 [別のユーザーとして接続する (Connect as another user)] チェック ボックスを選択します。
- 7 [ユーザーの設定... (Set User...)] ボタンをクリックします。[イベント ビューアー] ダイアログ ボックスが表示されます。
- 8 [ユーザー名 (User name)] フィールドに、作成したユーザーのユーザー名を入力します。
- 9 [パスワード (Password)] フィールドに、作成したユーザーのパスワードを入力します。
- 10 [OK] をクリックします。
- 11 もう一度 [OK] をクリックします。
- 12 ナビゲーション ツリーで [Windows ログ (Windows Logs)] ノードを展開します。
- 13 [Windows ログ (Windows Logs)] ノードの下に [セキュリティ] ノードを選択します。アカウントに必要な権限が付与されていれば、ログ イベントが表示されます。

SpoofGuard の使用

vCenter Server と同期した後、NSX Manager は各仮想マシン上の VMware Tools からすべての vCenter ゲスト仮想マシンの IP アドレスを収集します。仮想マシンのセキュリティが侵害された場合は、IP アドレスのなりすましにより、悪意のあるデータ転送がファイアウォール ポリシーを通り抜ける可能性があります。

特定のネットワークの SpoofGuard ポリシーを作成することにより、VMware Tools によって報告される IP アドレスを認証し、必要に応じて変更してなりすましを防止することができます。SpoofGuard は本質的に VMX ファイルと vSphere SDK から集められた仮想マシンの MAC アドレスを信用します。ファイアウォール ルールと別個に運用することにより、SpoofGuard を使用して、なりすましと判断されたトラフィックをブロックすることができます。

SpoofGuard では、IPv4 アドレスと IPv6 アドレスの両方がサポートされます。IPv4 を使用する場合、SpoofGuard ポリシーでは、vNIC に割り当てられた単一の IP アドレスがサポートされます。IPv6 では、vNIC に割り当てられた複数の IP アドレスがサポートされます。SpoofGuard ポリシーは、仮想マシンから報告された IP アドレスの監視と管理を、次のいずれかのモードで行います。

最初の使用時に IP 割り当てを自動的に信頼	このモードでは、仮想マシンからのトラフィックの通過をすべて許可しつつ、vNIC-to-IP アドレス割り当てテーブルを作成します。必要なときにこのテーブルをレビューし、IP アドレスを変更することができます。このモードでは、vNIC の IPv4 アドレスと IPv6 アドレスをすべて自動的に承認します。
-------------------------------	---

使用前にすべての IP 割り当てを手動で検査して承認	このモードでは、各 vNIC-to-IP アドレス割り当てを承認するまでは、すべてのトラフィックがブロックされます。
-----------------------------------	--

注: SpoofGuard ではモードに関わらず本質的に DHCP リクエストを許可します。しかし、手動検査モードでは、DHCP に割り当てられた IP アドレスが承認されるまで、トラフィックは通過できません。

SpoofGuard には、システムで生成されたデフォルト ポリシーが含まれており、他の SpoofGuard ポリシーの対象とならないポート グループと論理ネットワークに適用されます。新しく追加されたネットワークは、既存のポリシーに追加するか、そのネットワーク用に新しいポリシーを作成するまで、自動的にデフォルト ポリシーに追加されます。

SpoofGuard は、NSX Distributed Firewall ポリシーが仮想マシンの IP アドレスを特定できる方法の 1 つです。詳細については、「[仮想マシンの IP 検出](#)」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。

- [SpoofGuard ポリシーの作成](#)
- [IP アドレスの承認](#)
- [IP アドレスの編集](#)

■ IP アドレスのクリア

SpoofGuard ポリシーの作成

SpoofGuard ポリシーを作成して、特定のネットワークの操作モードを指定できます。既存の SpoofGuard ポリシーの対象となっていないポート グループと論理スイッチには、システム生成（デフォルト）ポリシーが適用されます。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [SpoofGuard] の順に移動します。
- 2 [追加 (Add)] アイコンをクリックします。
- 3 ポリシーの名前を入力します。
- 4 [有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、ポリシーを有効にするかどうかを指定します。
- 5 [操作モード (Operation Mode)] では、以下のうちの 1 つを選びます。

オプション	説明
最初の使用時に IP 割り当てを自動的に信頼	NSX Manager での最初の登録で IP の割り当てをすべて信頼するには、このオプションを選択します。
使用前にすべての IP 割り当てを手動で検査して承認	すべての IP アドレスを手動で承認するには、このオプションを選択します。承認されない IP アドレスから出入りするすべてのトラフィックはブロックされます。

- 6 セットアップでローカル IP アドレスを許可するには、[この名前空間でローカル アドレスを有効なアドレスとして許可する (Allow local address as valid address in this namespace)] をクリックします。

仮想マシンをパワーオンしても DHCP サーバに接続できない場合、その仮想マシンにはローカル IP アドレスが割り当てられます。このローカル IP アドレスは、SpoofGuard モードが [この名前空間でローカル アドレスを有効なアドレスとして許可する (Allow local address as valid address in this namespace)] に設定されている場合にのみ有効と見なされます。それ以外の場合、ローカル IP アドレスは無視されます。

- 7 [次へ (Next)] をクリックします。
- 8 ポリシーのスコープを指定するには、[追加 (Add)] をクリックして、このポリシーを適用するネットワーク、分散ポート グループ、または論理スイッチを選択します。

ポート グループまたは論理スイッチは、1 つの SpoofGuard ポリシーのみに属することができます。

- 9 [OK] をクリックし、[終了 (Finish)] をクリックします。

次のステップ

[編集 (Edit)] アイコンをクリックしてポリシーを編集したり、[削除 (Delete)] アイコンをクリックしてポリシーを削除したりすることができます。

IP アドレスの承認

SpoofGuard ですべての IP アドレス割り当てに対し手動承認が行われるように設定した場合、仮想マシンからのトラフィックを許可するには IP アドレス割り当てを承認する必要があります。

手順

- 1 [SpoofGuard] タブで、ポリシーを選択します。

ポリシーの詳細はポリシー テーブルの下に表示されます。

- 2 [表示 (View)] で、いずれかのオプション リンクをクリックします。

オプション	説明
アクティブな仮想 NIC	検証されたすべての IP アドレスのリスト
最後の発行以降、アクティブな仮想 NIC	ポリシーが最後に更新されて以降、承認された IP アドレスのリスト
承認が必要な仮想 NIC IP	トラフィックがこれらの仮想マシンに出入りできるようになる前に承認が必要な IP アドレスの変更
IP が重複している仮想 NIC	選択されたデータセンター内で割り当てられた既存の IP アドレスと重複する IP アドレス
無効な仮想 NIC	発行された IP アドレスに現在の IP アドレスがマッチしていない IP アドレスのリスト
未発行の仮想 NIC IP	IP アドレスの割り当てを編集後まだ発行していない仮想マシンのリスト

- 3 次のいずれかを実行します。

- 1 つの IP アドレスを承認するには、その IP アドレスの横にある [承認 (Approve)] をクリックします。
- 複数の IP アドレスを承認するには、該当する vNIC を選択し、[検出された IP の承認 (Approve Detected IP(s))] をクリックします。

IP アドレスの編集

MAC アドレスに割り当てた IP アドレスを編集し、割り当てた IP アドレスを修正できます。

注: SpoofGuard は仮想マシンから一意の IP アドレスを受け付けます。しかし、IP アドレスの割り当ては 1 度しかできません。承認された IP アドレスは NSX 全体で一意です。IP アドレスの重複承認はできません。

手順

- 1 [SpoofGuard] タブで、ポリシーを選択します。

ポリシーの詳細はポリシー テーブルの下に表示されます。

- 2 [表示 (View)] で、いずれかのオプション リンクをクリックします。

オプション	説明
アクティブな仮想 NIC	検証されたすべての IP アドレスのリスト
最後の発行以降、アクティブな仮想 NIC	ポリシーが最後に更新されて以降、承認された IP アドレスのリスト
承認が必要な仮想 NIC IP	トラフィックがこれらの仮想マシンに出入りできるようになる前に承認が必要な IP アドレスの変更
IP が重複している仮想 NIC	選択されたデータセンター内で割り当てられた既存の IP アドレスと重複する IP アドレス
無効な仮想 NIC	発行された IP アドレスに現在の IP アドレスがマッチしていない IP アドレスのリスト
未発行の仮想 NIC IP	IP アドレスの割り当てを編集後まだ発行していない仮想マシンのリスト

- 3 適切な vNIC で、[編集 (Edit)] アイコンをクリックして適切な変更を行います。

- 4 [OK] をクリックします。

IP アドレスのクリア

承認済み IP アドレスの割り当てを SpoofGuard ポリシーからクリアします。

手順

- 1 [SpoofGuard] タブで、ポリシーを選択します。
ポリシーの詳細はポリシー テーブルの下に表示されます。
- 2 [表示 (View)] で、いずれかのオプション リンクをクリックします。

オプション	説明
アクティブな仮想 NIC	検証されたすべての IP アドレスのリスト
最後の発行以降、アクティブな仮想 NIC	ポリシーが最後に更新されて以降、承認された IP アドレスのリスト
承認が必要な仮想 NIC IP	トラフィックがこれらの仮想マシンに出入りできるようになる前に承認が必要な IP アドレスの変更
IP が重複している仮想 NIC	選択されたデータセンター内で割り当てられた既存の IP アドレスと重複する IP アドレス
無効な仮想 NIC	発行された IP アドレスに現在の IP アドレスがマッチしていない IP アドレスのリスト
未発行の仮想 NIC IP	IP アドレスの割り当てを編集後まだ発行していない仮想マシンのリスト

- 3 次のいずれかを実行します。
 - 単一の IP アドレスをクリアするには、IP アドレスの横にある [クリア (Clear)] をクリックします。
 - 複数の IP アドレスをクリアするには、適切な vNIC を選択してから [承認済み IP のクリア (Clear Approved IP(s))] をクリックします。

Virtual Private Network (VPN)

NSX Edge では複数のタイプの VPN をサポートします。SSL VPN-Plus を使用することで、リモートユーザーがプライベートの企業アプリケーションにアクセスできます。IPSec VPN により、NSX Edge インスタンスとリモートサイトとのサイト間接続が提供されます。また、L2 VPN により、地理的境界を越えた仮想マシンによるネットワーク接続を維持できるようにすることで、データセンターを拡張できます。

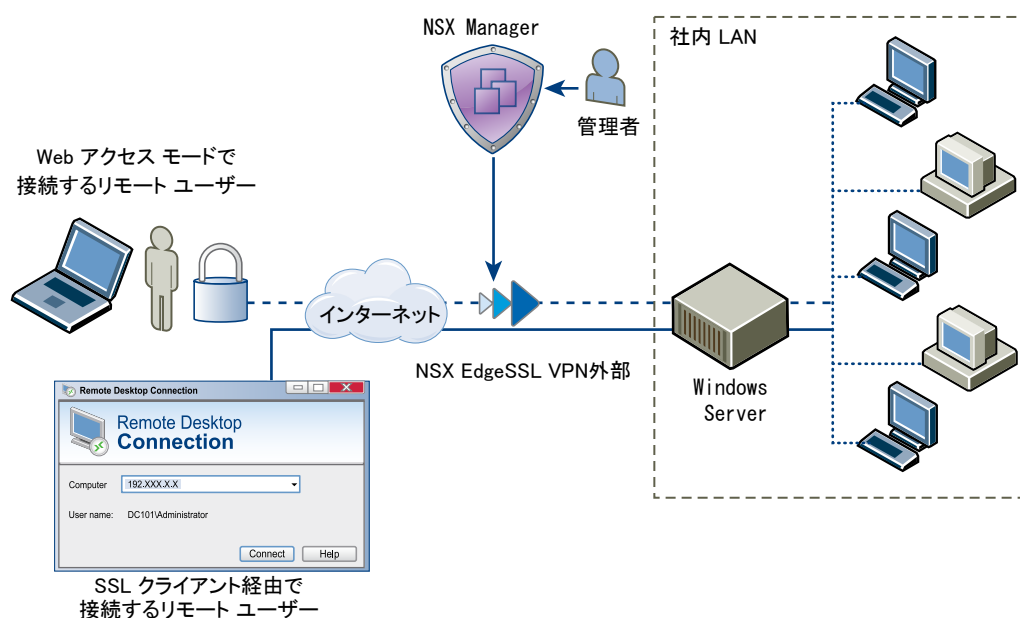
VPN を使用する前に、作業 NSX Edge インスタンスを設定する必要があります。NSX Edge のセットアップの詳細については、[「NSX Edge 設定」](#) を参照してください。

この章には、次のトピックが含まれています。

- [SSL VPN-Plus の概要](#)
- [IPSec VPN の概要](#)
- [L2 VPN の概要](#)

SSL VPN-Plus の概要

SSL VPN-Plus では、リモートユーザーが NSX Edge ゲートウェイの後方にあるプライベート ネットワークへ安全に接続できるようになります。リモートユーザーは、プライベート ネットワーク内のサーバやアプリケーションにアクセスできます。



サポートされているクライアント オペレーティング システムは次のとおりです。

- Windows XP 以降 (Windows 8 はサポート対象です)。
- Mac OS X Tiger、Leopard、Snow Leopard、Lion、Mountain Lion、Maverick、および Yosemite。これらは、手動または Java インストーラを使用してインストールできます。
- Linux : ユーザー インターフェイスを機能させるには TCL-TK が必要です。TCL-TK がない場合は、CLI を使用して、Linux クライアントを使用できます。

SSL VPN のトラブルシューティングについては、<https://kb.vmware.com/kb/2126671> を参照してください。

ネットワーク アクセス SSL VPN-Plus の設定

ネットワーク アクセス モードで、リモート ユーザーは、SSL クライアントをダウンロードし、インストールした後に、プライベート ネットワークにアクセスすることができます。

前提条件

SSL VPN ゲートウェイでは、ポート 443 に外部ネットワークからアクセスできるようにする必要があります。また、SSL VPN クライアントでは、NSX Edge ゲートウェイ IP アドレスおよびポート 443 にクライアント システムから接続できるようにする必要があります。

手順

1 SSL VPN-Plus サーバ設定の追加

NSX Edge インターフェイスで SSL を有効にするには、SSL VPN サーバの設定を追加する必要があります。

2 IP アドレス プールの追加

リモート ユーザーには、追加した IP アドレス プールから仮想 IP アドレスが割り当てられます。

3 プライベート ネットワークの追加

リモート ユーザーからのアクセスを許可するネットワークを追加します。

4 認証の追加

ローカル ユーザーのかわりに、SSL ゲートウェイにバインドされている外部認証サーバ (AD、LDAP、Radius、または RSA) を追加できます。バインドされた認証サーバにアカウントがあるすべてのユーザーが認証されます。

5 インストール パッケージの追加

リモート ユーザーのための SSL VPN-Plus Client のインストール パッケージを作成します。

6 ユーザーの追加

ローカル データベースにリモート ユーザーを追加します。

7 SSL VPN-Plus サービスを有効にする

SSL VPN-Plus サービスを設定したら、そのサービスを有効にして、リモート ユーザーがプライベート ネットワークへのアクセスを開始できるようにします。

8 スクリプトの追加

複数のログインまたはログオフ スクリプトを追加できます。たとえば、Internet Explorer を gmail.com で開始するようにログイン スクリプトをバインドすることができます。リモート ユーザーが SSL クライアントにログインすると、Internet Explorer が gmail.com を開きます。

9 リモート サイトへの SSL クライアントのインストール

このセクションでは、SSL VPN-Plus の設定後にリモート ユーザーが自分のデスクトップで実行できる手順について説明します。Windows、MAC、および Linux のデスクトップがサポートされます。

SSL VPN-Plus サーバ設定の追加

NSX Edge インターフェイスで SSL を有効にするには、SSL VPN サーバの設定を追加する必要があります。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [サーバ設定] を選択します。
- 2 [変更] をクリックします。
- 3 IPv4 または IPv6 アドレスを選択します。
- 4 必要に応じてポート番号を編集します。このポート番号は、インストール パッケージをするために必要です。
- 5 暗号化方式を選択します。
- 6 (オプション) [サーバの証明書] テーブルから、追加するサーバ証明書を選択します。
- 7 [OK] をクリックします。

IP アドレス プールの追加

リモート ユーザーには、追加した IP アドレス プールから仮想 IP アドレスが割り当てられます。

手順


- 1 [SSL Vpn-Plus] タブで、左側のパネルから [IP アドレス プール (IP Pools)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 IP アドレス プールの開始および終了の IP アドレスを入力します。
- 4 IP アドレス プールのネットマスクを入力します。
- 5 NSX Edge Gateway のルーティング インターフェイスに追加する IP アドレスを入力します。
- 6 (オプション) IP アドレス プールの説明を入力します。
- 7 IP アドレス プールを有効にするか無効にするかを選択します。
- 8 (オプション) [詳細 (Advanced)] パネルで、DNS 名を入力します。
- 9 (オプション) セカンダリ DNS 名を入力します。
- 10 ドメイン ベースのホスト名解決のための接続固有の DNS サフィックスを入力します。
- 11 WINS サーバ アドレスを入力します。

12 [OK] をクリックします。

プライベート ネットワークの追加

リモート ユーザーからのアクセスを許可するネットワークを追加します。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [非公開ネットワーク] を選択します。
- 2 [追加] () アイコンをクリックします。
- 3 プライベート ネットワークの IP アドレスを入力します。
- 4 プライベート ネットワークのネットマスクを入力します。
- 5 (オプション) ネットワークの説明を入力します。
- 6 プライベート ネットワークとインターネット トラフィックを SSL VPN-Plus が有効な NSX Edge を介して送信するのか、または NSX Edge を迂回することによってプライベート サーバに直接送信するのかを指定します。
- 7 [トンネルを介してトラフィックを送信する] を選択した場合は、[TCP 最適化の有効化] を選択してインターネットの速度を最適化します。

従来のフルアクセス SSL VPN トンネルは、インターネットを介した暗号化のために、TCP/IP データを 2 番目の TCP/IP スタックで送信します。これにより、アプリケーション レイヤーのデータは、2 つの別々の TCP ストリームで 2 度パケット化されることになります。パケット ロスが発生すると (最適なインターネット条件下でも発生)、TCP-over-TCP メルトダウンと呼ばれるパフォーマンスの低下が発生します。本質的に、2 つの TCP 計測ツールが 1 つの IP データ パケットを修正することにより、ネットワークのスループットが低下し、接続がタイムアウトになります。TCP の最適化によってこの TCP-over-TCP 問題を解消し、最適なパフォーマンスを確保します。

- 8 最適化が有効になっている場合、トラフィックを最適化するポート番号を指定します。

そのネットワークの残りのポートのトラフィックは最適化されません。

TCP トラフィックが最適化されると、TCP 接続はクライアントの代わりに SSL VPN サーバによって開かれます。TCP 接続が SSLVPN サーバによって開かれるため、最初に自動で生成されるルールが適用され、それによって Edge から開かれたすべての接続が通過できます。最適化されないトラフィックは通常の Edge ファイアウォールルールによって評価されます。デフォルト ルールは「すべてを許可」です。

- 9 プライベート ネットワークを有効または無効にするかどうかを指定します。
- 10 [OK] をクリックします。

次のステップ


対応するファイアウォール ルールを追加して、プライベート ネットワーク トラフィックを許可します。

認証の追加

ローカル ユーザーのかわりに、SSL ゲートウェイにバインドされている外部認証サーバ (AD、LDAP、Radius、または RSA) を追加できます。バインドされた認証サーバにアカウントがあるすべてのユーザーが認証されます。

SSL VPN 経由の認証の最大時間は 3 分です。これは、認証以外のタイムアウトが 3 分で、このプロパティは設定できないためです。そのため、設定されている AD 認証のタイムアウトが 3 分を超えている場合や、認可のチェーンに複数の認証サーバがあり、ユーザー認証の時間が 3 分を超える場合は、認証されません。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [認証 (Authentication)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 認証サーバのタイプを選択します。
- 4 選択した認証サーバのタイプに応じて、次のフィールドを指定します。

◆ AD 認証サーバ

表 14-1. AD 認証サーバのオプション

オプション	説明
[SSL の有効化 (Enable SSL)]	SSL を有効にすると、Web サーバとブラウザの間に、暗号化されたリンクを確立します。
[IP アドレス (IP Address)]	認証サーバの IP アドレス。
[ポート (Port)]	デフォルト ポートの名前を表示します。必要に応じて編集します。
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[検索ベース (Search base)]	検索対象とする外部のディレクトリ ツリーの部分です。検索ベースには、組織、グループ、あるいは外部ディレクトリのドメイン名 (AD)などを指定できます。
[バインド DN (Bind DN)]	定義された検索ベース内で AD ディレクトリを検索することを許可された外部 AD サーバ上のユーザーです。たいていの場合、バインド DN は、ディレクトリ全体の検索が許可されます。バインド DN のロールは、AD ユーザーの認証に関する DN (識別名) について、クエリ フィルタおよび検索ベースを使用してディレクトリをクエリすることです。DN が返されると、AD ユーザーの認証に DN とパスワードが使用されます。
[バインドパスワード (Bind Password)]	AD ユーザーを認証するためのパスワードです。
[バインドパスワードの再入力 (Retype Bind Password)]	パスワードを再入力します。
[ログイン属性名 (Login Attribute Name)]	リモート ユーザーが入力したユーザー ID に一致する名前です。Active Directory の場合、ログイン属性名は SAMAccountName です。
[検索フィルタ (Search Filter)]	検索を制限するフィルタの値です。検索フィルタ フォーマットは、<attribute operator value> です。

表 14-1. AD 認証サーバのオプション (続き)

オプション	説明
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、この AD サーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ LDAP 認証サーバ

表 14-2. LDAP 認証サーバのオプション

オプション	説明
[SSL の有効化 (Enable SSL)]	SSL を有効にすると、Web サーバとブラウザの間に、暗号化されたリンクを確立します。
[IP アドレス (IP Address)]	外部サーバの IP アドレスです。
[ポート (Port)]	デフォルト ポートの名前を表示します。必要に応じて編集します。
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[検索ベース (Search base)]	検索対象とする外部のディレクトリ ツリーの部分です。検索ベースには、組織、グループ、あるいは外部ディレクトリのドメイン名 (AD)などを指定できます。
[バインド DN (Bind DN)]	定義された検索ベース内で AD ディレクトリを検索することを許可された外部サーバ上のユーザーです。たいていの場合、バインド DN は、ディレクトリ全体の検索が許可されます。バインド DN のロールは、AD ユーザーの認証に関する DN (識別名) について、クエリ フィルタおよび検索ベースを使用してディレクトリをクエリすることです。DN が返されると、AD ユーザーの認証に DN とパスワードが使用されます。
[バインド パスワード (Bind Password)]	AD ユーザーを認証するためのパスワードです。
[バインド パスワードの再入力 (Retype Bind Password)]	パスワードを再入力します。
[ログイン属性名 (Login Attribute Name)]	リモート ユーザーが入力したユーザー ID に一致する名前です。Active Directory の場合、ログイン属性名は sAMAccountName です。
[検索フィルタ (Search Filter)]	検索を制限するフィルタの値です。検索フィルタ フォーマットは、<attribute operator value> です。

表 14-2. LDAP 認証サーバのオプション (続き)

オプション	説明
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ RADIUS 認証サーバ

表 14-3. RADIUS 認証サーバのオプション

オプション	説明
[IP アドレス (IP Address)]	外部サーバの IP アドレスです。
[ポート (Port)]	デフォルト ポートの名前を表示します。必要に応じて編集します。
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[シークレット (Secret)]	RSA セキュリティ コンソールに認証エージェントを追加するときに指定した共有シークレットです。
[シークレットの再入力 (Retype secret)]	共有シークレットを再入力します。
[NAS IP アドレス (NAS IP Address)]	RADIUS 属性番号 4 として設定および使用される IP アドレス (NAS-IP-Address) です。RADIUS パケットの IP ヘッダ内の接続元 IP アドレスは変更されません。
[再試行回数 (Retry Count)]	RADIUS サーバが応答しない場合に、認証が失敗する前に RADIUS サーバと通信する回数です。
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ RSA-ACE 認証サーバ

表 14-4. RSA-ACE 認証サーバのオプション

オプション	説明
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[構成ファイル (Configuration File)]	[参照 (Browse)] をクリックして RSA Authentication Manager からダウンロードした sdconf.rec ファイルを選択します。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[ソース IP アドレス (Source IP Address)]	RSA サーバへのアクセスが可能な NSX Edge インターフェイスの IP アドレスです。
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ ローカル認証サーバ

表 14-5. ローカル認証サーバのオプション

オプション	説明
[パスワード ポリシーの有効化 (Enable password policy)]	選択すると、パスワード ポリシーを定義します。必要な値を指定します。
[パスワード ポリシーの有効化 (Enable password policy)]	<p>選択すると、アカウント ロックアウト ポリシーを定義します。必要な値を指定します。</p> <ol style="list-style-type: none"> [再試行回数] には、リモート ユーザーが誤ったパスワードを入力した後、そのアカウントへのアクセスを試みることができる回数を入力します。 [再試行期間] には、この期間中にログインが成功しなかった場合にリモート ユーザーのアカウントがロックされる期間を入力します。 <p>たとえば、[再試行回数] を 5 に、[再試行期間] を 1 分間に設定すると、1 分間のうちにログインに 5 回失敗すると、そのリモート ユーザーのアカウントがロックされることになります。</p> <ol style="list-style-type: none"> [ロックアウト期間] には、ユーザー アカウントがロック状態となっている期間を入力します。この期間が過ぎると、アカウントのロックは自動的に解除されます。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。



表 14-5. ローカル認証サーバのオプション (続き)

オプション	説明
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

インストール パッケージの追加

リモート ユーザーのための SSL VPN-Plus Client のインストール パッケージを作成します。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [インストール パッケージ] を選択します。
- 2 [追加] () アイコンをクリックします。
- 3 インストール パッケージのプロファイル名を入力します。
- 4 [ゲートウェイ] で、NSX Edge のパブリック インターフェイスの IP アドレスまたは FQDN を入力します。
この IP アドレスまたは FQDN は、SSL クライアントにバインドされます。クライアントのインストール時に、この IP アドレスまたは FQDN が SSL クライアントに表示されます。
- 5 サーバ設定で SSL VPN-Plus に指定したポート番号を入力します。[\[SSL VPN-Plus サーバ設定の追加\]](#) を参照してください。
- 6 (オプション) 追加の NSX Edge アップリンク インターフェイスを SSL クライアントにバインドするには、
 - a [追加] () アイコンをクリックします。
 - b IP アドレスとポート番号を入力します。
 - c [OK] をクリックします。
- 7 インストール パッケージは、デフォルトでは Windows オペレーティング システム用に作成されます。Linux または Mac を選択すると、Linux または Mac オペレーティング システム用のインストール パッケージも作成できます。
- 8 (オプション) インストール パッケージの説明を入力します。
- 9 [有効化] を選択し、インストール パッケージ ページにインストール パッケージを表示します。

10 必要に応じて次のオプションを選択します。


オプション	説明
ログイン時にクライアントを起動	リモート ユーザーがこのシステムにログオンすると、SSL VPN クライアントが起動されます。
パスワード記録を許可	オプションを有効にします。
サイレント モード インストールの有効化	リモート ユーザーに対してインストール コマンドを表示しません。
SSL クライアント ネットワーク アダプタを非表示にする	VMware SSL VPN-Plus アダプタを非表示にします。これは、SSL VPN インストール パッケージと併せてリモート ユーザーのコンピュータにインストールされるものです。
クライアント システムトレイ アイコンを非表示にする	VPN 接続がアクティブかアクティブでないかを示す SSL VPN トレイ アイコンを非表示にします。
デスクトップ アイコンの作成	ユーザーのデスクトップに SSL クライアントを起動するアイコンを作成します。
サイレント モードの操作の有効化	インストールが完了したことを示すポップアップを非表示にします。
サーバ セキュリティ 証明書の検証	SSL VPN クライアントが安全な接続を確立する前に SSL VPN サーバ証明書を検証します。

11 [OK] をクリックします。

ユーザーの追加

ローカル データベースにリモート ユーザーを追加します。

手順

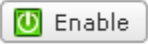
- 1 [SSL Vpn-Plus] タブで、左側のパネルから [ユーザー (Users)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 ユーザー ID を入力します。
- 4 パスワードを入力します。
- 5 パスワードを再入力します。
- 6 (オプション) ユーザーの姓名を入力します。
- 7 (オプション) ユーザーの説明を入力します。
- 8 [パスワードの詳細] で、[パスワードは無期限です (Password never expires)] を選択すると、そのユーザーには常に同じパスワードが適用されます。
- 9 ユーザーにパスワードの変更を許可するには、[パスワードの変更を許可 (Allow change password)] を選択します。
- 10 ユーザーが次回ログインするときにパスワードを変更させるには、[次のログイン時にパスワードを変更 (Change password on next login)] をクリックします。
- 11 ユーザー ステータスを設定します。
- 12 [OK] をクリックします。

SSL VPN-Plus サービスを有効にする

SSL VPN-Plus サービスを設定したら、そのサービスを有効にして、リモート ユーザーがプライベート ネットワークへのアクセスを開始できるようにします。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [ダッシュボード (Dashboard)] を選択します。

- 2  アイコンをクリックします。

ダッシュボードに、サービスのステータス、アクティブな SSL VPN セッションの数、およびセッションの統計とデータ フローの詳細が表示されます。[アクティブ セッションの数] の隣にある [詳細 (Details)] をクリックして、NSX Edge ゲートウェイの内側にあるプライベート ネットワークへの同時接続に関する情報を表示します。


次のステップ

- 1 SNAT ルールを追加して、NSX Edge アプライアンスの IP アドレスを VPN Edge の IP アドレスに変換します。
- 2 Web ブラウザに **https://<NSXEdgeIPAddress>** と入力して、NSX Edge インターフェイスの IP アドレスに移動します。
- 3 [\[ユーザーの追加\]](#) セクションで作成したユーザー名およびパスワードを使用してログインし、インストール パッケージをダウンロードします。
- 4 [\[SSL VPN-Plus サーバ設定の追加\]](#) で使用したポート番号に対して、ルーターでのポート転送を有効にします。
- 5 VPN クライアントを起動し、VPN サーバを選択してログインします。この時点で、ネットワーク上のサービスに移動できます。SSL VPN-Plus ゲートウェイのログが、NSX Edge アプライアンスで設定された Syslog サーバに送信されます。SSL VPN-Plus Client のログは、リモート ユーザーのコンピュータの **%PROGRAMFILES %\VMWARE\SSLVPN Client** ディレクトリに格納されます。

スクリプトの追加

複数のログインまたはログオフ スクリプトを追加できます。たとえば、Internet Explorer を gmail.com で開始するようにログイン スクリプトをバインドすることができます。リモート ユーザーが SSL クライアントにログインすると、Internet Explorer が gmail.com を開きます。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 [スクリプト (Script)] で、[参照 (Browse)] をクリックし、NSX Edge Gateway にバインドするスクリプトを選択します。
- 4 スクリプトの [タイプ (Type)] を選択します。

オプション	説明
ログイン	リモート ユーザーが SSL VPN にログインするときにスクリプト アクションを実行します。
ログオフ	リモート ユーザーが SSL VPN からログアウトするときにスクリプト アクションを実行します。
両方	リモート ユーザーが SSL VPN のログインおよびログアウトを実行するときにスクリプト アクションを実行します。

- 5 スクリプトの説明を入力します。

- 6 [有効 (Enabled)] を選択してスクリプトを有効にします。
- 7 [OK] をクリックします。

リモート サイトへの SSL クライアントのインストール

このセクションでは、SSL VPN-Plus の設定後にリモート ユーザーが自分のデスクトップで実行できる手順について説明します。Windows、MAC、および Linux のデスクトップがサポートされます。

手順

- 1 リモート ユーザーは、クライアント サイトのブラウザ ウィンドウで (<https://<ExternalEdgeInterfaceIP>/sslvpn-plus/>) と入力します。ここで、<ExternalEdgeInterfaceIP> は、SSL VPN-Plus を有効にした、Edge の外部インターフェイスの IP アドレスを指します。
- 2 ユーザーの認証情報を使用してポータルにログインします。
- 3 [フル アクセス] タブをクリックします。
SSL クライアントがダウンロードされます。
- 4 [ユーザー] セクションで指定した認証情報を使って、SSL クライアントにログインします。
SSL VPN サーバの証明書が、クライアントのオペレーティング システムに応じて検証されます。

■ Windows クライアント

インストール パッケージが作成されたときに [サーバ セキュリティ 証明書の検証] オプションが選択されていた場合は、Windows クライアントが認証されます。

■ Linux クライアント

NSX for vSphere バージョン 6.1.3 以降では、デフォルトで、SSL VPN Linux クライアントは、Firefox の証明書ストアに対してサーバ証明書を検証します。サーバ証明書の検証が失敗すると、システム管理者に問い合わせるように求めるメッセージが表示されます。サーバ証明書の検証が成功した場合は、ログイン プロンプトが表示されます。

信頼できる CA のトラスト ストア (Firefox の証明書ストア) への追加は、SSL VPN ワーク フローとは独立した手順です。

■ OS X クライアント

NSX for vSphere バージョン 6.1.3 以降では、デフォルトで、SSL VPN OS X クライアントは、サーバ証明書をキーチェーン (OS X に証明書を格納するために使用されるデータベース) に対して検証します。サーバ証明書の検証が失敗すると、システム管理者に問い合わせるように求めるメッセージが表示されます。サーバ証明書の検証が成功した場合は、ログイン プロンプトが表示されます。

信頼できる CA のトラスト ストア (キーチェーンなど) への追加は、SSL VPN ワーク フローとは独立した手順です。

これで、リモート ユーザーがプライベート ネットワークにアクセスできるようになりました。

Web Access SSL VPN-Plus の設定

Web アクセス モードでは、リモート ユーザーはハードウェアやソフトウェアの SSL クライアントがなくても、プライベート ネットワークにアクセスすることができます。

手順

1 Web リソースの作成

Web ブラウザ経由でリモート ユーザーが接続できるサーバを追加します。

2 ユーザーの追加

ローカル データベースにリモート ユーザーを追加します。

3 認証の追加

ローカル ユーザーのかわりに、SSL ゲートウェイにバインドされている外部認証サーバ (AD、LDAP、Radius、または RSA) を追加できます。バインドされた認証サーバにアカウントがあるすべてのユーザーが認証されます。

4 SSL VPN-Plus サーバ設定の追加

NSX Edge インターフェイスで SSL を有効にするには、SSL VPN サーバの設定を追加する必要があります。

5 SSL VPN-Plus サービスを有効にする

SSL VPN-Plus サービスを設定したら、そのサービスを有効にして、リモート ユーザーがプライベート ネットワークへのアクセスを開始できるようにします。

6 スクリプトの追加

複数のログインまたはログオフ スクリプトを追加できます。たとえば、Internet Explorer を gmail.com で開始するようにログイン スクリプトをバインドすることができます。リモート ユーザーが SSL クライアントにログインすると、Internet Explorer が gmail.com を開きます。

Web リソースの作成

Web ブラウザ経由でリモート ユーザーが接続できるサーバを追加します。

手順

1 vSphere Web Client にログインします。

2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。

3 [NSX Edge] をダブルクリックします。

4 [管理] タブをクリックして、[SSL VPN-Plus] タブをクリックします。

5 左側のパネルから [Web リソース] を選択します。

6 [追加] () アイコンをクリックします。

7 Web リソースの名前を入力します。


8 リモート ユーザーがアクセスする Web リソースの URL を入力します。

- 9 リモート ユーザーがその Web リソースの読み書きのいずれかを希望するかに応じて、[HTTPMethod] を選択して、GET 呼び出しまたは POST 呼び出しを入力します。
- 10 Web リソースの説明を入力します。この説明は、リモート ユーザーが Web リソースにアクセスしたときに、Web ポータルに表示されます。
- 11 [有効] をクリックして Web リソースを有効にします。リモート ユーザーがアクセスするには、Web リソースを有効にする必要があります。

ユーザーの追加

ローカル データベースにリモート ユーザーを追加します。

手順


- 1 [SSL Vpn-Plus] タブで、左側のパネルから [ユーザー (Users)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 ユーザー ID を入力します。
- 4 パスワードを入力します。
- 5 パスワードを再入力します。
- 6 (オプション) ユーザーの姓名を入力します。
- 7 (オプション) ユーザーの説明を入力します。
- 8 [パスワードの詳細] で、[パスワードは無期限です (Password never expires)] を選択すると、そのユーザーには常に同じパスワードが適用されます。
- 9 ユーザーにパスワードの変更を許可するには、[パスワードの変更を許可 (Allow change password)] を選択します。
- 10 ユーザーが次回ログインするときにパスワードを変更させるには、[次のログイン時にパスワードを変更 (Change password on next login)] をクリックします。
- 11 ユーザー ステータスを設定します。
- 12 [OK] をクリックします。

認証の追加

ローカル ユーザーのかわりに、SSL ゲートウェイにバインドされている外部認証サーバ (AD、LDAP、Radius、または RSA) を追加できます。バインドされた認証サーバにアカウントがあるすべてのユーザーが認証されます。

SSL VPN 経由の認証の最大時間は 3 分です。これは、認証以外のタイムアウトが 3 分で、このプロパティは設定できないためです。そのため、設定されている AD 認証のタイムアウトが 3 分を超えている場合や、認可のチェーンに複数の認証サーバがあり、ユーザー認証の時間が 3 分を超える場合は、認証されません。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [認証 (Authentication)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。

- 3 認証サーバのタイプを選択します。
- 4 選択した認証サーバのタイプに応じて、次のフィールドを指定します。

◆ AD 認証サーバ

表 14-6. AD 認証サーバのオプション

オプション	説明
[SSL の有効化 (Enable SSL)]	SSL を有効にすると、Web サーバとブラウザの間に、暗号化されたリンクを確立します。
[IP アドレス (IP Address)]	認証サーバの IP アドレス。
[ポート (Port)]	デフォルト ポートの名前を表示します。必要に応じて編集します。
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[検索ベース (Search base)]	検索対象とする外部のディレクトリ ツリーの部分です。検索ベースには、組織、グループ、あるいは外部ディレクトリのドメイン名 (AD)などを指定できます。
[バインド DN (Bind DN)]	定義された検索ベース内で AD ディレクトリを検索することを許可された外部 AD サーバ上のユーザーです。たいていの場合、バインド DN は、ディレクトリ全体の検索が許可されます。バインド DN のロールは、AD ユーザーの認証に関する DN (識別名) について、クエリ フィルタおよび検索ベースを使用してディレクトリをクエリすることです。DN が返されると、AD ユーザーの認証に DN とパスワードが使用されます。
[バインドパスワード (Bind Password)]	AD ユーザーを認証するためのパスワードです。
[バインドパスワードの再入力 (Retype Bind Password)]	パスワードを再入力します。
[ログイン属性名 (Login Attribute Name)]	リモート ユーザーが入力したユーザー ID に一致する名前です。Active Directory の場合、ログイン属性名は sAMAccountName です。
[検索フィルタ (Search Filter)]	検索を制限するフィルタの値です。検索フィルタ フォーマットは、<attribute operator value> です。

表 14-6. AD 認証サーバのオプション (続き)

オプション	説明
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、この AD サーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ LDAP 認証サーバ

表 14-7. LDAP 認証サーバのオプション

オプション	説明
[SSL の有効化 (Enable SSL)]	SSL を有効にすると、Web サーバとブラウザの間に、暗号化されたリンクを確立します。
[IP アドレス (IP Address)]	外部サーバの IP アドレスです。
[ポート (Port)]	デフォルト ポートの名前を表示します。必要に応じて編集します。
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[検索ベース (Search base)]	検索対象とする外部のディレクトリ ツリーの部分です。検索ベースには、組織、グループ、あるいは外部ディレクトリのドメイン名 (AD)などを指定できます。
[バインド DN (Bind DN)]	定義された検索ベース内で AD ディレクトリを検索することを許可された外部サーバ上のユーザーです。たいていの場合、バインド DN は、ディレクトリ全体の検索が許可されます。バインド DN のロールは、AD ユーザーの認証に関する DN (識別名) について、クエリ フィルタおよび検索ベースを使用してディレクトリをクエリすることです。DN が返されると、AD ユーザーの認証に DN とパスワードが使用されます。
[バインド パスワード (Bind Password)]	AD ユーザーを認証するためのパスワードです。
[バインド パスワードの再入力 (Retype Bind Password)]	パスワードを再入力します。
[ログイン属性名 (Login Attribute Name)]	リモート ユーザーが入力したユーザー ID に一致する名前です。Active Directory の場合、ログイン属性名は sAMAccountName です。
[検索フィルタ (Search Filter)]	検索を制限するフィルタの値です。検索フィルタ フォーマットは、<attribute operator value> です。

表 14-7. LDAP 認証サーバのオプション (続き)

オプション	説明
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ RADIUS 認証サーバ

表 14-8. RADIUS 認証サーバのオプション

オプション	説明
[IP アドレス (IP Address)]	外部サーバの IP アドレスです。
[ポート (Port)]	デフォルト ポートの名前を表示します。必要に応じて編集します。
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[シークレット (Secret)]	RSA セキュリティ コンソールに認証エージェントを追加するときに指定した共有シークレットです。
[シークレットの再入力 (Retype secret)]	共有シークレットを再入力します。
[NAS IP アドレス (NAS IP Address)]	RADIUS 属性番号 4 として設定および使用される IP アドレス (NAS-IP-Address) です。RADIUS パケットの IP ヘッダ内の接続元 IP アドレスは変更されません。
[再試行回数 (Retry Count)]	RADIUS サーバが応答しない場合に、認証が失敗する前に RADIUS サーバと通信する回数です。
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ RSA-ACE 認証サーバ

表 14-9. RSA-ACE 認証サーバのオプション

オプション	説明
[タイムアウト (Timeout)]	AD サーバが応答しなければならない期間 (秒) です。
[構成ファイル (Configuration File)]	[参照 (Browse)] をクリックして RSA Authentication Manager からダウンロードした sdconf.rec ファイルを選択します。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。
[ソース IP アドレス (Source IP Address)]	RSA サーバへのアクセスが可能な NSX Edge インターフェイスの IP アドレスです。
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

◆ ローカル認証サーバ

表 14-10. ローカル認証サーバのオプション

オプション	説明
[パスワード ポリシーの有効化 (Enable password policy)]	選択すると、パスワード ポリシーを定義します。必要な値を指定します。
[パスワード ポリシーの有効化 (Enable password policy)]	<p>選択すると、アカウント ロックアウト ポリシーを定義します。必要な値を指定します。</p> <ol style="list-style-type: none"> [再試行回数] には、リモート ユーザーが誤ったパスワードを入力した後、そのアカウントへのアクセスを試みることができる回数を入力します。 [再試行期間] には、この期間中にログインが成功しなかった場合にリモート ユーザーのアカウントがロックされる期間を入力します。 <p>たとえば、[再試行回数] を 5 に、[再試行期間] を 1 分間に設定すると、1 分間のうちにログインに 5 回失敗すると、そのリモート ユーザーのアカウントがロックされることになります。</p> <ol style="list-style-type: none"> [ロックアウト期間] には、ユーザー アカウントがロック状態となっている期間を入力します。この期間が過ぎると、アカウントのロックは自動的に解除されます。
[ステータス (Status)]	[有効 (Enabled)] あるいは [無効 (Disabled)] を選択し、サーバが有効になっているかどうかを指定します。

表 14-10. ローカル認証サーバのオプション (続き)

オプション	説明
[セカンダリ認証にこのサーバの使用 (Use this server for secondary authentication)]	選択すると、このサーバが認証の第 2 レベルとして使用されます。
[認証に失敗した場合はセッションを終了 (Terminate Session if authentication fails)]	選択すると、認証に失敗した場合にセッションを終了します。

SSL VPN-Plus サーバ設定の追加

NSX Edge インターフェイスで SSL を有効にするには、SSL VPN サーバの設定を追加する必要があります。

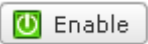
手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [サーバ設定] を選択します。
- 2 [変更] をクリックします。
- 3 IPv4 または IPv6 アドレスを選択します。
- 4 必要に応じてポート番号を編集します。このポート番号は、インストール パッケージをするために必要です。
- 5 暗号化方式を選択します。
- 6 (オプション) [サーバの証明書] テーブルから、追加するサーバ証明書を選択します。
- 7 [OK] をクリックします。

SSL VPN-Plus サービスを有効にする

SSL VPN-Plus サービスを設定したら、そのサービスを有効にして、リモートユーザーがプライベート ネットワークへのアクセスを開始できるようにします。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [ダッシュボード (Dashboard)] を選択します。
- 2  アイコンをクリックします。

ダッシュボードに、サービスのステータス、アクティブな SSL VPN セッションの数、およびセッションの統計とデータ フローの詳細が表示されます。[アクティブ セッションの数] の隣にある [詳細 (Details)] をクリックして、NSX Edge ゲートウェイの内側にあるプライベート ネットワークへの同時接続に関する情報を表示します。

次のステップ


- 1 SNAT ルールを追加して、NSX Edge アプライアンスの IP アドレスを VPN Edge の IP アドレスに変換します。

- 2 Web ブラウザに **https://<NSXEdgeIPAddress>** と入力して、NSX Edge インターフェイスの IP アドレスに移動します。
- 3 **「ユーザーの追加」** セクションで作成したユーザー名およびパスワードを使用してログインし、インストール パッケージをダウンロードします。
- 4 **「SSL VPN-Plus サーバ設定の追加」** で使用したポート番号に対して、ルーターでのポート転送を有効にします。
- 5 VPN クライアントを起動し、VPN サーバを選択してログインします。この時点で、ネットワーク上のサービスに移動できます。SSL VPN-Plus ゲートウェイのログが、NSX Edge アプライアンスで設定された Syslog サーバに送信されます。SSL VPN-Plus Client のログは、リモートユーザーのコンピュータの **%PROGRAMFILES %/VMWARE/SSLVPN Client/** ディレクトリに格納されます。

スクリプトの追加

複数のログインまたはログオフ スクリプトを追加できます。たとえば、Internet Explorer を gmail.com で開始するようにログイン スクリプトをバインドすることができます。リモートユーザーが SSL クライアントにログインすると、Internet Explorer が gmail.com を開きます。

手順

- 1 [SSL Vpn-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] を選択します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 [スクリプト (Script)] で、[参照 (Browse)] をクリックし、NSX Edge Gateway にバインドするスクリプトを選択します。
- 4 スクリプトの [タイプ (Type)] を選択します。

オプション	説明
ログイン	リモートユーザーが SSL VPN にログインするときにスクリプト アクションを実行します。
ログオフ	リモートユーザーが SSL VPN からログアウトするときにスクリプト アクションを実行します。
両方	リモートユーザーが SSL VPN のログインおよびログアウトを実行するときにスクリプト アクションを実行します。

- 5 スクリプトの説明を入力します。
- 6 [有効 (Enabled)] を選択してスクリプトを有効にします。
- 7 [OK] をクリックします。

SSL VPN-Plus のログ

SSL VPN-Plus ゲートウェイのログが、NSX Edge アプライアンスで設定された Syslog サーバに送信されます。SSL VPN-Plus Client のログは、リモートユーザーのコンピュータの次のディレクトリに格納されます。**%PROGRAMFILES %/VMWARE/SSL VPN Client/**。

クライアント設定の編集

リモート ユーザーが SSL VPN にログインしたときに SSL VPN クライアント トンネルが応答する方法を変更できます。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [クライアント (Client Configuration)] を選択します。
- 2 [トンネル モード (Tunneling Mode)] を選択します。
分割トンネル モードでは、VPN のみが NSX Edge Gateway を通過します。フル トンネルの場合、NSX Edge Gateway はリモート ユーザーのデフォルト ゲートウェイとなり、すべてのトラフィック (VPN、ローカルおよびインターネット) がこのゲートウェイを通過します。
- 3 フル トンネル モードを選択した場合 :
 - a [ローカル サブネットを除外 (Exclude local subnets)] を選択すると、VPN トンネルを通過するトラフィックからローカル トラフィックが除外されます。
 - b リモート ユーザーのシステムのデフォルト ゲートウェイの IP アドレスを入力します。
- 4 リモート ユーザーが切断後に自動的に SSL VPN クライアントに再接続するようにするには、[自動再接続の有効化 (Enable auto reconnect)] を選択します。
- 5 [クライアントのアップグレードを通知 (Client upgrade notification)] を選択すると、クライアントのアップグレードが使用可能になったときに、リモート ユーザーに通知が送信されます。リモート ユーザーはそのときに、アップグレードのインストールを選択できます。
- 6 [OK] をクリックします。

全般設定の編集

デフォルトの VPN 設定を編集することができます。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [全般設定] を選択します。
- 2 必要な選択を行います。

選択	宛先
複数のログインが同じユーザー名を使用することを防ぐ	リモート ユーザーが 1 つのユーザー名で 1 度だけログインすることを許可します。
圧縮の有効化	TCP ベースのインテリジェント データ圧縮を有効にし、データ転送速度を改善します。
ログの有効化	SSL VPN ゲートウェイを通過するトラフィックのログを保持します。
強制仮想キーボード	リモート ユーザーによる Web またはクライアントのログイン情報の入力を、仮想キーボードからの入力のみに限定します。
仮想キーボードのキーのランダム化	仮想キーボードのキーをランダムに配置します。
強制タイムアウトの有効化	指定したタイムアウト時間の経過後、リモート ユーザーを切断します。タイムアウト時間を分単位で入力します。
セッション アイドル タイムアウト	一定期間ユーザー セッションにアクティビティがない場合、その期間の経過後にユーザー セッションを終了します。

選択	宛先
ユーザー通知	ログイン後にリモート ユーザーに表示されるメッセージを入力します。
パブリック URL アクセスの有効化	リモート ユーザーが管理者によって設定されていない (Web ポータルにリストされていない) 任意のサイトにアクセスすることを許可します。

- 3 [OK] をクリックします。

Web ポータル デザインの編集

SSL VPN クライアントにバインドされたクライアント バナーを編集できます。

手順

- 1 [NSX Edge (NSX Edges)] タブで、NSX Edge をダブルクリックします。
- 2 [監視 (Monitor)] タブをクリックして、[SSL VPN-Plus] タブをクリックします。
- 3 左側のパネルから [ポータルのカスタマイズ (Portal Customization)] を選択します。
- 4 ポータル タイトルを入力します。
- 5 リモート ユーザーの会社名を入力します。
- 6 [ロゴ (Logo)] で、[変更 (Change)] をクリックし、リモート ユーザーのロゴのイメージ ファイルを選択します。
- 7 [色 (Colors)] で、色を変更する対象の番号付き項目の横にある色ボックスをクリックし、好みの色を選択します。
- 8 必要に応じて、クライアント バナーを変更します。
- 9 [OK] をクリックします。

IP アドレス プールの操作

IP アドレス プールを編集または削除できます。

IP アドレス プール追加の詳細については、[「ネットワーク アクセス SSL VPN-Plus の設定」](#) または [「Web Access SSL VPN-Plus の設定」](#) を参照してください。

IP アドレス プールの編集

IP アドレス プールを編集できます。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [IP アドレス プール (IP Pool)] をクリックします。
- 2 編集する IP アドレス プールを選択します。
- 3 [編集 (Edit)] (✎) アイコンをクリックします。
[IP アドレス プールの編集] ダイアログ ボックスが開きます。
- 4 必要に応じて編集します。
- 5 [OK] をクリックします。

IP アドレス プールの削除

IP アドレス プールを削除できます。

手順


- 1 [SSL VPN-Plus] タブで、左側のパネルから [IP アドレス プール (IP Pool)] をクリックします。
- 2 削除する IP アドレス プールを選択します。
- 3 [削除 (Delete)] () アイコンをクリックします。

選択した IP アドレス プールが削除されます。

IP アドレス プールを有効にする

IP アドレス プールの IP アドレスがリモート ユーザーに割り当てられるようにする場合は、その IP アドレス プールを有効にする必要があります。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [IP アドレス プール (IP Pool)] をクリックします。
- 2 有効にする IP アドレス プールを選択します。
- 3 [有効化 (Enable)] () アイコンをクリックします。

IP アドレス プールを無効にする

リモート ユーザーに IP プールから IP アドレスを割り当てない場合は、その IP アドレス プールを無効にすることができます。



手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [IP アドレス プール (IP Pool)] を選択します。
- 2 無効にする IP アドレス プールを選択します。
- 3 [無効化 (Disable)] () アイコンをクリックします。

IP アドレス プールの順序の変更

SSL VPN は、IP アドレス プール テーブルの順序に基づいてリモート ユーザーに IP アドレス プールから IP アドレスを割り当てます。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [IP アドレス プール (IP Pool)] をクリックします。
- 2 順序を変更する IP アドレス プールを選択します。
- 3 [上へ移動 (Move Up)] () または [下へ移動] () アイコンをクリックします。

プライベート ネットワークの操作


リモート ユーザーがアクセスできるプライベート ネットワークを編集または削除できます。

プライベート ネットワークの追加の詳細については、「[ネットワーク アクセス SSL VPN-Plus の設定](#)」または「[Web Access SSL VPN-Plus の設定](#)」を参照してください。

プライベート ネットワークの削除

プライベート ネットワークを削除できます。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [非公開ネットワーク (Private Networks)] をクリックします。
- 2 削除するネットワークを選択し、[削除 (Delete)] () アイコンをクリックします。

プライベート ネットワークを有効にする

プライベート ネットワークを有効にすると、リモート ユーザーは SSL VPN-Plus を介してそのネットワークにアクセスできます。

手順


- 1 [SSL VPN-Plus] タブで、左側のパネルから [非公開ネットワーク (Private Networks)] をクリックします。
- 2 有効にするネットワークをクリックします。
- 3 [有効化 (Enable)] アイコン () をクリックします。

選択したネットワークが有効になります。

プライベート ネットワークを無効にする

プライベート ネットワークを無効にすると、リモート ユーザーは SSL VPN-Plus を介してそのネットワークにアクセスできなくなります。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [非公開ネットワーク (Private Networks)] をクリックします。
- 2 無効にするネットワークをクリックします。
- 3 [無効化 (Disable)] () アイコンをクリックします。




選択したネットワークが無効になります。

プライベート ネットワークの順序の変更

SSL VPN-Plus では、リモート ユーザーがプライベート ネットワーク パネルに表示されている順番でプライベート ネットワークにアクセスすることを許可します。

プライベート ネットワークに [TCP 最適化の有効化] を選択すると、アクティブ モードの FTP など、一部のアプリケーションがサブネット内で機能しない場合があります。アクティブ モードで設定されている FTP サーバを追加するには、その FTP サーバに、TCP 最適化を無効にして別のプライベート ネットワークを追加する必要があります。また、アクティブな TCP プライベート ネットワークを有効にし、サブネット プライベート ネットワークの上に置く必要もあります。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [非公開ネットワーク] をクリックします。
- 2 [順序の変更] () アイコンをクリックします。
- 3 順序を変更するネットワークを選択します。
- 4 [上へ移動] () または [下へ移動] () アイコンをクリックします。
- 5 [OK] をクリックします。

インストール パッケージの操作


SSL クライアントのインストール パッケージを削除または編集できます。

インストール パッケージの作成の詳細については、「[ネットワーク アクセス SSL VPN-Plus の設定](#)」または「[Web Access SSL VPN-Plus の設定](#)」を参照してください。

インストール パッケージの編集

インストール パッケージを編集できます。


手順

- 1 [SSL VPN-Plus] タブの左側のパネルで、[インストール パッケージ (Installation Package)] をクリックします。
- 2 編集するインストール パッケージを選択します。
- 3 [編集] () アイコンをクリックします。
[インストール パッケージの編集] ダイアログ ボックスが開きます。
- 4 必要に応じて編集します。
- 5 [OK] をクリックします。

インストール パッケージの削除

インストール パッケージを削除できます。

手順

- 1 [SSL VPN-Plus] タブの左側のパネルで、[インストール パッケージ (Installation Package)] をクリックします。
- 2 削除するインストール パッケージを選択します。
- 3 [削除 (Delete)] () アイコンをクリックします。

ユーザーの操作


ローカル データベースのユーザーを編集、または削除できます。

ユーザーの追加の詳細については、「[ネットワーク アクセス SSL VPN-Plus の設定](#)」または「[Web Access SSL VPN-Plus の設定](#)」を参照してください。

ユーザーの編集

ユーザー ID を除くユーザーの詳細を編集できます。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ユーザー (Users)] をクリックします。
- 2 [編集 (Edit)] () アイコンをクリックします。
- 3 必要に応じて編集します。
- 4 [OK] をクリックします。

ユーザーの削除

ユーザーを削除できます。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ユーザー (Users)] をクリックします。
- 2 [構成 (Configure)] パネルの [ユーザー (Users)] で、[ユーザー (Users)] をクリックします。
- 3 削除するユーザーを選択し、[削除 (Delete)] () アイコンをクリックします。

ユーザーのパスワードの変更

ユーザーのパスワードを変更できます。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ユーザー (Users)] をクリックします。
- 2 [パスワードの変更 (Change Password)] アイコンをクリックします。
- 3 新しいパスワードを入力してから再入力します。
- 4 ユーザーが次にシステムにログインするときにパスワードを変更するには、[次のログイン時にパスワードを変更] をクリックします。
- 5 [OK] をクリックします。


ログインおよびログオフ スクリプトの操作

ログインまたはログオフ スクリプトを NSX Edge Gateway にバインドできます。

スクリプトの編集

NSX Edge Gateway にバインドされたログインまたはログオフ スクリプトのタイプ、説明、およびステータスは、編集することができます。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] をクリックします。
- 2 スクリプトを選択して、[編集 (Edit)] () アイコンをクリックします。
- 3 適切に変更します。
- 4 [OK] をクリックします。

スクリプトの削除

ログインまたはログオフ スクリプトを削除できます。


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] をクリックします。
- 2 スクリプトを選択して、[削除 (Delete)] () アイコンをクリックします。

スクリプトを有効にする

スクリプトを実行するには、有効にする必要があります


手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] をクリックします。
- 2 スクリプトを選択して、[有効化 (Enable)] () アイコンをクリックします。

スクリプトを無効にする

ログイン/ログオフ スクリプトを無効にすることができます。



手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] をクリックします。
- 2 スクリプトを選択して、[無効化 (Disable)] () アイコンをクリックします。

スクリプトの順序の変更

スクリプトの順序を変更できます。たとえば、Internet Explorer で gmail.com を開くログイン スクリプトを、yahoo.com を開くログイン スクリプトの上に配置してあるとします。リモート ユーザーが SSL VPN にログインすると、yahoo.com の前に gmail.com が表示されます。ログイン スクリプトの順序を逆にすると、gmail.com の前に yahoo.com が表示されるようになります。

手順

- 1 [SSL VPN-Plus] タブで、左側のパネルから [ログイン/ログオフ スクリプト (Login/Logoff Scripts)] をクリックします。
- 2 順序を変更するスクリプトを選択し、[上へ移動 (Move Up)] () または [下へ移動 (Move Down)] () アイコンをクリックします。
- 3 [OK] をクリックします。

IPSec VPN の概要

NSX Edge は NSX Edge インスタンスとリモート サイトとのサイト間 IPSec VPN をサポートします。NSX Edge インスタンスとリモート VPN ルーター間での証明書認証、プリシェアード キー モード、IP ユニキャスト トラフィック、および非動的ルーティング プロトコルがサポートされています。

各リモート VPN ルーターの背後では、IPSec トンネル経由で NSX Edge の背後の内部ネットワークに接続するための複数のサブネットを構成できます。

注: NSX Edge の背後にあるサブネットと内部ネットワークはアドレス範囲がお互い重ならないようにします。

IPsec VPN のローカル ピアとリモート ピアで IP アドレスが重なっている場合、ローカル接続のルートと自動接続のルートが存在するかどうかによって、トンネルを経由して転送されるトラフィックの整合性が維持されない可能性があります。

NAT デバイスの背後に NSX Edge エージェントをデプロイできます。このデプロイでは、NAT デバイスは NSX Edge インスタンスの 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 ルーターはこのパブリック アドレスを使用して NSX Edge インスタンスにアクセスします。

リモート VPN ルーターを NAT デバイスの背後に設置することもできます。トンネルをセットアップするには、VPN のネイティブ アドレスと VPN ゲートウェイ ID が必要です。両端では、VPN アドレスのために静的な一対一の NAT が要求されます。

必要なトンネルの数は、ローカル サブネットの数にピア サブネットの数を掛けて求められます。たとえば、10 個のローカル サブネットと 10 個のピア サブネットがある場合、100 個のトンネルが必要です。サポートされるトンネルの最大数は、下記に示すように ESG のサイズによって決まります。

表 14-11. ESG あたりの IPSec トンネルの数

ESG	IPSec トンネルの数
Compact	512
Large	1600

表 14-11. ESG あたりの IPSec トンネルの数 (続き)

ESG	IPSec トンネルの数
Quad-Large	4096
X-Large	6000

次の IPSec VPN アルゴリズムがサポートされています。

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie-Hellman グループ 2)
- DH-5 (Diffie-Hellman グループ 5)

IPSec VPN の設定については、章 24 「NSX Edge VPN 構成例」を参照してください。

IPSec VPN のトラブルシューティングについては、<https://kb.vmware.com/kb/2123580> を参照してください。

IPSec VPN サービスの設定

ローカル サブネットとピア サブネットとの間の NSX Edge トンネルを設定できます。

注: IPSec VPN 経由でリモート サイトに接続すると、Edge アップリンク上の動的ルーティングはそのサイトの IP アドレスを学習できません。

1 IPSec VPN サービスを有効にする

ローカル サブネットからピア サブネットにトラフィックが流れるようにするには、IPSec VPN サービスを有効にする必要があります。

2 OpenSSL を使用した IPSec VPN 用の CA 署名証明書の生成

IPSec 用の証明書認証を有効にするには、サーバ証明書と対応する CA 署名証明書をインポートする必要があります。または、OpenSSL などのオープンソースのコマンドライン ツールを使用して CA 署名証明書を生成することもできます。

3 グローバル IPSec VPN 設定の指定

これにより、NSX Edge インスタンス上で IPSec VPN が有効になります。

4 IPSec VPN のログの有効化

すべての IPSec VPN トラフィックのログを有効にできます。

5 IPSec VPN パラメータの設定

IPSec VPN サービスを提供するには、NSX Edge で少なくとも 1 つの外部 IP アドレスを設定する必要があります。

IPSec VPN サービスを有効にする

ローカル サブネットからピア サブネットにトラフィックが流れるようにするには、IPSec VPN サービスを有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 [有効化 (Enable)] をクリックします。

OpenSSL を使用した IPSec VPN 用の CA 署名証明書の生成

IPSec 用の証明書認証を有効にするには、サーバ証明書と対応する CA 署名証明書をインポートする必要があります。または、OpenSSL などのオープンソースのコマンドライン ツールを使用して CA 署名証明書を生成することもできます。

前提条件

OpenSSL がインストールされている必要があります。

手順

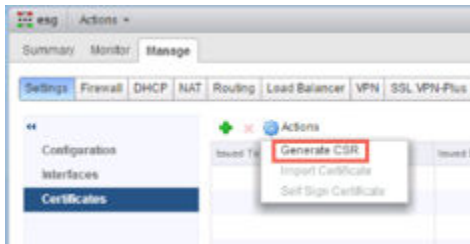
- 1 OpenSSL がインストールされた Linux または Mac マシンで、`/opt/local/etc/openssl/openssl.cnf` ファイルまたは `/System/Library/OpenSSL/openssl.cnf` ファイルを開きます。
- 2 `dir = .` であることを確認します。
- 3 次のコマンドを実行します。

```
mkdir newcerts
mkdir certs
mkdir req
mkdir private
echo "01" > serial
touch index.txt
```

- 4 次のコマンドを実行して CA 署名証明書を生成します。

```
openssl req -new -x509 -newkey rsa:2048 -keyout private/cakey.pem -out cacert.pem -days 3650
```

- 5 NSX Edge1 で証明書署名要求 (CSR) を生成し、Privacy Enhanced Mail (PEM) ファイルの内容をコピーし、**req/edge1.req** ファイルとして保存します。



「[CA 署名証明書の設定](#)」を参照してください。

- 6 次のコマンドを実行して証明書署名要求に署名します。

```
sudo openssl ca -policy policy_anything -out certs/edge1.pem -in req/edge1.req
```

- 7 NSX Edge2 で CSR を生成し、PEM ファイルの内容をコピーし、**req/edge2.req** ファイルとして保存します。

- 8 次のコマンドを実行して証明書署名要求に署名します。

```
sudo openssl ca -policy policy_anything -out certs/edge2.pem -in req/edge2.req
```

- 9 **certs/edge1.pem** ファイルの最後にある PEM 証明書を Edge1 にアップロードします。
- 10 **certs/edge2.pem** ファイルの最後にある PEM 証明書を Edge2 にアップロードします。
- 11 **cacert.pem** ファイルの CA 証明書を Edge1 および Edge2 に CA 署名証明書としてアップロードします。
- 12 Edge1 および Edge2 の IPsec グローバル設定で、アップロードした PEM 証明書とアップロードした CA 証明書を選択し、設定を保存します。
- 13 [証明書 (Certificate)] タブで、アップロードした証明書をクリックして DN 文字列を記録します。
- 14 DN 文字列を **C=IN,ST=ka,L=b1r,O=bmware,OU=vmware,CN=edge2.eng.vmware.com** の形式に戻し、Edge1 および Edge2 用に保存します。
- 15 ローカル ID とピア ID を指定形式の識別名 (DN) 文字列として使用して、Edge1 および Edge2 で IPsec VPN サイトを作成します。

[IPsec 統計の表示 (Show IPsec Statistics)] をクリックしてステータスを確認します。チャンネルをクリックしてトンネルステータスを表示します。チャンネルとトンネルステータスの両方が緑色になっている必要があります。

グローバル IPsec VPN 設定の指定

これにより、NSX Edge インスタンス上で IPsec VPN が有効になります。

前提条件

証明書認証を有効にするには、サーバ証明書および対応する CA 署名の証明書をインポートする必要があります。または、OpenSSL などのオープンソースのコマンドラインツールを使用して CA 署名証明書を生成することもできます。

自己署名証明書は IPSec VPN には使用できません。これらは、ロード バランシングと SSL VPN にしか使用できません。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 [グローバル設定ステータス] の横にある [変更 (Change)] をクリックします。
- 7 ピア エンドポイントが「任意」に設定されているサイトのグローバル プリシェアード キーを入力し、[シェアード キーの表示 (Display shared key)] を選択してキーを表示します。
- 8 [証明書認証の有効化] を選択し、該当する証明書を選択します。
- 9 [OK] をクリックします。

IPSec VPN のログの有効化

すべての IPSec VPN トラフィックのログを有効にできます。

デフォルトでは、ログが有効になり、「警告」レベルに設定されます。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 ローカル サブネットとピア サブネット間のトラフィック フローをログに記録してログ レベルを選択するには、[ログ ポリシー] の横の  をクリックして、[ログの有効化] をクリックします。
- 7 ログ レベルを選択して、[変更の発行] をクリックします。

IPSec VPN パラメータの設定

IPSec VPN サービスを提供するには、NSX Edge で少なくとも 1 つの外部 IP アドレスを設定する必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックします。
- 7 IPSec VPN の名前を入力します。
- 8 NSX Edge インスタンスの IP アドレスを [ローカル ID (Local Id)] に入力します。これは、リモート サイトのピア ID となります。
- 9 ローカル エンドポイントの IP アドレスを入力します。
プリシェアード キーを使用して IP トンネルに IP を追加する場合は、ローカル ID とローカル エンドポイント IP が同じになる可能性があります。
- 10 CIDR フォーマットで、サイト間で共有するサブネットを入力します。複数のサブネットを入力するには、コンマ区切りを使用します。
- 11 ピア サイトを一意に識別するためにピア ID を入力します。証明書認証を使用するピアの場合、この ID はピアの証明書の共通名である必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。VMware では、VPN のパブリック IP アドレス、または VPN サービスの FQDN をピア ID として使用することをお勧めしています。
- 12 ピア サイトの IP アドレスを [ピア エンドポイント] に入力します。ここを空白のままにしておくと、NSX Edge はピア デバイスの接続リクエストまで待機します。
- 13 ピア サブネットの内部 IP アドレスを CIDR フォーマットで入力します。複数のサブネットを入力するには、コンマ区切りを使用します。
- 14 暗号化アルゴリズムを選択します。
- 15 [認証方法] で、次のいずれかを選択します。

オプション	説明
PSK (Pre Shared Key)	このオプションを選択すると、NSX Edge とピア サイトが共有する秘密鍵が認証に使用されます。秘密鍵は、最大長が 128 バイトの文字列です。
証明書	このオプションを選択すると、グローバル レベルで定義された証明書が認証に使用されます。

- 16 匿名サイトが VPN サービスに接続する場合は、共有鍵を入力します。
- 17 [シェアード キーの表示 (Display Shared Key)] をクリックし、ピア サイト上に鍵を表示します。
- 18 [Diffie-Hellman (DH) グループ] で、ピア サイトと NSX Edge が安全でない通信チャンネル上で共有シークレットを確立できるようにする暗号化スキームを選択します。

19 [エクステンション] に次のいずれかを入力します。

- `securelocaltrafficbyip=<IPAddress>` : Edge のローカル トラフィックを IPSec VPN トンネル経由でリダイレクトします。デフォルトの値は、次のとおりです。
- `passthroughSubnets=<PeerSubnetIPAddress>` : サブネットの重複をサポートします。

20 [OK] をクリックします。

NSX Edge で、ローカル サブネットからピア サブネットへのトンネルが作成されます。

次のステップ

IPSec VPN サービスを有効にします。

IPsec VPN サービスの編集

IPsec VPN サービスを編集できます。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 編集する IPSec サービスを選択します。
- 7 [編集 (Edit)] (✎) アイコンをクリックします。
- 8 適切に編集します。
- 9 [OK] をクリックします。

IPSec サービスを無効にする

IPSec サービスを無効にすることができます。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。

- 6 無効にする IPSec サービスを選択します。
- 7 [無効化 (Disable)] () アイコンをクリックします。

IPSec サービスの削除

IPSec サービスを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 削除する IPSec サービスを選択します。
- 7 [削除 (Delete)] () アイコンをクリックします。

L2 VPN の概要

L2 VPN では、2 つのサイト間のトンネルを設定できます。仮想マシンはこれらのサイト間を移動しても同じサブネット上にあるため、データセンターを拡張できます。一方のサイトの NSX Edge から他方のサイトの仮想マシンにすべてのサービスを提供できます。

L2 VPN トンネルを作成するには、L2 VPN サーバと L2 VPN クライアントを設定します。

L2 VPN の設定

L2 VPN を使用してネットワークを拡張するには、L2 VPN サーバ (ターゲット Edge) と L2 VPN クライアント (ソース Edge) を構成します。次に、サーバとクライアントの両方で L2 VPN サービスを有効にする必要があります。

前提条件

サブインターフェイスが NSX Edge のトランク インターフェイスに追加されている必要があります。[「サブインターフェイスの追加」](#)を参照してください。

手順

1 [L2 VPN のベスト プラクティス](#)

ベスト プラクティスに従って L2 VPN を設定することで問題 (ルーピング、ping と応答の重複など) を回避できます。

2 [L2 VPN サーバの設定](#)

L2 VPN サーバは、クライアントの接続先であるターゲット NSX Edge です。

3 ピア サイトの追加

複数のサイトを L2 VPN サーバに接続できます。

4 サーバ上で L2 VPN サービスを有効にする

L2 VPN サービスを L2 VPN サーバ（ターゲット NSX Edge）で有効にする必要があります。この Edge アプライアンスで高可用性が構成済みの場合は、Edge に複数の内部インターフェイスが設定されていることを確認します。インターフェイスが 1 つしかなく、高可用性によって既に使用されている場合は、同じ内部インターフェイス上での L2 VPN の設定に失敗します。

5 L2 VPN クライアントの設定

L2 VPN クライアントは、ターゲット Edge（L2 VPN サーバ）との通信を開始する送信元 NSX Edge です。

6 クライアント上で L2 VPN サービスを有効にする

L2 VPN サービスを L2 VPN クライアント（ソース NSX Edge）で有効にする必要があります。

L2 VPN のベスト プラクティス

ベスト プラクティスに従って L2 VPN を設定することで問題（ルーピング、ping と応答の重複など）を回避できます。

ルーピングを軽減するための L2VPN のオプション

ルーピングを軽減するには、2 つのオプションがあります。NSX Edge と仮想マシンを別々の ESXi ホストに配置するか、NSX Edge と仮想マシンを同じ ESXi ホストに配置するかです。

■ オプション 1：L2VPN Edge と仮想マシンを個別の ESXi ホストに配置する場合

- a Edge と仮想マシンを個別の ESXi ホストでデプロイします。
- b Edge の TRUNK vNic に関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
 - 1 ロード バランシングを「発信元の仮想ポートに基づいたルート」にします。
 - 2 1 つのアップリンクのみをアクティブとして、他のアップリンクをスタンバイとして設定します。
- c 仮想マシンに関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
 - 1 任意のチーミング ポリシーを使用できます。
 - 2 複数のアクティブ アップリンクを設定できます。
- d シンク ポート モードを使用して TRUNK vNic で無差別モードを無効にするように Edge を設定します。

■ オプション 2：Edge と仮想マシンを同じ ESXi ホストに配置する場合

- a Edge の TRUNK vNic に関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
 - 1 ロード バランシングを「発信元の仮想ポートに基づいたルート」にします。
 - 2 1 つのアップリンクをアクティブとして、他のアップリンクをスタンバイとして設定します。

- b 仮想マシンに関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
 - 1 任意のチーミング ポリシーを使用できます。
 - 2 アクティブにできるアップリンクは 1 つだけです。
 - 3 アクティブ/スタンバイのアップリンクの順序は仮想マシンの分散ポート グループおよび Edge の TRUNK vNic 分散ポート グループと同じである必要があります。
- c シンク ポート モードを使用して TRUNK vNic で無差別モードを無効にするようにクライアント側のスタンドアロン Edge を設定します。

シンク ポートの設定

NSX で管理する NSX Edge を L2 VPN クライアントとしてセットアップすると、一部の設定が NSX によって自動的に実行されます。スタンドアロン NSX Edge を L2 VPN クライアントとしてセットアップする場合、この設定手順を手動で行う必要があります。

VPN サイトのいずれかに NSX がデプロイされていない場合、そのサイトにスタンドアロンの NSX Edge をデプロイすることで L2 VPN を設定できます。スタンドアロン Edge は、OVF ファイルを使用してデプロイされます。NSX で管理されていないホストでデプロイされ、L2 VPN クライアントとして機能するための Edge ゲートウェイとなります。

スタンドアロン Edge のトランク vNIC を vSphere Distributed Switch に接続する場合、L2 VPN 機能用に無差別モードまたはシンク ポートが必要になります。無差別モードを使用すると、ping が重複するために応答も重複する可能性があります。そのため、L2 VPN のスタンドアロン NSX Edge の設定ではシンク ポート モードを使用することをお勧めします。

前提条件

スタンドアロン Edge のトランク vNIC のポート番号が必要です。

手順

- 1 dvsUuid 値を取得します。
 - a <https://<vc-ip>/mob?vmodl=1> にアクセスし、vCenter Server 管理対象オブジェクト ブラウザ (MOB) ユーザー インターフェイスに移動します。
 - b [内容 (content)] 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。

2 vCenter Server MOB の selectionSet を変更します。

- a `https://<vc-ip>/mob?vmodl=1` にログインし、vCenter Server MOB ユーザー インターフェイスにログインします。
- b [内容 (content)] をクリックします。
- c [DVSManger] をクリックします。
- d [updateOpaqueDataEx] をクリックします。
- e [selectionSet] 値ボックスに次の XML ブロックを貼り付けます。

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!--example
only-->
  <portKey>393</portKey> <!--port number of the DVPG where SINK to be set-->
</selectionSet>
```

vCenter Server MOB から取得した dvsUuid 値を使用します。

- f opaqueDataSpec 値ボックスで、次の XML ブロックのいずれかを貼り付けます。

シンク ポートを有効にする場合：

```
<opaqueDataSpec>  
    <operation>edit</operation>  
    <opaqueData>  
        <key>com.vmware.etherswitch.port.extraEthFRP</key>  
        <opaqueData  
xsi:type="vmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA= </opaqueData>  
        </opaqueData>  
</opaqueDataSpec>
```

シンク ポートが無効にする場合：

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmidl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
    </opaqueData>
  </opaqueDataSpec>
```

- g isRuntime ブール値を [false] に設定します。
- h [Invoke Method]をクリックします。

L2 VPN サーバの設定

L2 VPN サーバは、クライアントの接続先であるターゲット NSX Edge です。

手順

- 1 [L2 VPN] タブで、[サーバ (Server)] を選択し、[変更 (Change)] をクリックします。
- 2 [リスナ IP (Listener IP)] で、NSX Edge の外部インターフェイスのプライマリまたはセカンダリ IP アドレスを入力します。
- 3 L2 VPN サービスのデフォルト ポートは 443 です。必要に応じてこのポートを編集します。
- 4 サーバとクライアント間の通信のための暗号化アルゴリズムを選択します。
- 5 SSL VPN サーバにバインドする証明書を選択します。
- 6 [OK] をクリックします。

ピア サイトの追加

複数のサイトを L2 VPN サーバに接続できます。

注: サイトの設定を変更すると、NSX Edge は既存の接続をすべて切断して、再接続します。

手順

- 1 [L2 VPN] タブで、[L2 VPN モード (L2 VPN Mode)] が [サーバ (Server)] になっていることを確認します。
- 2 [サイト構成の詳細 (Site Configuration Details)] で、[追加 (Add)] アイコンをクリックします。
- 3 ピア サイトの一意の名前を入力します。
- 4 ピア サイトの認証に使用するユーザー名とパスワードを入力します。ピア サイトのユーザー認証情報は、クライアント側と同じである必要があります。
- 5 [拡張されたインターフェイス (Stretched Interfaces)] で、[サブインターフェイスの選択 (Select Sub Interfaces)] をクリックし、クライアントで拡張されるサブ インターフェイスを選択します。
 - a [オブジェクトの選択] で、Edge のトランク インターフェイスを選択します。

トランク vNIC で設定されたサブ インターフェイスが表示されます。
 - b 拡張するサブ インターフェイスをダブルクリックします。
 - c [OK] をクリックします。
- 6 2 つのサイトで仮想マシンのデフォルト ゲートウェイが同じ場合、トラフィックをローカルにルーティングする、またはトラフィックをトンネルでブロックするゲートウェイ IP アドレスを [出力側を最適化するゲートウェイ アドレス (Egress Optimization Gateway Address)] に入力します。
- 7 [OK] をクリックして、[変更の発行 (Publish Changes)] をクリックします。

サーバ上で L2 VPN サービスを有効にする

L2 VPN サービスを L2 VPN サーバ（ターゲット NSX Edge）で有効にする必要があります。この Edge アプライアンスで高可用性が構成済みの場合は、Edge に複数の内部インターフェイスが設定されていることを確認します。インターフェイスが 1 つしかなく、高可用性によって既に使用されている場合は、同じ内部インターフェイス上での L2 VPN の設定に失敗します。

手順

- 1 ターゲット NSX Edge の場合は、[管理 (Manage)] - [VPN] - [L2 VPN] の順に移動します。
- 2 [L2VPN サービス設定 (L2VPN Service Configuration)] で、[有効化 (Enable)] をクリックします。

次のステップ

インターネット側のファイアウォールで NAT またはファイアウォール ルールを作成して、クライアントとサーバが相互に接続できるようにします。

L2 VPN クライアントの設定

L2 VPN クライアントは、ターゲット Edge（L2 VPN サーバ）との通信を開始する送信元 NSX Edge です。

スタンドアロン Edge を L2 VPN クライアントとして設定することもできます。[「スタンドアロン Edge を L2 VPN クライアントとして設定する」](#)を参照してください。

手順

- 1 [L2 VPN] タブで、[L2 VPN モード (L2 VPN Mode)] を [クライアント (Client)] に設定して、[変更 (Change)] をクリックします。
- 2 このクライアントが接続する L2 VPN サーバのアドレスを入力します。アドレスは、ホスト名または IP アドレスになります。
- 3 必要に応じて、L2 VPN クライアントの接続先となるデフォルト ポートを編集します。
- 4 サーバとの通信のための暗号化アルゴリズムを選択します。
- 5 [拡張されたインターフェイス (Stretched Interfaces)] で、[サブインターフェイスの選択 (Select Sub Interfaces)] をクリックして、サーバに拡張されるサブ インターフェイスを選択します。
 - a [オブジェクトの選択 (Select Object)] で、Edge のトランク インターフェイスを選択します。
トランク vNIC で設定されたサブ インターフェイスが表示されます。
 - b 拡張するサブ インターフェイスをダブルクリックします。
 - c [OK] をクリックします。
- 6 説明を入力します。
- 7 [出力側を最適化するゲートウェイ アドレス (Egress Optimization Gateway Address)] に、サブ インターフェイスのゲートウェイ IP アドレス、またはトラフィックがトンネル経由でフローされない IP アドレスを入力します。
- 8 [ユーザー詳細 (User Details)] で、サーバで認証されるためのユーザー認証情報を入力します。

9 [詳細 (Advanced)] タブをクリックします。

インターネットに直接アクセスできないクライアント NSX Edge がプロキシ サーバ経由でソース (サーバ) NSX Edge にアクセスする必要がある場合、[プロキシ設定 (Proxy Settings)] を指定します。

10 セキュアなプロキシ接続のみを有効にするには、[セキュア プロキシの有効化 (Enable Secure Proxy)] を選択します。

11 プロキシ サーバのアドレス、ポート、ユーザー名、およびパスワードを入力します。

12 サーバ証明書の検証を有効にするには、[サーバ証明書の検証 (Validate Server Certificate)] を選択し、適切な CA 証明書を選択します。

13 [OK] をクリックして、[変更の発行 (Publish Changes)] をクリックします。

次のステップ

ファイアウォールに接するインターネットで、L2 VPN Edge からインターネットへのトラフィックのフローが許可されていることを確認します。宛先ポートは 443 です。

クライアント上で L2 VPN サービスを有効にする

L2 VPN サービスを L2 VPN クライアント (ソース NSX Edge) で有効にする必要があります。

手順

1 ソース NSX Edge の場合は、[管理 (Manage)] - [VPN] - [L2 VPN] の順に移動します。

2 [L2VPN サービス設定 (L2VPN Service Configuration)] で、[有効化 (Enable)] をクリックします。

次のステップ

- インターネット側のファイアウォールで NAT またはファイアウォール ルールを作成して、クライアントとサーバが相互に接続できるようにします。
- 標準のポートグループによってバックアップされている trunk vNIC を拡張する場合は、次の手順に従って L2 VPN トラフィックを手動で有効にします。
 - a [無差別モード (Promiscuous mode)] を [許可 (Accept)] に設定します。
 - b [偽装転送 (Forged Transmits)] を [許可 (Accept)] に設定します。

詳細については、ESXi および vCenter Server 5.5 のドキュメントを参照してください。

スタンドアロン Edge を L2 VPN クライアントとして設定する

拡張するサイトの 1 つが NSX によってバックアップされていない場合は、スタンドアロン Edge を L2 VPN クライアントとしてそのサイトにデプロイできます。

前提条件

接続先のスタンドアロン Edge のトランク インターフェイス用のトランク ポート グループは作成されています。このポート グループの一部の設定を手動で行う必要があります。

- トランク ポート グループが vSphere Standard スイッチ上にある場合、以下の操作を行う必要があります。

- 偽装転送を有効にする
- 無差別モードを有効にする

『vSphere ネットワーク ガイド』を参照してください。

- トランク ポート グループが vSphere Distributed Switch 上にある場合、以下の操作を行う必要があります。

- 偽装転送を有効にする。『vSphere ネットワーク ガイド』を参照してください。
- トランク vNIC のシンク ポートを有効にするか、無差別モードを有効にする。シンク ポートを有効にすることを強くお勧めします。

スタンドアロン Edge をデプロイした後、シンク ポートの設定を行う必要があります。Edge のトランク vNIC に接続したポートの設定を変更する必要があるためです。

手順

- 1 vSphere Web Client を使用して、非 NSX 環境を管理している 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 スタンドアロン 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、スタンドアロン 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 [OVF テンプレートの詳細] ページで、テンプレートの詳細を確認して、[次へ] をクリックします。
- 6 [名前およびフォルダの選択] ページで、スタンドアロン Edge の名前を入力して、デプロイ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。
- 7 [ストレージの選択] ページで、デプロイするテンプレートのファイルを格納する場所を選択します。
- 8 [ネットワークの選択] ページで、デプロイ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。[次へ] をクリックします。
 - パブリック インターフェイスがアップリンク インターフェイスです。
 - トランク インターフェイスを使用して、拡張するネットワークのサブインターフェイスを作成します。このインターフェイスを、作成したトランク ポート グループに接続します。
- 9 [テンプレートのカスタマイズ] ページで、次の値を指定します。
 - a CLI の admin パスワードを入力および再入力します。
 - b CLI を有効にするためのパスワードを入力および再入力します。
 - c CLI の root パスワードを入力および再入力します。

- d アップリンク IP アドレスと、プリフィックスの長さを入力し、オプションでデフォルト ゲートウェイと DNS IP アドレスを入力します。
- e 認証に使用する暗号を選択します。これは、L2VPN サーバで使用する暗号と一致する必要があります。
- f 出力側の最適化を有効にするには、トラフィックがローカルにルーティングされるゲートウェイ IP アドレス、つまりトラフィックがトンネルを介してブロックされるゲートウェイ IP アドレスを入力します。
- g L2 VPN サーバ アドレスとポートを入力します。
- h ピア サイトの認証に使用するユーザー名とパスワードを入力します。
- i サブインターフェイスの VLAN (トンネル ID) に、拡張するネットワークの VLAN ID を入力します。VLAN ID は、カンマ区切りのリストまたは範囲として指定できます。たとえば、2,3,10-20 のように指定します。

ネットワークをスタンドアロン Edge サイトに拡張する前に、そのネットワークの VLAN ID を変更する場合は、ネットワークの VLAN ID、次に括弧で囲んだトンネル ID を入力します。たとえば、2(100),3(200) のように入力します。トンネル ID は、拡張されるネットワークをマッピングするために使用されます。ただし、トンネル ID は範囲として指定できません。つまり、10(100)-14(104) のようには指定できません。これは、10(100),11(101),12(102),13(103),14(104) に変更する必要があります。
- j インターネットに直接アクセスできない NSX Edge がプロキシ サーバ経由でソース (サーバ) NSX Edge にアクセスする必要がある場合は、プロキシ アドレス、ポート、ユーザー名、およびパスワードを入力します。
- k ルート CA を利用できる場合は、それを [証明書] セクションに貼り付けることができます。
- l [次へ] をクリックします。

10 [設定内容の確認] ページでスタンドアロン Edge 設定を確認して、[終了] をクリックします。

次のステップ

スタンドアロン Edge 仮想マシンをパワーオンします。

トランク vNIC のポート番号をメモし、シンク ポートを設定します。[\[シンク ポートの設定\]](#) を参照してください。

スタンドアロン Edge のコマンドライン インターフェイスを使用して、その他の設定を変更します。『NSX 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。

L2 VPN 統計の表示

L2 VPN 統計情報 (トンネル ステータス、送受信されたバイト数など) を、NSX Edge のソースおよびターゲットに関して表示できます。

手順

- 1 [L2 VPN] タブで、次のように操作します。[L2 VPN モード (L2 VPN Mode)] が [クライアント (Client)] であることを確認します。
- 2 [ステータスの取得 (Fetch Status)] をクリックし、[トンネル ステータス (Tunnel Status)] を展開します。

L2 VPN サーバに複数のピア サイトがある場合、すべてのピア サイトの統計情報が表示されます。

次のステップ

トランク インターフェイス上に設定されたネットワークを表示するには、Edge の [管理 (Manage)] - [設定 (Settings)] - [インターフェイス (Interfaces)] に移動し、[タイプ] 列の [トランク (Trunk)] をクリックします。

論理ロード バランサ

NSX Edge ロード バランサは、高可用性サービスにより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。受信サービス リクエストは、負荷配分がユーザーにとって透過的になるように、複数のサーバ間で均等に配分されます。このように、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。NSX Edge は、レイヤー 7 までのロード バランシングを提供します。

ロード バランシングのために、外部（またはパブリック）IP アドレスを内部サーバのセットにマッピングします。ロード バランサは外部 IP アドレスによる TCP、UDP、HTTP、または HTTPS リクエストを受け入れ、どの内部サーバを使用するか決定します。ポート 80 は HTTP のデフォルト ポートであり、ポート 443 は HTTPS のデフォルト ポートです。

ロード バランシングを行う前に、NSX Edge インスタンスが動作している必要があります。NSX Edge のセット アップの詳細については、[「NSX Edge 設定」](#)を参照してください。

NSX Edge 証明書の設定に関する詳細については、[「証明書の操作」](#)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。

- [ロード バランシングの設定](#)
- [アプリケーション プロファイルの管理](#)
- [サービス モニターの管理](#)
- [サーバ プールの管理](#)
- [仮想サーバの管理](#)
- [アプリケーション ルールの管理](#)
- [NTLM 認証を使用する Web サーバのロード バランシング](#)
- [NSX ロード バランサ構成のシナリオ](#)

ロード バランシングの設定

NSX Edge ロード バランサは、ネットワーク トラフィックを複数のサーバに分散して最適ナリソース使用を実現します。

NSX ロード バランサは、レイヤー 4 およびレイヤー 7 のロード バランシング エンジンをサポートします。レイヤー 4 のロード バランサはパケット ベースであり、レイヤー 7 のロード バランサはソケット ベースです。

パケットベースのロードバランシングは、TCP および UDP レイヤーに実装されます。パケットベースのロードバランシングは、接続の停止や要求全体のバッファの作成は行わず、代わりにパケット処理後に選択されたサーバに直接パケットを送信します。TCP および UDP セッションはロードバランサで維持され、これによって単一セッションのパケットが同一サーバに送信されます。グローバル設定と関連する仮想サーバの設定の両方で [アクセラレーションの有効化] を選択することで、パケットベースのロードバランシングを有効にできます。

ソケットベースのロードバランシングは、ソケットインターフェイスの上位に実装されます。1つの要求について、クライアント方向とサーバ方向の2つの接続が確立されます。サーバ方向の接続は、サーバを選択した後に確立されます。HTTP ソケットベースの実装では、オプションの L7 処理を使用して選択されたサーバに送信される前に、すべての要求が受信されます。HTTPS ソケットベースの実装については、クライアント方向の接続またはサーバ方向の接続のいずれかで、認証情報が交換されます。ソケットベースのロードバランシングは、TCP、HTTP、および HTTPS 仮想サーバのデフォルトのモードです。

NSX ロードバランサの主なコンポーネントは、仮想サーバ、サーバプール、サーバプールメンバー、およびサービスモニターです。

仮想サーバ	アプリケーションサービスを抽象化したもので、IP アドレス、ポート、およびプロトコル (TCP、UDP など) の一意の組み合わせを持ちます。
サーバプール	バックエンドサーバのグループです。
サーバプールメンバー	プール内のメンバーとしてのバックエンドサーバです。
サービスモニター	バックエンドサーバの健全性ステータスの検証方法を定義します。

最初に、ロードバランサのグローバルオプションを設定します。バックエンドサーバメンバーが含まれるサーバプールを作成し、サービスモニターをプールに関連付けてバックエンドサーバを効率的に管理し、共有します。

次に、アプリケーションプロファイルを作成して、クライアント SSL、サーバ SSL、x-forwarded-for、パーシステンスなど、アプリケーションの共通の動作をロードバランサに定義します。パーシステンスを設定すると、ソース IP アドレスや Cookie などの特性が類似する後続の要求は、ロードバランシングアルゴリズムを実行せずに、同じプールメンバーに送信されます。アプリケーションプロファイルは、仮想サーバ全体で再利用できます。

次に、オプションのアプリケーションルールを作成して、アプリケーション固有のトラフィック処理を設定します。たとえば、特定の URL やホスト名との一致により、異なる要求を異なるプールで処理するように定義します。次に、サービスモニターを作成して、ロードバランサの健全性チェックパラメータを定義します。

仮想サーバが要求を受信するとき、ロードバランシングアルゴリズムではプールメンバーの設定とランタイムステータスが考慮されます。次に、アルゴリズムは適切なプールを計算して、1つ以上のメンバーにトラフィックを分散します。プールメンバーの設定には、重み、最大接続数、状態ステータスなどの設定が含まれます。ランタイムステータスには、現在の接続、応答時間、健全性チェックのステータス情報などが含まれます。計算方法としては、ラウンドロビン、加重ラウンドロビン、最小接続数、またはソース IP ハッシュが使用されます。

各プールは、関連付けられたサービスモニターで監視されます。ロードバランサがプールメンバーの問題を検出すると、メンバーの状態は「切断」とマークされます。サーバプールからプールメンバーを選択するときには、状態が「接続中」のサーバのみが選択されます。サーバプールにサービスモニターが設定されていない場合は、すべてのメンバーが「接続中」とであるとみなされます。

■ ロードバランササービスの設定

ロードバランサのグローバル構成パラメータを指定できます。

■ サービス モニターの作成

ネットワーク トラフィックの特定のタイプの健全性チェック パラメータを定義するには、サービス モニターを作成します。サービス モニターとプールを関連付けると、サービス モニター パラメータに従ってプール メンバーが監視されます。

■ サーバ プールの追加

サーバ プールを追加して、バックエンド サーバを柔軟かつ効率的に管理、共有することができます。プールはロード バランサの分散方法の管理に使用されます。プールには、健全性チェック パラメータ用のサービス モニターが接続されます。

■ アプリケーション プロファイルの作成

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するには、アプリケーション プロファイルを作成します。プロファイルを設定したら、仮想サーバに関連付けます。関連付けられた仮想サーバは、プロファイルに指定された値に従ってトラフィックを処理します。プロファイルを使用すると、ネットワーク トラフィックの管理に対する制御が強化され、トラフィック管理タスクがより容易で効率的になります。

■ アプリケーション ルールの追加

アプリケーション ルールを作成して、アプリケーション トラフィックの操作と管理を直接行うことができます。

■ 仮想サーバの追加

仮想サーバとして NSX Edge 内部インターフェイスまたはアップリンク インターフェイスを追加します。

ロード バランサ サービスの設定

ロード バランサのグローバル構成パラメータを指定できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] をクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 [編集 (Edit)] をクリックします。

6 有効にするオプションの横にあるチェック ボックスを選択します。


オプション	説明
ロード バランサーの有効化	NSX Edge ロード バランサーで、トラフィックを内部サーバに分散してロード バランシングできるようにします。
アクセラレーションの有効化	<p>グローバルに有効にされている各仮想 IP アドレスは、L7 LB エンジンではなく、より高速な L4 LB エンジンを使用します。</p> <p>L4 TCP VIP は Edge ファイアウォールの前に処理されるため、ファイアウォールの許可ルールは必要ありません。L7 HTTP/HTTPS VIP は Edge ファイアウォールの後に処理されます。</p> <p>[アクセラレーションの有効化] が選択されている場合は、Edge ファイアウォール ルールが L7 HTTP/HTTPS VIP へのアクセスを許可する必要があります。</p> <p>L4 TCP VIP で [アクセラレーションの有効化] フラグが選択され、サーバプールが非透過モードになっている場合は、SNAT ルールが追加されます。そのため、NSX Edge でファイアウォールが有効になっていることを確認します。</p> <p>L4 TCP VIP で [アクセラレーションの有効化] フラグが選択解除され、ファイアウォールが有効になっている場合は、Edge ファイアウォール ルールが L7 HTTP/HTTPS VIP へのアクセスを許可する必要があります。</p>
ログ	<p>NSX Edge ロード バランサーで、トラフィックのログが収集されます。</p> <p>ログ レベルはドロップダウン メニューから選択できます。ログは、設定されている Syslog サーバにエクスポートされます。また、show log follow コマンドを使用すると、ロード バランシング ログを表示できます。</p> <p>[デバッグ] オプションと [情報] オプションは、エンドユーザーの要求のログを収集します。</p> <p>[警告] オプション、[エラー] オプション、および [重大] オプションは、エンドユーザーの要求のログを収集しません。</p>
Service Insertion の有効化	<p>ロード バランサーで、サードパーティ ベンダーのサービスを操作できるようにします。</p> <p>サードパーティ ベンダーのロード バランサー サービスをご使用の環境にデプロイする場合は、[パートナーのロード バランサーの使用] を参照してください。</p>

7 [OK] をクリックします。

サービス モニターの作成

ネットワーク トラフィックの特定のタイプの健全性チェック パラメータを定義するには、サービス モニターを作成します。サービス モニターとプールを関連付けると、サービス モニター パラメータに従ってプール メンバーが監視されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] をクリックして、[ロード バランサー (Load Balancer)] タブをクリックします。
- 5 左側のナビゲーション パネルで、[サービス モニタリング (Service Monitoring)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックします。

- 7 サービス モニターの名前を入力します。
- 8 サーバが ping される間隔を秒単位で入力します。
- 9 サーバが切断していると判断するまでにサーバに ping する回数を入力します。
- 10 サーバからの応答に受信するまでの最長時間を秒単位で入力します。
- 11 健全性チェック要求をサーバに送信する方法を、ドロップダウン メニューから選択します。
- 12 HTTP および HTTPS トラフィックの場合は、以下のステップを実行します。
 - a [期待値] セクションに、HTTP 応答のステータス行で一致するためにモニターが期待する文字列を入力します
たとえば、200,301,302,401 と指定します。
 - b サーバステータスの検出方法を、ドロップダウン メニューから選択します。
 - c サンプル要求で使用する URL を入力します。
 - d POST メソッドを選択した場合は、送信するデータを入力します。
- 13 応答内容で一致する文字列を、[受信] セクションに入力します。
[期待値] セクションの文字列が一致しない場合、モニターは [受信] の内容との一致を試行しません。
- 14 詳細なモニター パラメータを key=value ペアとして [エクステンション] セクションに入力します。
たとえば、エクステンションを warning=10 と指定すると、サーバが 10 秒以内に応答しない場合に、ステータスが警告に設定されることを示します。
すべてのエクステンション項目を、キャリッジ リターン文字で区切る必要があります。

```
<extension>eregi="(0K1|0K2)"</extension>
```

サポートされるプロトコルのエクステンションについては、次の表を参照してください。

表 15-1. TCP プロトコルのエクステンション

監視のエクステンション	説明
escape	send 文字列または quit 文字列で、\n、\r、\t、または \ を使用できます。send オプションまたは quit オプションの前に指定する必要があります。デフォルト：send には何も追加されません。quit の最後に \n が追加されます。
all	すべての expect 文字列がサーバ応答に含まれている必要があります。デフォルトは any です。
quit=<STRING>	接続の正常な終了を開始するために、サーバに送信する文字列。
refuse=ok warn crit	OK、警告、重大ステータスで TCP 拒否を受け入れます。デフォルトは crit です。
mismatch=ok warn crit	OK、警告、重大ステータスで、想定される文字列の不一致を受け入れます。デフォルトは warn です。
jail	TCP ソケットからの出力を非表示にします。
maxbytes=<INTEGER>	指定数より多いバイト数を受信すると、接続を閉じます。
delay=<INTEGER>	文字列の送信から応答のポーリングまでの待ち時間（秒数）。

表 15-1. TCP プロトコルのエクステンション (続き)

監視のエクステンション	説明
certificate=<INTEGER>[,<INTEGER>]	証明書の最少有効日数。最初の値は警告ステータスまでの日数、2 番目の値は重大ステータスまでの日数（指定されない場合は 0）。
ssl-version=3	SSLv3 を使用する SSL ハンドシェイクを強制的に実行します。 健全性チェック オプションで、SSLv3 と TLSv1 はデフォルトで無効になっています。
ssl-version=10	TLS 1.0 を使用する SSL ハンドシェイクを強制的に実行します。
ssl-version=11	TLS 1.1 を使用する SSL ハンドシェイクを強制的に実行します。
ssl-version=12	TLS 1.2 を使用する SSL ハンドシェイクを強制的に実行します。
ciphers='ECDHE-RSA-AES256-GCM-SHA384'	HTTPS 健全性チェックで使用される暗号を表示します。
warning=DOUBLE	警告ステータスになる応答時間（秒）
critical=DOUBLE	重大ステータスになる応答時間（秒）

表 15-2. HTTP/HTTPS プロトコルのエクステンション

監視のエクステンション	説明
no-body	ドキュメントの本文を待たない：ヘッダの読み込み後に処理を停止します。それでも、HEAD ではなく、HTTP GET や POST を実行することに注意してください。
max-age=<SECONDS>	ドキュメントが SECONDS より古い場合は警告します。数値は、分の場合は 10m、時間の場合は 10h、日の場合は 10d の書式で指定することもできます。
content-type=<STRING>	POST 呼び出しでの Content-Type ヘッダーのメディア タイプを指定します。
linespan	正規表現で改行記号を許可します（-r または -R より前に指定する必要があります）。
regex=<STRING> または ereg=<STRING>	正規表現の文字列をページで検索します。
eregi=<STRING>	正規表現の文字列をページで検索します（大文字小文字は区別されません）。
invert-regex	見つければ CRITICAL を返し、見つからなければ OK を返します。
proxy-authorization=<AUTH_PAIR>	基本認証を使用しているプロキシ サーバ上のユーザー名：パスワード。
useragent=<STRING>	User Agent として、HTTP ヘッダで送信される文字列。
header=<STRING>	HTTP ヘッダで送信されるその他のタグ。追加のヘッダで複数回使用できます。
onredirect=ok warning critical follow sticky stickyport	リダイレクト ページの処理方法。 sticky は follow に似ていますが、指定された IP アドレスと連携します。 stickyport ではさらに、ポートが同じであることを確認します。
pagesize=<INTEGER><:INTEGER>	必要な最小ページサイズ（バイト）：必要な最大ページサイズ（バイト）。
warning=DOUBLE	警告ステータスになる応答時間（秒）
critical=DOUBLE	重大ステータスになる応答時間（秒）

表 15-3. HTTPS プロトコルのエクステンション

監視のエクステンション	説明
sni	SSL/TLS ホスト名の拡張をサポートします (SNI)。
certificate=<INTEGER>	証明書の最少有効日数。ポート番号のデフォルトは 443 です。このオプションを使用すると、URL はチェックされません。
authorization=AUTH_PAIR	基本認証を使用しているサイト上のユーザー名：パスワード。

15 [OK] をクリックします。


次のステップ

サービス モニターとプールを関連付けます。

サーバ プールの追加

サーバ プールを追加して、バックエンド サーバを柔軟かつ効率的に管理、共有することができます。プールはロード バランサの分散方法の管理に使用されます。プールには、健全性チェック パラメータ用のサービス モニターが接続されます。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] をクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 左側のナビゲーション パネルで、[プール (Pools)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックします。
- 7 ロード バランサ プールの名前と説明を入力します。
- 8 有効にしたサービスごとにアルゴリズムのバランシング方法を選択できます。

オプション	説明
IP-HASH	ソース 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。 このオプションでは、アルゴリズムのパラメータは無効になります。
LEASTCONN	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。 このオプションでは、アルゴリズムのパラメータは無効になります。
ROUND_ROBIN	各サーバは、割り当てられている重みに従って順番に使用されます。 これは、サーバの処理時間が等分されたままになる場合に、最も円滑で公平なアルゴリズムです。 このオプションでは、アルゴリズムのパラメータは無効になります。

オプション	説明
URI	<p>URI の左側の部分 (疑問符の前の部分) がハッシュされ、実行中のサーバの合計重みによって除算されます。</p> <p>結果により、要求を受信するサーバが指定されます。これにより、サーバが起動したり停止したりしない限り、URI がいつも同じサーバに送信されるようにします。</p> <p>URI アルゴリズム パラメータには 2 つのオプション (uriLength=<len>、uriDepth=<dep>) があります。長さのパラメータの範囲は $1 \leq len < 256$ です。深さのパラメータの範囲は $1 \leq dep < 10$ です。</p> <p>長さおよび深さのパラメータには、正の整数が続きます。これらのオプションでは、URI の最初の部分のみに基づいてサーバのバランシングを行うことができます。長さのパラメータは、アルゴリズムが URI の最初の部分に定義された文字だけを対象としてハッシュを計算することを示します。</p> <p>深さのパラメータは、ハッシュの計算に使用されるディレクトリの最大の深さを示します。要求に含まれる各スラッシュが 1 つのレベルとして数えられます。両方のパラメータが指定されている場合は、いずれかのパラメータに達したときに評価が停止します。</p>
HTTPHEADER	<p>各 HTTP 要求で HTTP ヘッダー名の検索が行われます。</p> <p>カッコで囲まれたヘッダー名は、ACL の <code>hdr()</code> 関数と同様に大文字と小文字が区別されません。ヘッダーがない、または値を含んでいない場合は、ラウンドロビンアルゴリズムが適用されます。</p> <p>HTTPHEADER アルゴリズム パラメータのオプションは 1 つ (headerName=<name>) です。たとえば、host を HTTPHEADER アルゴリズム パラメータとして使用できます。</p>
URL	<p>引数に指定される URL パラメータは、各 HTTP GET 要求のクエリ文字列内で検索されます。</p> <p>パラメータの後ろに等号の <code>=</code> と値が続く場合、その値がハッシュされ、実行されるサーバの重みの合計で割られます。結果により、要求を受信するサーバが指定されます。このプロセスを使用して要求に含まれるユーザー ID が追跡され、サーバの起動または停止が起こらない限り、常に同じユーザー ID が同じサーバに送信されます。</p> <p>値またはパラメータが検出されない場合は、ラウンドロビンアルゴリズムが適用されます。</p> <p>URL アルゴリズム パラメータのオプションは 1 つ (urlParam=<url>) です。</p>

9 (オプション) [モニター (Monitors)] ドロップダウン メニューから、既存のデフォルトまたはカスタムのモニターを選択します。

10 メンバーをプールに追加します。

- a [追加 (Add)] アイコン () をクリックします。
- b サーバメンバーの名前と IP アドレスを入力するか、または [選択 (Select)] をクリックしてグループオブジェクトを割り当てます。
 グループオブジェクトは、vCenter Server または NSX のいずれかです。
- c メンバーがトラフィックを受信するポートと、健全性を監視する ping をメンバーが受信する監視ポートを入力します。
 関連する仮想サーバにポート範囲が設定されている場合、ポートの値は Null になります。
- d [重み] セクションに、このメンバーに割り当てるトラフィックの割合を入力します。
- e メンバーが処理できる最大同時接続数を入力します。
 受信要求は、最大数を超えるとキューに入れられ、接続が解放されるまで待機します。

f メンバーが常に受け入れる最小同時接続数を入力します。

g [OK] をクリックします。

- 11 [透過的 (Transparent)] を選択すると、クライアント IP アドレスをバックエンド サーバで確認できるようになります。


[透過的] を選択しないと (これがデフォルト値)、トラフィック ソース IP アドレスはバックエンド サーバにロード バランサの内部 IP アドレスとして示されます。[透過的] を選択する場合、ソース IP アドレスは実際のクライアント IP アドレスであり、戻りパケットに NSX Edge デバイスを経由させるには NSX Edge をデフォルト ゲートウェイとして設定する必要があります。

- 12 [OK] をクリックします。

アプリケーション プロファイルの作成

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するには、アプリケーション プロファイルを作成します。プロファイルを設定したら、仮想サーバに関連付けます。関連付けられた仮想サーバは、プロファイルに指定された値に従ってトラフィックを処理します。プロファイルを使用すると、ネットワーク トラフィックの管理に対する制御が強化され、トラフィック管理タスクがより容易で効率的になります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] をクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 左側のナビゲーション パネルで、[アプリケーション プロファイル (Application Profiles)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックします。
- 7 プロファイルの名前を入力し、ドロップダウン メニューからプロファイル作成の対象となるトラフィック タイプを選択します。

トラフィック タイプ	サポートされるパーシステンス メソッド
TCP	ソース IP アドレス、MSRDP
HTTP	Cookie、ソース IP アドレス
HTTPS	Cookie、SSL セッション ID (SSL パススルーが有効)、ソース IP アドレス
UDP	ソース IP アドレス

- 8 HTTP トラフィックのリダイレクト先となる URL を入力します。

たとえば、トラフィックを <http://myweb.com> から <https://myweb.com> に転送できます。

9 プロファイルのパーシステンス タイプをドロップダウン メニューから指定します。

パーシステンス設定により、クライアント要求を処理した特定のプール メンバーなど、セッション データが追跡されて保存されます。また、同じセッションまたは後続のセッションでは、クライアント要求が同じプール メンバーにリダイレクトされます。

- クライアントで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するには、[Cookie] のパーシステンスを選択します。

その後の要求で Cookie が参照され、適切なサーバへの接続が維持されます。

- ソース IP アドレスに基づいてセッションを追跡するには、[ソース IP (Source IP)] のパーシステンスを選択します。

接続元アドレスのアフィニティパーシステンスをサポートする仮想サーバへの接続をクライアントが要求すると、ロード バランサは、そのクライアントが以前接続したかどうかを確認し、接続したことがあれば、クライアントを同じプール メンバーに返します。

- Microsoft Remote Desktop Protocol ([MSRDP]) のパーシステンスを選択すると、Windows クライアントと、Microsoft Remote Desktop Protocol (RDP) サービスが実行されているサーバ間の永続セッションを維持できます。

MSRDP パーシステンスを有効にするための推奨シナリオとして、Windows Server 2003 または Windows Server 2008 を実行しているメンバーで構成されるロード バランシング プールを作成し、そこですべてのメンバーが Windows クラスタに属し、Windows セッション ディレクトリに参加するようにすることです。

10 Cookie 名を入力し、Cookie の挿入に使用するモードを選択します。

オプション	説明
挿入	NSX Edge が Cookie を送信します。 サーバが 1 つ以上の Cookie を送信すると、クライアントはもう 1 つ Cookie (サーバの Cookie + Edge の Cookie) を受信します。サーバが Cookie を送信しない場合は、クライアントは Edge の Cookie を受信します。
プリフィックス	クライアントが複数の Cookie をサポートしていない場合は、このオプションを選択します。 注: すべてのブラウザは、複数の Cookie を受け付けます。1 つの Cookie のみをサポートする専用クライアントを使用した専用アプリケーションを使用している場合、Web サーバは Cookie を通常通り送信します。NSX Edge は、その Cookie 情報を (プリフィックスとして) サーバの Cookie 値に挿入します。この Cookie が追加された情報は、NSX Edge がサーバに送信したときに削除されます。
アプリケーション セッション	サーバは Cookie を送信しません。その代わりに、ユーザー セッション情報を URL として送信します。 たとえば、 <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=0l24B9ASD7BSSD</code> が送信される場合、 jsessionid がユーザー セッション情報であり、またパーシステンスのために使用されます。トラブルシューティングのために、アプリケーション セッションのパーシステンス テーブルを見ることはできません。

11 パーシステンスの有効期間を秒単位で入力します。

パーシステンスの有効期間のデフォルトは 5 分間です。

L7 ロード バランシングで TCP でソース IP アドレス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。

12 (オプション) HTTPS トラフィックのアプリケーション プロファイルを作成します。

次の HTTPS トラフィック パターンがサポートされます。

- SSL オフロード - クライアント -> HTTPS -> LB (SSL を終了) -> HTTP -> サーバ
 - SSL プロキシ - クライアント -> HTTPS -> LB (SSL を終了) -> HTTPS -> サーバ
 - SSL パススルー - クライアント -> HTTPS -> LB (SSL を終了) -> HTTPS -> サーバ
 - クライアント -> HTTP -> LB -> HTTP -> サーバ
- a (オプション) [X-Forwarded-For HTTP ヘッダの挿入 (Insert X-Forwarded-For HTTP header)] を選択し、ロード バランサを通じて Web サーバに接続するクライアントの発信 IP アドレスを特定できるようにします。
- b [サービス証明書の構成 (Configure Service Certificate)] を選択し、[仮想サーバ証明書 (Virtual Server Certificates)] タブで、適用可能なサービス証明書、CA 証明書、およびロード バランサ上のクライアントからの HTTPS トラフィックの終了に使用する証明書失効リスト (CRL) を選択します。

これは、クライアント -> LB の接続が HTTPS の場合にのみ必要です。

- c (オプション) [プール側の SSL の有効化 (Enable Pool Side SSL)] を選択して、ロード バランサとバックエンド サーバの間の HTTPS 通信を有効にします。

プール サイド SSL を使用して、エンドツーエンドの SSL を設定できます。

- d (オプション) [サービス証明書の構成 (Configure Service Certificate)] を選択し、を [プール証明書 (Pool Certificates)] タブで、サーバからロード バランサを認証するために使用する適用可能なサービス証明書、CA 証明書、および CRL を選択します。

これは、クライアント -> HTTPS -> LB -> HTTPS -> サーバのパターンの場合にのみ必要です。

NSX Edge ロード バランサに CA 証明書と CRL がすでに設定され、バックエンド サーバからサービス証明書を検証する必要がある場合は、サービス証明書を設定できます。また、バックエンド サーバがロード バランサのサービス 証明書を検証する必要がある場合に、このオプションを使用してロード バランサ証明書をバックエンド サーバに提供することもできます。

13 SSL/TLS ハンドシェイク時にネゴシエートされる暗号アルゴリズムまたは暗号スイートを選択します。

たとえば、**3DES** 暗号スイートのみを使用するように許可できます。

14 クライアント認証を無視するか必須に設定するかを、ドロップダウン メニューから指定します。

必須に設定した場合、クライアントは、要求またはハンドシェイクが中止された後、証明書を提供する必要があります。

15 [OK] をクリックします。

アプリケーション ルールの追加

アプリケーション ルールを作成して、アプリケーション トラフィックの操作と管理を直接行うことができます。

アプリケーション ルールの例は、「[アプリケーション ルールの例](#)」を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 5 左側のナビゲーション パネルで、[アプリケーション ルール (Application Rules)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックします。
- 7 ルールの名前とスクリプトを入力します。
アプリケーション ルールの構文の詳細については、
<http://cbonte.github.io/haproxy-dconv/configuration-1.5.html> を参照してください。
- 8 [OK] をクリックします。

アプリケーション ルールの例

条件に基づく HTTP/HTTPS のリダイレクト

アプリケーション プロファイルでは、要求 URL に関係なく常にトラフィックをリダイレクトする、HTTP/HTTPS のリダイレクトを指定できます。また、HTTP/HTTPS トラフィックをリダイレクトする条件を柔軟に指定できます。

```
move the login URL only to HTTPS.
acl clear dst_port 80
acl secure dst_port 8080
acl login_page url_beg /login
acl logout url_beg /logout
acl uid_given url_reg /login?userid=[^&]+
acl cookie_set hdr_sub(cookie) SEEN=1
redirect prefix https://mysite.com set-cookie SEEN=1 if !cookie_set
redirect prefix https://mysite.com if login_page !secure
redirect prefix http://mysite.com drop-query if login_page !uid_given
redirect location http://mysite.com/ if !login_page secure
redirect location / clear-cookie USERID= if logout
```

ドメイン名によるルーティング

ドメイン名に応じて要求を特定のロード バランサ プールにダイレクトするアプリケーション ルールを作成できます。次のルールは、foo.com への要求を pool_1 に、bar.com への要求を pool_2 にダイレクトします。

```
acl is_foo hdr_dom(host) -i foo
acl is_bar hdr_dom(host) -i bar
use_backend pool_1 if is_foo
use_backend pool_2 if is_bar
```

Microsoft RDP のロード バランシングおよび保護

次のサンプル シナリオでは、ロード バランサが負荷の少ないサーバに新しいユーザーを分散し、切断されたセッションを再開します。このシナリオでは、NSX Edge の内部インターフェイス IP アドレスが 10.0.0.18、内部インターフェイス IP アドレスが 192.168.1.1、仮想サーバが 192.168.1.100、192.168.1.101、192.168.1.102 になります。

- 1 MSRDP を永続化する TCP トラフィックのアプリケーション プロファイルを作成します。
- 2 TCP 健全性モニター (tcp_monitor) を作成します。
- 3 192.168.1.100:3389、192.168.1.101:3389、192.168.1.102:3389 をメンバーとする (rdp-pool という名前の) プールを作成します。
- 4 tcp_monitor を rdp-pool に関連付けます。
- 5 次のアプリケーション ルールを作成します。

```
tcp-request content track-sc1 rdp_cookie(msthash) table rdp-pool
tcp-request content track-sc2 src table ipv4_ip_table

# each single IP can have up to 2 connections on the VDI infrastructure
tcp-request content reject if { sc2_conn_cur ge 2 }

# each single IP can try up to 5 connections in a single minute
tcp-request content reject if { sc2_conn_rate ge 10 }

# Each user is supposed to get a single active connection at a time, block the second one
tcp-request content reject if { sc1_conn_cur ge 2 }

# if a user tried to get connected at least 10 times over the last minute,
# it could be a brute force
tcp-request content reject if { sc1_conn_rate ge 10 }
```

- 6 (rdp-vs という名前の) 仮想サーバを作成します。
- 7 アプリケーション プロファイルをこの仮想サーバに関連付け、手順 4 で作成したアプリケーション ルールを追加します。

仮想サーバで新規に適用されるアプリケーション ルールは、RDP サーバを保護します。

高度なログ

NSX ロード バランサは、デフォルトで基本的なログ作成をサポートしています。トラブルシューティングのより詳細なログ メッセージを表示する場合は、次のようなアプリケーション ルールを作成します。

```
# log the name of the virtual server
capture request header Host len 32

# log the amount of data uploaded during a POST
capture request header Content-Length len 10
# log the beginning of the referrer
capture request header Referer len 20

# server name (useful for outgoing proxies only)
capture response header Server len 20

# logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

# log the expected cache behaviour on the response
capture response header Cache-Control len 8

# the Via header will report the next proxy's name
capture response header Via len 20

# log the URL location during a redirection
capture response header Location len 20
```

アプリケーション ルールを仮想サーバに関連付けると、ログには次の例のように詳細なメッセージが記載されます。

```
2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 --
[25/Apr/2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51656 856 "vip-http-
complete"
"pool-http-complete" "m2" 145 0 1 26 172 --NI 1 1 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux) ""

2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 --
[25/Apr/2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51657 856 "vip-http-
complete"
"pool-http-complete" "m2" 412 0 0 2 414 --NI 0 0 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux) ""
```

HTTPS トラフィックをトラブルシューティングする場合に、複数のルールを追加しなければならないことがあります。ほとんどの Web アプリケーションでは、(通常、ログインまたは POST 呼び出しの後に) クライアントをページにリダイレクトするロケーション ヘッダの付いた 301/302 応答を使用します。また、アプリケーションの Cookie を必要とします。そのため、アプリケーション サーバがクライアントの接続情報を認識することが難しい場合や、適切に応答できない場合があります。アプリケーションが機能しなくなる場合もあります。

Web アプリケーションで SSL オフロードをサポートするには、次のルールを追加します。

```
# See clearly in the log if the application is setting up response for HTTP or HTTPS
capture response header Location len 32
capture response header Set-Cookie len 32

# Provide client side connection info to application server over HTTP header
http-request set-header X-Forwarded-Proto https if { ssl_fc }
http-request set-header X-Forwarded-Proto http if !{ ssl_
```

SSL 経由で接続される場合は、ロード バランサにより次のヘッダが挿入されます。

```
X-Forwarded-Proto: https
```

HTTP 経由で接続される場合は、ロード バランサにより次のヘッダが挿入されます。

```
X-Forwarded-Proto: http
```

特定の URL のブロック

URL に特定のキーワードが含まれる要求をブロックできます。次のサンプルルールは、要求が /private または /finance で始まるかどうかを確認して、これらのキーワードを含む要求をブロックします。

```
acl block_url_list path_beg -i /private /finance
block if block_url_list
```

Cookie を含まない場合の認証への HTTP リダイレクト

Cookie を含まないクライアント要求が認証を受けるようにリダイレクトできます。次のサンプルルールは、HTTP 要求が信頼できるものであり、Cookie をヘッダーに含んでいることを確認します。要求が Cookie を含まない場合、ルールは要求が認証を受けるように /authent.php にリダイレクトします。

```
acl authent_url url /authent.php
acl cookie_present hdr_sub(cookie) cookie1=
redirect prefix /authent.php if !authent_url !cookie_present
```

デフォルト ページへのリダイレクト

クライアント要求 / をデフォルトのページにリダイレクトできます。次のサンプルルールは、HTTP 要求が / であるかどうかを確認して、そのような要求をデフォルトのログイン ページにリダイレクトします。

```
acl default_url url /
redirect prefix /login.php if default_url
```

メンテナンス サイトへのリダイレクト

プライマリ プールがダウンしているときに、メンテナンス サーバ プールを使用して、URL をメンテナンス Web サイトにリダイレクトできます。

```
redirect location http://maintenance.xyz.com/maintenance.htm
```

NT LAN Manager (NTLM) 認証

各要求の後にサーバ セッションを終了しないようにする場合は、NTLM プロトコルを使用することで、サーバ セッションを保持および保護できます。

```
no option http-server-close
```

サーバ ヘッダーの置き換え

既存の応答サーバ ヘッダーを削除して、別のサーバに置き換えることができます。次のサンプル ルールは、サーバ ヘッダーを削除して NGINX Web サーバに置き換えます。NGINX Web サーバは、HTTP、HTTPS、SMTP、POP3 および IMAP プロトコルのリバース プロキシ サーバ、HTTP キャッシュ、およびロード バランサとして機能することが可能です。

```
rspidel Server
rspadd Server:\ nginx
```

リダイレクトの書き換え

ロケーション ヘッダーを HTTP から HTTPS に書き換えることができます。次のサンプル ルールは、ロケーション ヘッダーを特定して、HTTP を HTTPS に置き換えます。

```
rspirep ^Location:\ http://(.*) Location:\ https://\1
```

ホスト ベースの特定プールの選択

特定のホストが指定された要求を、定義されたプールにリダイレクトできます。次のサンプル ルールは、特定のホスト (app1.xyz.com、app2.xyz.com、host_any_app3) が指定された要求を確認して、これらの要求をそれぞれに定義されたプール (pool_app1、pool_app2、pool_app3) にリダイレクトします。その他すべての要求は、仮想サーバに定義された既存のプールにリダイレクトされます。

```
acl host_app1 hdr(Host) -i app1.xyz.com
acl host_app2 hdr(Host) -i app2.xyz.com
acl host_any_app3 hdr_beg(host) -i app3

use_backend pool_app1 if host_app1
use_backend pool_app2 if host_app2
use_backend pool_app3 if host_any_app3
```

URL に基づく特定プールの選択

URL キーワードが指定された要求を、特定のプールにリダイレクトできます。次のサンプルルールは、要求が `/private` または `/finance` で始まるかどうかを確認して、これらの要求を定義されたプール (`pool_private` または `pool_finance`) にリダイレクトします。その他すべての要求は、仮想サーバに定義された既存のプールにリダイレクトされます。

```
acl site_private path_beg -i /private
acl site_finance path_beg -i /finance
use_backend pool_private if site_private
use_backend pool_finance if site_finance
```

プライマリ プールがダウンしている場合のリダイレクト

プライマリ プールのサーバがダウンしている場合に、セカンダリ プールのサーバを使用するようにユーザーをリダイレクトできます。次のサンプルルールは、`pool_production` がダウンしているかどうかを確認して、ユーザーを `pool_sorry_server` に転送します。

```
acl pool_production_down nbsrv(pool_production) eq 0
use_backend pool_sorry_server if pool_production_down
```

TCP 接続のホワイトリスト

クライアント IP アドレスがサーバにアクセスしないようにブロックできます。次のサンプルルールは、定義された IP アドレスをブロックし、IP アドレスがホワイトリストに含まれていない場合に接続を拒否します。

```
acl whitelist src 10.10.10.0 20.20.20.0
tcp-request connection reject if !whitelist
```

SSLv3 と TLSv1 を有効にする

デフォルトでは、SSLv3 と TLSv1 は無効に設定されているサービス モニター エクステンションです。次のアプリケーションルールを使用して、これらを有効にすることができます。

```
ssl3 enable
tls1 enable
```

クライアントのセッション タイムアウト設定

セッション タイムアウトとは、クライアント接続が非アクティブ状態になった場合の最長期限のことです。非アクティブ状態のタイムアウトは、想定していたクライアントからのデータが確認または送信されない場合に適用されます。HTTP モードでは、クライアントが要求を送信する最初の段階、およびサーバから送信されたデータをクライアントが読み取る応答時に、このタイムアウトを考慮することが特に重要です。デフォルトのタイムアウトは、5 分間です。

次のサンプル ルールでは、タイムアウト期間を 100 秒に設定します。

```
timeout client 100s
```

時間は、ミリ秒、秒、分、時間、または日を単位として整数で設定できます。


仮想サーバの追加

仮想サーバとして NSX Edge 内部インターフェイスまたはアップリンク インターフェイスを追加します。

前提条件

- アプリケーション プロファイルを使用できることを確認します。[「アプリケーション プロファイルの作成」](#)を参照してください。
- アプリケーション ルールを仮想サーバに関連付ける場合は、[「アプリケーション プロファイルの作成」](#)を参照してください。
- より高速なロード バランサを使用するためにアクセラレーションを有効にする場合は、ロード バランサの設定時にアクセラレーションを有効にする必要があります。[「ロード バランサ サービスの設定」](#)を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] をクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 左側のナビゲーション ペインで、[仮想サーバ (Virtual Servers)] をクリックします。
- 6 [追加 (Add)] () アイコンをクリックします。
- 7 この仮想サーバを使用可能にするには、[仮想サーバの有効化 (Enable Virtual Server)] を選択します。
- 8 (オプション) NSX Edge ロード バランサが、L7 ロード バランサ エンジンではなく、より高速な L4 ロード バランサ エンジンを使用するように設定するには、[アクセラレーションの有効化 (Enable Acceleration)] を選択します。

アプリケーション ルール、HTTP タイプ、Cookie のパーシステンスなどの仮想サーバ設定で L7 ロード バランサ エンジンを使用する場合は、アクセラレーションを有効にしたかどうかに関係なく、L7 ロード バランサ エンジンが使用されます。

CLI コマンド **show service load balancer virt** を使用すると、使用中のロード バランサ エンジンを確認できます。

- 9 仮想サーバに関連付けるアプリケーション プロファイルを選択します。

追加する仮想サーバとして同じプロトコルに関連付けることができるアプリケーション プロファイルは 1 つのみです。選択したプールにサポートされているサービスが表示されます。

- 10 仮想サーバの名前と説明を入力します。

- 11 [IP アドレスの選択 (Select IP Address)] をクリックし、ロード バランサが待機する IP アドレスを設定して、仮想サーバが処理するプロトコルを入力します。

[IP アドレスの選択] ダイアログ ボックスには、プライマリ IP アドレスのみが表示されます。セカンダリ IP アドレスを使用して VIP を作成する場合は、手動で入力します。
- 12 仮想サーバが処理するプロトコルを、ドロップダウン メニューから選択します。
- 13 ロード バランサが listen するポート番号を入力します。

また、80,8001-8004,443 のようにポート範囲を設定して、サーバ プール、アプリケーション プロファイル、アプリケーション ルールなどの仮想サーバ設定を共有できます。

FTP を使用するには、TCP プロトコルにポート 21 が割り当てられている必要があります。
- 14 アプリケーション ルールを選択します。
- 15 [接続の制限] セクションに、仮想サーバが処理可能な同時接続の最大数を入力します。
- 16 [接続速度の制限] セクションに、1 秒あたりに受信する新規接続要求の最大数を入力します。
- 17 (オプション) [詳細 (Advanced)] タブをクリックして、仮想サーバに関連付けるアプリケーション ルールを追加します。
- 18 [OK] をクリックします。

アプリケーション プロファイルの管理

アプリケーション プロファイルを作成して仮想サーバに関連付けます。作成したプロファイルを更新したり、システム リソースを節約するために削除することができます。

アプリケーション プロファイルの編集

アプリケーション プロファイルを編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[ロード バランサー (Load Balancer)] タブをクリックします。
- 5 左側のナビゲーション パネルで、[アプリケーション プロファイル (Application Profiles)] をクリックします。
- 6 プロファイルを選択して、[編集 (Edit)] (✎) アイコンをクリックします。
- 7 トラフィック、パーシステンス、証明書、または暗号の設定を適切に変更して、[終了 (Finish)] をクリックします。

ロード バランサ用 SSL Termination の設定

SSL Termination を設定していない場合、HTTP 要求は検査されません。ロード バランサは、ソースとターゲットの IP アドレスや、暗号化されたデータを認識します。HTTP 要求を精査する場合、ロード バランサで SSL セッションを終了して、セル プールに対する新しい SSL セッションを作成します。

前提条件

[管理 (Manage)] > [設定 (Settings)] > [証明書 (Certificates)] の順に移動して、有効な証明書があることを確認します。

手順

- 1 アプリケーション プロファイルで、[管理 (Manage)] > [ロード バランサー (Load Balancer)] > [アプリケーション プロファイル (Application Profiles)] の順に選択します。
- 2 ドロップダウン メニューから [HTTPS] タイプを選択します。
- 3 [SSL パススルーの有効化 (Enable SSL Passthrough)] が選択解除されていることを確認します。
- 4 [サービス証明書の構成 (Configure Service Certificate)] が選択されていることを確認します。
- 5 適切な証明書をリストから選択します。

Edit Profile ?

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

アプリケーション プロファイルの削除

アプリケーション プロファイルを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 5 左側のナビゲーション パネルで、[アプリケーション プロファイル (Application Profiles)] をクリックします。
- 6 プロファイルを選択し、[削除 (Delete)] アイコンをクリックします。

サービス モニターの管理

サービス モニターを作成して、ネットワーク トラフィックの健全性チェック パラメータを定義し、プールに関連付けます。作成したサービス モニターは更新したり、システム リソース節約のために削除することもできます。

サービス モニターの編集

サービス モニターを編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 5 左側のナビゲーション パネルで、[サービス モニタリング (Service Monitoring)] をクリックします。
- 6 サービス モニターを選択し、[編集 (Edit)] アイコンをクリックします。
- 7 必要な変更を行い、[OK] をクリックします。

サービス モニターの削除

サービス モニターを削除できます。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 5 左側のナビゲーション パネルで、[サービス モニタリング (Service Monitoring)] をクリックします。
- 6 サービス モニターを選択し、[削除 (Delete)] アイコンをクリックします。

サーバ プールの管理

ロード バランサによる分散を管理するためにサーバ プールを追加した後で、既存のプールを更新したり、システム リソースを節約するために削除したりできます。

サーバ プールの編集

サーバ プールを編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 [プール] タブが開かれていることを確認します。
- 6 編集するプールを選択します。
- 7 [編集 (Edit)] (✎) アイコンをクリックします。
- 8 必要な変更を行い、[終了 (Finish)] をクリックします。

ロード バランサでの透過モードの設定

[透過的] は、クライアント IP アドレスがバックエンド サーバで確認できるかどうかを示します。デフォルトでは [透過的] は選択されていません。この場合、バックエンド サーバは、トラフィック ソースの IP アドレスをロード バランサの内部 IP アドレスとして認識します。[透過的] を選択した場合、ソース IP アドレスは実際のクライアント IP アドレスになり、NSX Edge がサーバ応答のパス上に存在する必要があります。典型的な設計では、NSX Edge をサーバのデフォルト ゲートウェイとして設定します。

手順

- ◆ [管理 (Manage)] > [ロード バランサー (Load Balancer)] > [プール (Pools)] の順にクリックし、サーバ プールの設定で、透過モードを有効にします。

Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	web-01a	172.16.1...	1	443	443	0	0
✓	web-02a	172.16.1...	1	443	443	0	0

☒ Transparent

OK Cancel

サーバ プールの削除

サーバ プールを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 [プール] タブが開かれていることを確認します。
- 6 削除するプールを選択します。
- 7 [削除 (Delete)] (✖) アイコンをクリックします。


仮想サーバの管理

仮想サーバを追加した後で、既存の仮想サーバの設定を更新または削除できます。

仮想サーバの編集

仮想サーバを編集できます。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 [仮想サーバ (Virtual Servers)] タブをクリックします。
- 6 編集する仮想サーバを選択します。
- 7 [編集 (Edit)] () アイコンをクリックします。
- 8 必要な変更を行い、[終了 (Finish)] をクリックします。

仮想サーバの削除

仮想サーバを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [監視 (Monitor)] タブをクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
- 5 [仮想サーバ (Virtual Servers)] タブをクリックします。
- 6 削除する仮想サーバを選択します。
- 7 [削除 (Delete)] () アイコンをクリックします。

アプリケーション ルールの管理

アプリケーション ルールを作成して、アプリケーション トラフィックを設定します。作成したルールは編集または削除できます。

アプリケーション ルールの編集

アプリケーション ルールを編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。

- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 5 左側のナビゲーション パネルで、[アプリケーション ルール (Application Rules)] をクリックします。
- 6 ルールを選択し、[編集 (Edit)] アイコンをクリックします。
- 7 必要な変更を行い、[OK] をクリックします。

アプリケーション ルールの削除

アプリケーション ルールを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 [NSX Edge] をダブルクリックします。
- 4 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 5 左側のナビゲーション パネルで、[アプリケーション プロファイル (Application Profiles)] をクリックします。
- 6 プロファイルを選択し、[削除 (Delete)] アイコンをクリックします。

NTLM 認証を使用する Web サーバのロード バランシング

デフォルトでは、NSX ロード バランサは、クライアントの要求が終わるごとに、サーバの TCP 接続を閉じます。NTLM 認証では、1 つの TCP セッションで複数の HTTP 要求を必要とするため、NSX ロード バランサを介する認証で障害が発生します。

前提条件

この問題を回避するため、NTLM 認証を使用する Web サーバのロード バランシングを行う仮想 IP アドレスに、次のアプリケーション ルールを追加します。

```
add # NTLM authentication and keep the server connection open between requests
no option http-server-close
```

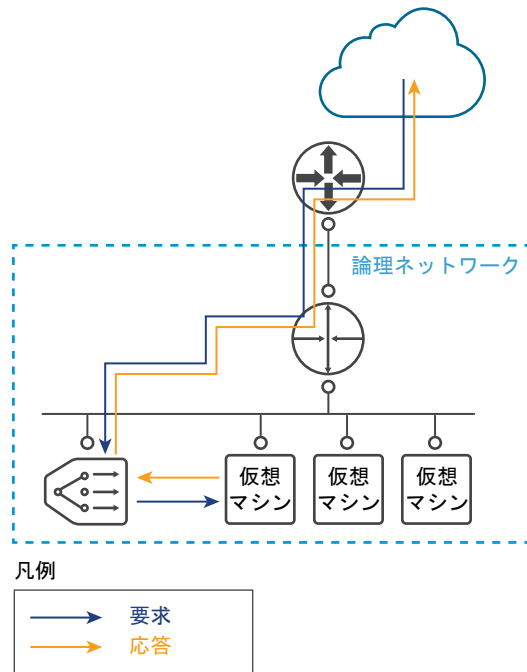
このアプリケーション ルールによって、複数の要求の間でサーバ接続が開かれた状態が維持されます。

NSX ロード バランサ構成のシナリオ

NSX ロード バランサ構成シナリオを使用して、必要な End-to-End のワークフローを理解します。

シナリオ：ワンアーム ロード バランサの構成

Edge Services Gateway (ESG) は、受信するクライアント トラフィックのプロキシとして考えることができます。



プロキシ モードでは、ロード バランサは、自身の IP アドレスを送信元アドレスとして使用して、リクエストをバックエンド サーバに送信します。バックエンド サーバには、ロード バランサから送信されるときにすべてのトラフィックが表示され、このサーバはロード バランサに直接応答します。このモードは、SNAT モードまたは非透過モードとも呼ばれます。

一般的な NSX ワンアーム ロード バランサは、バックエンド サーバと同じで論理ルーターとは異なるサブネットにデプロイされます。NSX ロード バランサ仮想サーバは、クライアントから受信したリクエストを仮想 IP で listen し、バックエンド サーバにリクエストを送信します。リターン トラフィックについては、リバース NAT が必要となります。これは、バックエンド サーバの送信元 IP アドレスを仮想アドレス (VIP) に変更してから、クライアントに仮想 IP アドレスを送信するためです。この操作を行わないと、クライアントへの接続が切断されます。

ESG はトラフィックを受信した後に、VIP アドレスをいずれかのロード バランサ マシンの IP アドレスに変更する宛先ネットワーク アドレス変換 (DNAT) とクライアント IP アドレスを ESG IP アドレスに交換する送信元ネットワーク アドレス変換 (SNAT) の 2 つの操作を実行します。

次に、ESG サーバはトラフィックをロード バランサ サーバに送信し、ロード バランサ サーバは応答を ESG に返し、さらにクライアントに返します。このオプションでは、インライン モードよりも構成が大幅に容易になりますが、2 つの注意点があります。最初の注意点は、専用の ESG サーバが必要となることであり、2 番目の注意点はロード バランサは元のクライアント IP アドレスを認識しないことです。HTTP/HTTPS アプリケーションでの 1 つの回避策として、HTTP アプリケーション プロファイルで Insert X-Forwarded-For を有効にすることによって、バックエンド サーバに送信される要求の X-Forwarded-For HTTP ヘッダーにクライアント IP アドレスが追加されます。

バックエンド サーバでのクライアント IP アドレスの可視化が、HTTP/HTTPS 以外のアプリケーションで必要となる場合には、透過的になるように IP アドレス プールを設定できます。クライアントがバックエンド サーバと同じサブ ネットにない場合には、インライン モードが推奨されます。インライン モードを使用しない場合には、バックエン ドサーバのデフォルト ゲートウェイとしてロード バランサの IP アドレスを使用する必要があります。

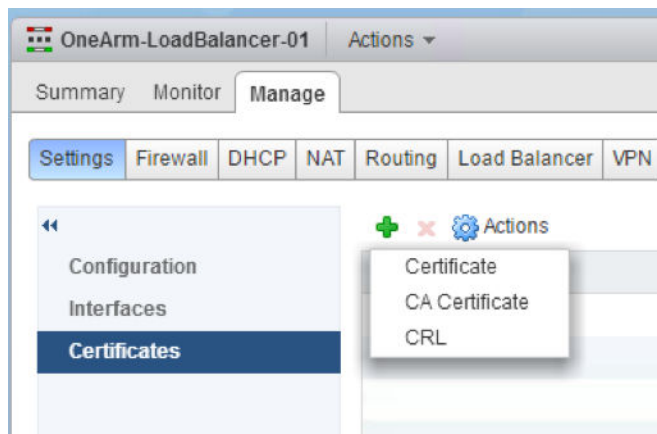
注: 接続の整合性を保証する方法には、通常、次の 2 つがあります。

- SNAT/プロキシ/非透過モード（上記で説明）
- DSR (Direct Server Return)

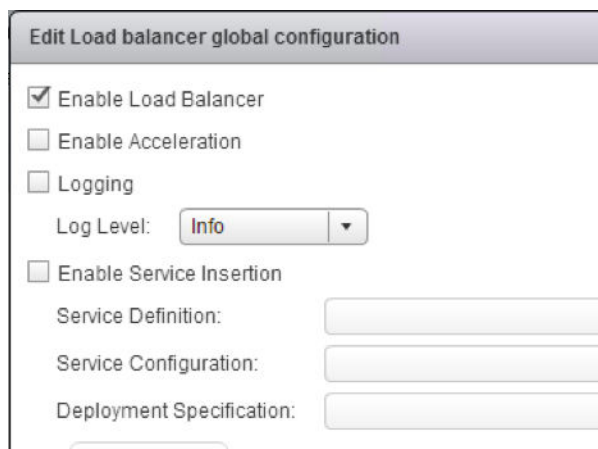
DSR モードでは、バックエンド サーバが直接クライアントに応答します。現在、NSX ロード バランサは、DSR をサ ポートしていません。

手順

- 1 Edge をダブルクリックしてから、[管理 (Manage)] > [設定 (Settings)] > [証明書 (Certificate)] を選択して、証 明書を作成します。



- 2 [管理 (Manage)] > [ロード バランサー (Load Balancer)] > [グローバル構成 (Global Configuration)] > [編集 (Edit)] を選択して、ロード バランサ サービスを有効にします。



- 3 [管理 (Manage)] > [ロードバランサー (Load Balancer)] > [アプリケーション プロファイル (Application Profiles)] を選択して、HTTPS アプリケーション プロファイルを作成します。

New Profile

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificate... **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

注: ドキュメント作成の都合上、上記のスクリーンショットでは、自己署名の証明書が使用されています。

- 4 オプションで、[管理 (Manage)] > [ロードバランサー (Load Balancer)] > [サービス モニタリング] (Service Monitoring)] をクリックして、デフォルトのサービスモニタリングを編集し、必要に応じて、基本の HTTP/HTTPS から特定の URL/URI に変更します。

- 5 [管理 (Manage)] > [ロード バランサー (Load Balancer)] > [プール (Pools)] を選択して、サーバ プールを作成します。

SNAT モードを使用するには、プール設定の [透過的 (Transparent)] チェック ボックスをオフのままにします。

Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

☐ Transparent

OK Cancel

仮想マシンが表示され有効になっていることを確認します。

- 6 オプションで、[管理 (Manage)] > [ロード バランサー (Load Balancer)] > [プール (Pools)] > [プール統計の表示 (Show Pool Statistics)] をクリックして、ステータスを確認します。

メンバー ステータスが [UP] であることを確認します。

- 7 [管理 (Manage)] > [ロード バランサー (Load Balancer)] > [仮想サーバ (Virtual Servers)] を選択して、仮想サーバを作成します。

UDP やさらに高パフォーマンスの TCP に L4 ロード バランサを使用する場合には、[アクセラレーションの有効化 (Enable Acceleration)] をオンにします。[アクセラレーションの有効化 (Enable Acceleration)] をオンにしている場合、L4 SNAT でファイアウォールが必要であるため、ファイアウォールのステータスがロード バランサ NSX Edge で [有効 (Enabled)] になっていることを確認します。

General Advanced

☒ Enable Virtual Server

☐ Enable Acceleration

Application Profile: * OneArmWeb-01

Name: * Web-Tier-VIP-01

Description:

IP Address: * 172.16.10.10 [Select IP Address](#)

Protocol: HTTPS

Port: * 443

Default Pool: Web-Tier-Pool-01

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

IP アドレスがサーバ プールに関連付けられていることを確認します。

- 8 オプションで、アプリケーション ルールを使用している場合、[管理 (Manage)] > [ロード バランサー (Load Balancer)] > [アプリケーション ルール (Application Rules)] で設定を確認します。

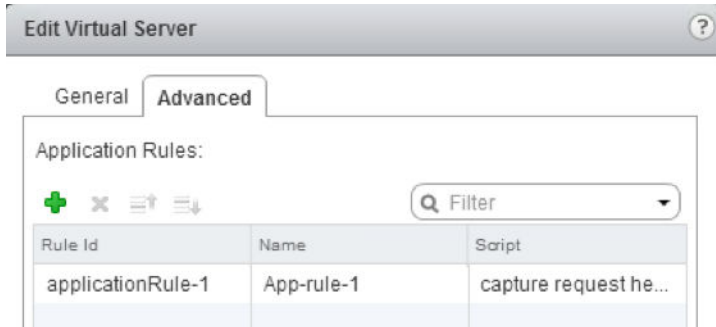
Add Application Rule ?

Name: App-Rule-1

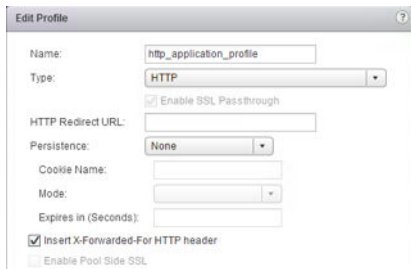
Script: # A sample application rule to log the name of the virtual server
capture request header Host len 32

- 9 アプリケーション ルールを使用する場合、[管理 (Manage)] > [ロード バランサー (Load Balancer)] > [仮想サーバ (Virtual Servers)] > [詳細 (Advanced)] で仮想サーバにアプリケーション ルールが関連付けられていることを確認します。

サポートされる例については、<https://communities.vmware.com/docs/DOC-31772> を参照してください。



非透過モードでは、バックエンドサーバはクライアント IP を確認できませんが、ロード バランサ内部の IP アドレスは確認できます。HTTP/HTTPS トラフィックのための回避策として、[X-Forwarded-For HTTP ヘッダの挿入 (Insert X-Forwarded-For HTTP header)] をオンにします。このオプションをオンにすると、Edge ロード バランサは、クライアント ソース IP アドレスの値にヘッダー「X-Forwarded-For」を追加します。



シナリオ：Platform Services Controller 用 NSX ロード バランサの設定

Platform Services Controller (PSC) は、vCenter Single Sign-On、ライセンス、証明書管理、サーバの予約など、インフラストラクチャのセキュリティ機能を提供します。

NSX ロード バランサを設定したら、vCenter Single Sign-On 向けに NSX Edge デバイスのアップリンク インターフェイス IP アドレスを提供できます。

前提条件

- ナレッジベースに記載されている、PSC の高可用性を実現するための準備タスクを実行します。
<http://kb.vmware.com/kb/2113315> を参照してください。
- 証明書を設定するため、最初の PSC ノードの /ha/lb.crt および /ha/lb_rsa.key を保存します。
- NSX Edge デバイスが設定されていることを確認します。
- 仮想 IP アドレスの設定用アップリンクと内部論理スイッチに接続するインターフェイスが、それぞれ 1 つ以上設定されていることを確認します。

手順

- 1 NSX Edge に PSC CA 証明書を追加します。
 - a OpenSSL コマンドを使用して、PSC の root.cer と証明書、RSA、およびパスフレーズを生成し、保存します。
 - b Edge をダブルクリックして、[管理 (Manage)] - [設定 (Settings)] - [証明書 (Certificate)] の順に選択します。
 - c 保存された root.cer ファイルの内容を CA 証明書に追加します。
 - d 保存されたパスフレーズをプライベート キー セクションに追加します。
- 2 ロード バランサ サービスを有効にします。
 - a [管理 (Manage)] - [ロード バランサー (Load Balancer)] - [編集 (Edit)] の順に選択します。
 - b [ロード バランサーの有効化 (Enable Load Balancing)] および [ログ (Logging)] オプションを選択します。

3 TCP および HTTPS プロトコルを使用してアプリケーション プロファイルを作成します。

- a [管理 (Manage)] - [ロード バランサー (Load Balancer)] - [アプリケーション プロファイル (Application Profiles)] の順に選択します。
- b TCP アプリケーション プロファイルを作成します。

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso_tcp_profile
- Type:** TCP
- ☐ Enable SSL Passthrough
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- ☐ Insert X-Forwarded-For HTTP header
- ☐ Enable Pool Side SSL
- Virtual Server Certificates:** Pool Certificates
- Service Certificates:** CA Certificates, CRL
- ☐ Configure Service Certificate
- | Common Name | Issuer | Validity |
|--------------------|--------|-----------------------|
| NSX-ESG-1-0.system | CA | Thu Jul 30 2015 - Thu |
| | | |
| | | |
| | | |
| | | |
- Cipher:** (empty)
- Client Authentication:** Ignore
- Buttons:** OK, Cancel

- c HTTPS アプリケーション プロファイルを作成します。

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso_https_profile
- Type:** HTTPS
- ☐ Enable SSL Passthrough
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- ☐ Insert X-Forwarded-For HTTP header
- ☒ Enable Pool Side SSL
- Virtual Server Certificates:** Pool Certificates
- Service Certificates:** CA Certificates, CRL
- ☒ Configure Service Certificate
- | Common Name | Issuer | Validity |
|--------------------|--------|-----------------------|
| NSX-ESG-1-0.system | CA | Thu Jul 30 2015 - Thu |
| | | |
| | | |
| | | |
| | | |
- Cipher:** (empty)
- Client Authentication:** Ignore
- Buttons:** OK, Cancel

- 4 メンバー PSC ノードを追加するためのアプリケーション プールを作成します。
 - a [管理 (Manage)] - [ロード バランサー (Load Balancer)] - [プール (Pools)] の順に選択します。
 - b モニター ポート 443 を使用して、アプリケーション プールを 2 つ作成します。

PSC ノードの IP アドレスを使用してください。

Edit Pool

Name: * sso_tcp_pool1

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168.1.1	1	443		0	0
✓	PSC02	192.168.1.2	1	443		0	0

☐ Transparent

OK Cancel

- c モニター ポート 389 を使用して、アプリケーション プールを 2 つ作成します。
- PSC ノードの IP アドレスを使用してください。

New Pool

Name: * sso_tcp_pool2

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168.1.1	1	389		0	0
✓	PSC02	192.168.1.2	1	389		0	0

☐ Transparent

OK Cancel

- 5 TCP および HTTPS プロトコル用の仮想サーバを作成します。
 - a [管理 (Manage)] - [ロード バランサー (Load Balancer)] - [仮想サーバ (Virtual Servers)] の順に選択します。
 - b TCP 仮想 IP アドレス用の仮想サーバを作成します。

The screenshot shows the 'New Virtual Server' dialog box with the 'General' tab selected. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'sso_tcp_profile'. The 'Name' is 'sso_tcp_vip'. The 'IP Address' is '10.156.209.158' with a 'Select IP Address' link. The 'Protocol' is 'TCP'. The 'Port' is '389,636,2012,2014,2020'. The 'Default Pool' is 'sso_tcp_pool2'. The 'Connection Limit' and 'Connection Rate Limit' fields are empty. The 'OK' and 'Cancel' buttons are at the bottom right.

- c HTTPS VIP 用の仮想サーバを作成します。

The screenshot shows the 'New Virtual Server' dialog box with the 'General' tab selected. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'sso_https_profile'. The 'Name' is 'sso_https_vip'. The 'IP Address' is '10.156.209.158' with a 'Select IP Address' link. The 'Protocol' is 'HTTPS'. The 'Port' is '443'. The 'Default Pool' is 'sso_tcp_pool1'. The 'Connection Limit' and 'Connection Rate Limit' fields are empty. The 'OK' and 'Cancel' buttons are at the bottom right.

その他の Edge サービス

NSX Services ゲートウェイは、IP アドレスのプーリング、1 対 1 の固定 IP アドレス割り当て、外部 DNS サーバ構成をサポートします。

上記のサービスを使用する前に、NSX Edge インスタンスが動作している必要があります。NSX Edge のセットアップの詳細については、[「NSX Edge 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。

- [DHCP サービスの管理](#)
- [DHCP リレーの設定](#)
- [DNS サーバの設定](#)

DHCP サービスの管理

NSX Edge は、IP アドレスのプーリングと 1 対 1 の固定 IP アドレス割り当てをサポートします。固定 IP アドレスバインディングは vCenter Server の管理するオブジェクト ID と、リクエストするクライアントのインターフェイス ID を基にします。

NSX Edge DHCP サービスは以下のガイドラインに従います。

- DHCP 検出のために、NSX Edge の内部インターフェイスで待機します。
- NSX Edge 上の内部インターフェイスの IP アドレスを、すべてのクライアント（ただし、直接接続されていないプールを除く）のデフォルト ゲートウェイ アドレスとして、またコンテナ ネットワークの内部インターフェイスのブロードキャストとサブネット マスクの値として使います。


以下の状況では、クライアントの仮想マシン上の DHCP サービスを再起動する必要があります。

- DHCP プール、デフォルト ゲートウェイ、または DNS サーバを変更または削除した場合。
- NSX Edge インスタンスの内部 IP アドレスを変更した場合。

DHCP IP アドレス プールの追加

DHCP サーバには IP アドレスのプールが必要です。IP アドレス プールとは、ネットワーク内の連続した IP アドレスの範囲です。アドレス バインディングを持たない NSX Edge によって保護されている仮想マシンには、このプールから IP アドレスが割り当てられます。IP アドレス プールの範囲は、互いに交わることはないため、1 つの IP アドレスは、必ず 1 つの IP アドレス プールに属することになります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理] タブをクリックして、[DHCP] タブをクリックします。
- 5 [追加] () アイコンをクリックします。
- 6 プールを設定します。

オプション	アクション
[DNS の自動設定]	DHCP バインドに DNS サービス設定を使用することを選択します。
[リースの有効期限なし]	アドレスを仮想マシンの MAC アドレスに永久にバインドすることを選択します。これを選択すると、[リース時間] が無効になります。
[開始 IP]	プールの開始 IP アドレスを入力します。
[終了 IP]	プールの終了 IP アドレスを入力します。
[ドメイン名]	DNS サーバのドメイン名を入力します。これは省略できます。
[プライマリ ネーム サーバ]	[DNS の自動] を選択していない場合は、DNS サービスの [プライマリ ネーム サーバ] を入力します。hostname-to-IP アドレス解決のために DNS サーバの IP アドレスを入力する必要があります。これは省略できます。
[セカンダリ ネーム サーバ]	[DNS の自動] を選択していない場合は、DNS サービスの [セカンダリ ネーム サーバ] を入力します。hostname-to-IP アドレス解決のために DNS サーバの IP アドレスを入力する必要があります。これは省略できます。
[デフォルト ゲートウェイ]	デフォルトのゲートウェイ アドレスを入力します。デフォルトのゲートウェイ IP アドレスを指定しない場合は、NSX Edge インスタンスの内部インターフェイスがデフォルト ゲートウェイとして取得されます。これは省略できます。
[サブネット マスク]	サブネット マスクを指定します。分散ルーターの場合に備えて、サブネット マスクは Edge インターフェイスまたは DHCP リレーのサブネット マスクと同じである必要があります。
[リース時間]	アドレスをクライアントにデフォルトの期間 (1 日) リースするか、秒数で値を指定するかを選択します。[リースの有効期限なし] を選択した場合は、リース時間を指定できません。これは省略できます。

- 7 [OK] をクリックします。

DHCP サービスを有効にする

DHCP サービスを有効にすると、NSX Edge によって、定義された IP アドレス プールから IP アドレスを自動的に仮想マシンに割り当てることができます。

前提条件

DHCP IP アドレス プールが追加されている必要があります。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理] タブをクリックして、[DHCP] タブをクリックします。
- 5 [有効化] をクリックします。
- 6 [ログの有効化] を必要に応じて選択し、ログ レベルを選択します。
- 7 [変更の発行] をクリックします。

次のステップ

IP アドレス プールとバインドを作成します。

DHCP IP アドレス プールの編集

DHCP IP アドレス プールを編集して、IP アドレスを追加または削除できます。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[DHCP] タブをクリックします。
- 5 DHCP プールを選択し、[編集 (Edit)] アイコンをクリックします。
- 6 必要な変更を行い、[OK] をクリックします。

DHCP 静的バインドの追加

仮想マシン上で動作しているサービスがあり、IP アドレスを変更したくない場合は、IP アドレスを仮想マシンの MAC アドレスにバインドすることができます。バインドする IP アドレスは、IP アドレス プールと重複しないようにしてください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[DHCP] タブをクリックします。
- 5 左側のパネルから [バインド (Bindings)] を選択します。
- 6 [追加 (Add)] () アイコンをクリックします。

7 バインドを設定します。

オプション	アクション
[DNS の自動設定 (Auto Configure DNS)]	DHCP バインドに DNS サービス設定を使用することを選択します。
[リースの有効期限なし (Lease never expires)]	アドレスを仮想マシンの MAC アドレスに永久にバインドすることを選択します。
[インターフェイス (Interface)]	バインドする NSX Edge インターフェイスを選択します。
[仮想マシン名 (VM Name)]	バインドする仮想マシンを選択します。
[仮想マシン vNIC インデックス (VM vNIC Index)]	IP アドレスにバインドする仮想マシンの NIC を選択します。
[ホスト名 (Host Name)]	DHCP クライアント仮想マシンのホスト名を入力します。
[IP アドレス (IP Address)]	選択した仮想マシンの MAC アドレスをバインドするアドレスを入力します。
[サブネット マスク (Subnet Mask)]	サブネット マスクを指定します。分散ルーターの場合に備えて、サブネット マスクは Edge インターフェイスまたは DHCP リレーのサブネット マスクと同じである必要があります。
[ドメイン名 (Domain Name)]	DNS サーバのドメイン名を入力します。
[プライマリ ネーム サーバ (Primary Name Server)]	[DNS の自動設定 (Auto Configure DNS)] を選択していない場合は、DNS サービスの [プライマリ ネーム サーバ (Primary Nameserver)] を入力します。hostname-to-IP アドレス解決のために DNS サーバの IP アドレスを入力する必要があります。
[セカンダリ ネーム サーバ (Secondary Name Server)]	[DNS の自動設定 (Auto Configure DNS)] を選択していない場合は、DNS サービスの [セカンダリ ネーム サーバ (Secondary Nameserver)] を入力します。hostname-to-IP アドレス解決のために DNS サーバの IP アドレスを入力する必要があります。
[デフォルト ゲートウェイ (Default Gateway)]	デフォルトのゲートウェイ アドレスを入力します。デフォルトのゲートウェイ IP アドレスを指定しない場合は、NSX Edge インスタンスの内部インターフェイスがデフォルト ゲートウェイとして取得されます。
[リース時間 (Lease Time)]	[リースの有効期限なし (Lease never expires)] を選択していない場合は、アドレスをクライアントにデフォルトの期間 (1 日) リースするか、秒数で値を指定するかを選択します。

8 [追加 (Add)] をクリックします。

9 [変更の発行 (Publish Changes)] をクリックします。

DHCP バインドの編集

仮想マシンの MAC アドレスにバインドされる固定 IP アドレスとして、異なるアドレスを割り当てます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[DHCP] タブをクリックします。
- 5 左側のパネルから [バインド (Bindings)] を選択し、編集するバインドをクリックします。
- 6 [編集] アイコンをクリックします。
- 7 必要な変更を行い、[OK] をクリックします。

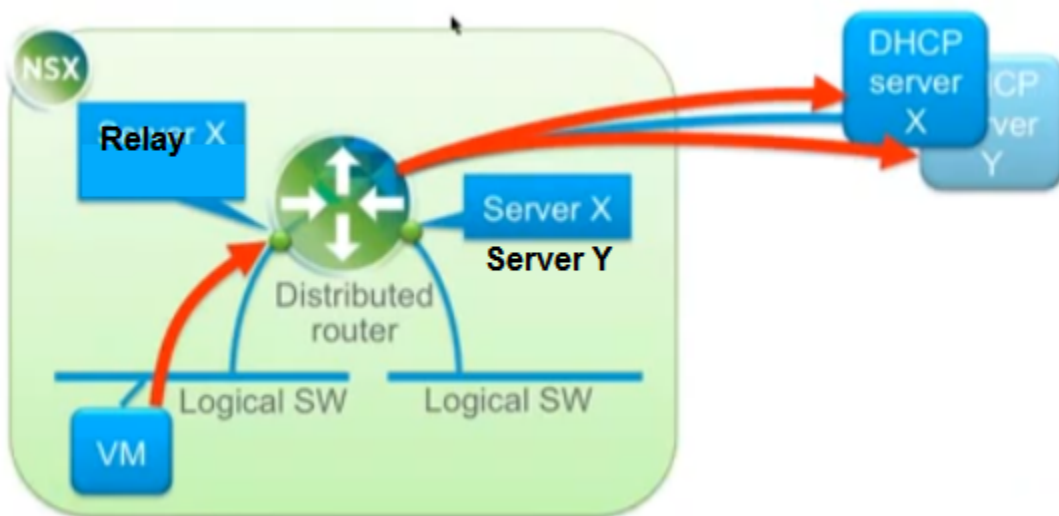
DHCP リレーの設定

DHCP (Dynamic Host Configuration Protocol) リレーを使用すると、環境で IP アドレス管理を中断することなく、NSX 内から既存の DHCP インフラストラクチャを活用することが可能になります。DHCP メッセージは、仮想マシンから、物理環境にある指定された DHCP サーバにリレーされます。これにより、NSX 内の IP アドレスが他の環境の IP アドレスと同期した状態を維持できます。

DHCP は分散論理ルーター ポートに適用され、複数の DHCP サーバがリストされる可能性があります。要求は、リストされたすべてのサーバに送信されます。DHCP 要求がクライアントからリレーされている間に、ゲートウェイ IP アドレスがその要求に追加されます。外部の DHCP サーバは、このゲートウェイ アドレスを使用してプールを照合し、要求に対する IP アドレスを割り当てます。ゲートウェイ アドレスは、リレーが実行されている NSX ポートのサブネットに属している必要があります。

複数の IP アドレスドメインをサポートするために、論理スイッチごとに異なる DHCP サーバを指定し、分散論理ルーターごとに複数の DHCP サーバを設定することができます。

DHCP サーバでプールおよびバインドを設定する場合、リレーされるクエリのプール/バインドのサブネット マスクが DHCP リレーのインターフェイスと同じであることを確認してください。サブネット マスク情報は、仮想マシンと DHCP サービスを提供する Edge の間で分散論理ルーターが DHCP リレーとして機能しているときに、API で提供する必要があります。このサブネット マスクは、分散論理ルーターの仮想マシンのゲートウェイ インターフェイスで設定したものと一致する必要があります。



注:

- DHCP リレーでは、重複する IP アドレス空間はサポートしません (オプション 82)。
- DHCP リレーと DHCP サービスを 1 つのポート/VNIC で同時に実行することはできません。ポート上でリレーエージェントが設定されている場合、DHCP プールをこのポートのサブネットに設定することはできません。

DHCP リレー サーバの追加

DHCP メッセージのリレー先となる外部リレー サーバを追加します。リレー サーバは、IP セット、IP アドレス ブロック、ドメイン、またはこれらのすべての組み合わせになります。メッセージは、リストされている各 DHCP サーバにリレーされます。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [NSX Edge (NSX Edges)] の順に移動します。
- 2 適切な Edge をダブルクリックして、[管理 (Manage)] - [DHCP] タブが開いていることを確認します。
- 3 [DHCP リレーのグローバル設定 (DHCP Relay Global Configuration)] の横にある [編集 (Edit)] をクリックします。
- 4 IP セットをサーバとして追加するには：
 - a [追加 (Add)] アイコンをクリックし、IP セットを選択します。
 - b  アイコンをクリックして、選択した IP セットを [選択したオブジェクト] リストに移動します。
 - c [OK] をクリックします。
- 5 IP アドレスまたはドメイン名を追加するには、適切な領域にアドレスまたは名前を入力します。
- 6 [OK] をクリックします。

リレー エージェントの追加

DHCP メッセージを外部 DHCP リレー サーバにリレーする Edge インターフェイスを追加します。

手順

- 1 [DHCP リレー エージェント (DHCP Relay Agents)] 領域で、[追加 (Add)] アイコンをクリックします。
- 2 [vNIC] で、内部 vNIC が選択されていることを確認します。

[ゲートウェイ IP アドレス (Gateway IP Address)] には、選択した vNIC のプライマリ IP アドレスが表示されます。
- 3 [OK] をクリックします。

DNS サーバの設定

NSX Edge がクライアントからの名前解決要求をリレーできる外部の DNS サーバを設定できます。NSX Edge は、クライアント アプリケーションの要求を DNS サーバにリレーし、ネットワーク名を完全に解決し、サーバからの応答をキャッシュします。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 [DNS (DNS Configuration)] パネルで、[変更 (Change)] をクリックします。
- 6 [DNS サービスの有効化 (Enable DNS Service)] をクリックして DNS サービスを有効にします。
- 7 両方の DNS サーバの IP アドレスを入力します。
- 8 必要に応じてデフォルトのキャッシュ サイズを変更します。
- 9 [ログの有効化 (Enable Logging)] をクリックして、DNS トラフィックのログを記録し、ログ レベルを選択します。
生成されたログは Syslog サーバに送信されます。
- 10 [OK] をクリックします。

Service Composer

Service Composer では、ネットワークおよびセキュリティ サービスを仮想インフラストラクチャ内のアプリケーションにプロビジョニングして割り当てることができます。これらのサービスをセキュリティ グループにマッピングすると、サービスがセキュリティ グループの仮想マシンに適用されます。

セキュリティ グループ

まず、保護する資産を定義するためにセキュリティ グループを作成します。セキュリティ グループは、固定（特定の仮想マシンを含む）または動的のどちらでもかまいません。動的の場合は、次の 1 つ以上の方法でメンバーシップを定義できます。

- vCenter コンテナ（クラスタ、ポート グループ、またはデータセンター）
- セキュリティ タグ、IPset、MACset、または他のセキュリティ グループ。たとえば、指定したセキュリティ タグ（AntiVirus.virusFound など）でタグ付けされたメンバーのすべてをセキュリティ グループに追加するための基準を含めることができます。
- ディレクトリ グループ（NSX Manager が Active Directory に登録されている場合）
- <VM1> という名前の仮想マシンなどの正規表現

セキュリティ グループ メンバーシップは常に変動します。たとえば、AntiVirus.virusFound タグが付けられた仮想マシンは、検疫セキュリティ グループに追加されます。ウイルスがクリーンアップされ、このタグが仮想マシンから削除されると、検疫セキュリティ グループから除外されます。

セキュリティ ポリシー

セキュリティ ポリシーは、次のサービス設定の集合体です。

表 17-1. セキュリティ ポリシーに含まれるセキュリティ サービス

サービス	説明	適用先
ファイアウォール ルール	セキュリティ グループとの間、またはセキュリティ グループ内で許可されるトラフィックを定義するルール。	vNIC
Endpoint サー ビス	Data Security、またはアンチウイルスや脆弱性管理サービスなどのサードパーティ ソリューション プロバイダのサービス。	仮想マシン
ネットワーク イン トロスペクション サービス	ネットワークを監視するサービス（IPS など）。	仮想マシン

NSX でのサービス デプロイ中、サード パーティ ベンダーはデプロイするサービスのサービス カテゴリを選択します。デフォルトのサービス プロファイルが、各ベンダー テンプレートに対して作成されます。

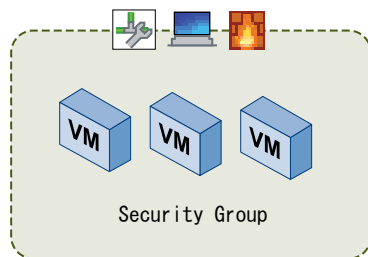
サード パーティ ベンダーのサービスが NSX 6.1 にアップグレードされるときに、アップグレードされるベンダー テンプレートに対してデフォルトのサービス プロファイルが作成されます。ゲスト イントロスペクション ルールを含む既存のサービス ポリシーは、アップグレード中に作成されたサービス プロファイルを参照するように更新されます。

セキュリティ グループへのセキュリティ ポリシーのマッピング

セキュリティ ポリシー (SP1 など) をセキュリティ グループ (SG1 など) にマッピングします。SP1 に設定されたサービスは、SG1 のメンバーであるすべての仮想マシンに適用されます。

注: 同じセキュリティ ポリシーを添付する必要がある多数のセキュリティ グループがある場合、1 つのアンブレラ セキュリティ グループを作成し、その中にそれらのすべての子セキュリティ グループを格納し、そのアンブレラ セキュリティ グループに共通セキュリティ ポリシーを適用します。これにより、NSX Distributed Firewall が ESXi ホスト メモリを効率的に利用することが保証されます。

図 17-1. Service Composer の概要



仮想マシンが複数のセキュリティ グループに属している場合は、セキュリティ グループにマッピングされたセキュリティ ポリシーの優先順位によって、仮想マシンに適用されるサービスが異なります。

Service Composer プロファイルは、他の環境で使用するためのバックアップとしてエクスポートおよびインポートできます。ネットワークおよびセキュリティ サービスをこの方法で管理すると、繰り返し可能で実用的なセキュリティ ポリシー管理を行うことができます。

この章には、次のトピックが含まれています。

- [Service Composer の使用](#)
- [Service Composer のグラフィック表示](#)
- [セキュリティ タグの操作](#)
- [有効なサービスの表示](#)
- [セキュリティ ポリシーの操作](#)
- [セキュリティ グループの編集](#)
- [Service Composer のシナリオ](#)

Service Composer の使用

Service Composer を使用すると、セキュリティ サービスを簡単に利用できます。

ここでは、例を追いながら、Service Composer がネットワークのエンドツーエンドの保護にどのように役立つかを確認しましょう。環境に次のセキュリティ ポリシーが定義されているとします。

- 脆弱性スキャン サービスを含む、初期状態のセキュリティ ポリシー (InitStatePolicy)
- ファイアウォール ルールとアンチウイルス サービスに加えてネットワーク IPS サービスを含む、修正セキュリティ ポリシー (RemPolicy)

RemPolicy の重み（優先順位）が InitStatePolicy の重みよりも高いことを確認します。

また、次のセキュリティ グループも設定しているとします。

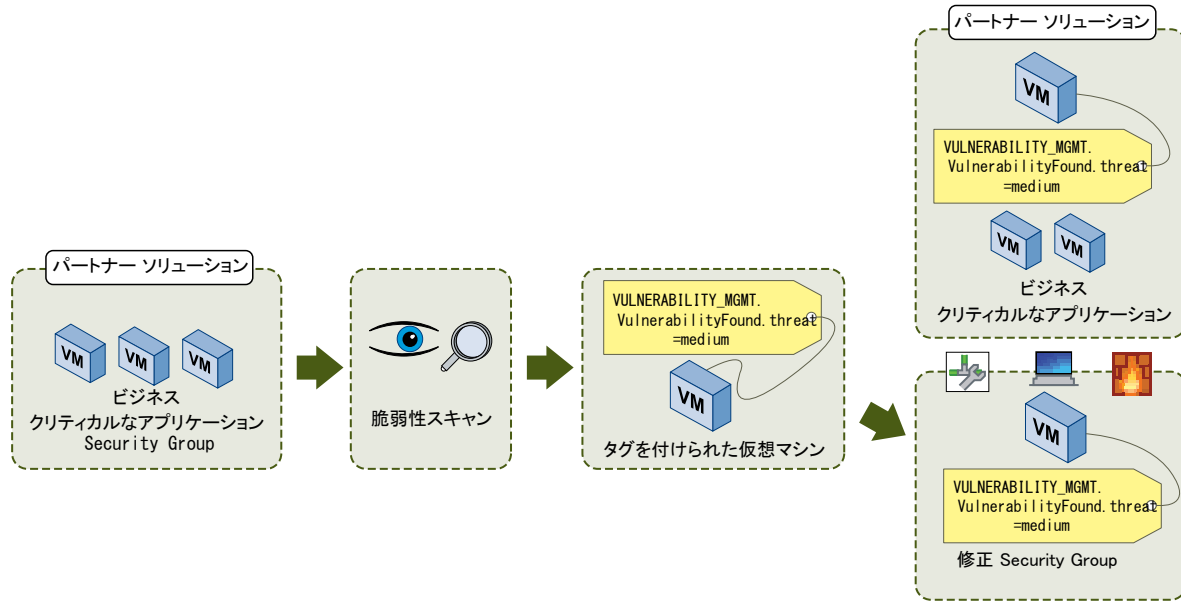
- 環境内のビジネス上重要なアプリケーションを含むアプリケーション資産グループ (AssetGroup)
- 仮想マシンが脆弱であることを示すタグ
(`VULNERABILITY_MGMT.VulnerabilityFound.threat=medium`) で定義された、RemGroup という名前の修正セキュリティ グループ

次に、InitStatePolicy を AssetGroup にマッピングして環境内のビジネス上重要なアプリケーションすべてを保護します。また、RemPolicy を RemGroup にマッピングして脆弱な仮想マシンも保護します。

脆弱性スキャンを開始すると、AssetGroup 内のすべての仮想マシンがスキャンされます。スキャンで脆弱性のある仮想マシンが特定された場合、`VULNERABILITY_MGMT.VulnerabilityFound.threat=medium` タグがその仮想マシンに適用されます。

Service Composer は即座にこのタグ付けされた仮想マシンを RemGroup に追加します。RemGroup ではネットワーク IPS ソリューションがすでに設定されており、この脆弱な仮想マシンが保護されます。

図 17-2. 動作中の Service Composer



次に、このトピックでは Service Composer が提供するセキュリティ サービスを使用するのに必要な手順について説明します。

1 Service Composer でのセキュリティ グループの作成

NSX Manager レベルでセキュリティ グループを作成できます。

2 セキュリティ ポリシーの作成

セキュリティ ポリシーは、セキュリティ グループに適用可能な一連の ゲスト イントロスペクション、ファイアウォール、およびネットワーク イントロスペクション サービスです。セキュリティ ポリシーが表示される順序は、ポリシーに関連付けられた重みによって決まります。デフォルトでは、新しいポリシーには、テーブルの最上位になるように最も大きい重みが割り当てられます。ただし、デフォルトの推奨される重みを変更して、新しいポリシーに割り当てられた順序を変更できます。

3 セキュリティ グループへのセキュリティ ポリシーの適用

セキュリティ ポリシーをセキュリティ グループに適用して、仮想デスクトップ、ビジネス上重要なアプリケーション、およびその間の接続を保護することができます。適用されなかったサービスと適用に失敗した理由のリストも表示できます。

Service Composer でのセキュリティ グループの作成

NSX Manager レベルでセキュリティ グループを作成できます。

手順

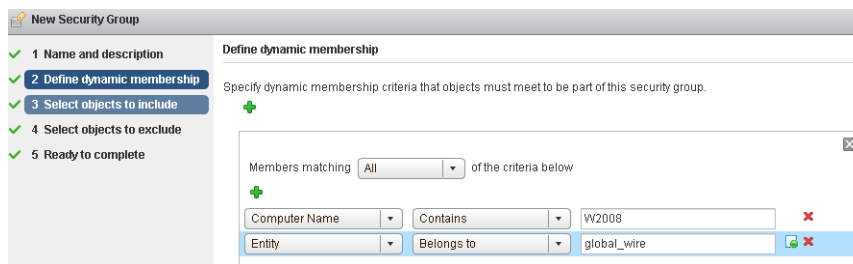
- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ グループ] タブをクリックし、[セキュリティ グループの追加] アイコンをクリックします。
- 4 セキュリティ グループの名前と説明を入力して、[次へ] をクリックします。

- 5 [動的メンバーシップ] ページで、作成中のセキュリティ グループに追加するオブジェクトが満たす必要のある基準を定義します。

たとえば、指定したセキュリティ タグ (AntiVirus.virusFound など) でタグ付けされたメンバーのすべてをセキュリティ グループに追加するための基準を含めることができます。セキュリティ タグでは大文字と小文字が区別されます。

注: 特定のセキュリティ タグが適用された仮想マシンでセキュリティ グループを定義する場合、動的ワークフローまたは条件付きワークフローを作成できます。タグが仮想マシンに適用されるとすぐに、仮想マシンは自動的にそのセキュリティ グループに追加されます。

または、**W2008** という名前を含むすべての仮想マシンや、論理スイッチ **global_wire** に含まれる仮想マシンをセキュリティ グループに追加することもできます。



- 6 [次へ] をクリックします。
- 7 [含めるオブジェクトの選択] ページで、ドロップダウンからオブジェクト タイプを選択します。
- 8 含めるリストに追加するオブジェクトをダブルクリックします。セキュリティ グループには次のオブジェクトを含めることができます。

- 作成中のセキュリティ グループ内にネストされた他のセキュリティ グループ。
- クラスタ
- 論理スイッチ
- ネットワーク
- 仮想 App
- データセンター
- IP セット
- Active Directory グループ

注: NSX セキュリティ グループの Active Directory 設定は、vSphere SSO の Active Directory 設定とは異なります。NSX Active Directory グループの設定はゲスト仮想マシンにアクセスするエンド ユーザー用であり、vSphere SSO は vSphere および NSX を使用する管理者用です。

- MAC セット
- セキュリティ タグ
- vNIC

- 仮想マシン
- リソース プール
- 分散仮想ポート グループ

ここで選択したオブジェクトは、動的基準を満たすかどうかにかかわらず、常にセキュリティ グループに含まれます。

セキュリティ グループに 1 つのリソースを追加すると、関連するすべてのリソースも自動的に追加されます。たとえば、仮想マシンを選択すると、関連する vNIC が自動的にそのセキュリティ グループに追加されます。

- 9 [次へ] をクリックして、セキュリティ グループから除外するオブジェクトをダブルクリックします。

ここで選択されるオブジェクトは、動的基準に一致する場合や含めるリストに選定されている場合でも、常にセキュリティ グループから除外されます。

- 10 [終了] をクリックします。

セキュリティ グループのメンバーシップは、次のように決まります。

{式の結果 (手順 5 で生成) + 含まれるアイテム (手順 8 で指定)} - 除外されるアイテム (手順 9 で指定)

つまり、含めるアイテムが最初に式の結果に追加されます。次に、除外されるアイテムが、結合された結果から差し引かれます。

セキュリティ ポリシーの作成


セキュリティ ポリシーは、セキュリティ グループに適用可能な一連の ゲスト イントロスペクション、ファイアウォール、およびネットワーク イントロスペクション サービスです。セキュリティ ポリシーが表示される順序は、ポリシーに関連付けられた重みによって決まります。デフォルトでは、新しいポリシーには、テーブルの最上位になるように最も大きい重みが割り当てられます。ただし、デフォルトの推奨される重みを変更して、新しいポリシーに割り当てられた順序を変更できます。

前提条件

次のように設定されていることを確認します。

- 必要な VMware 組み込みサービス (Distributed Firewall、Data Security、ゲスト イントロスペクション など) がインストールされている。
- 必要なパートナー サービスが NSX Manager サービスに登録されている。
- デフォルトの適用先設定が Service Composer のファイアウォールルールに設定されている。[\[Service Composer ファイアウォールの適用先設定の編集\]](#) を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー] タブをクリックします。
- 4 [Security Policy の作成] () アイコンをクリックします。

- 5 [セキュリティ ポリシーの追加] ダイアログ ボックスで、セキュリティ ポリシーの名前を入力します。

- 6 セキュリティ ポリシーの説明を入力します。


NSX では、ポリシーにデフォルトの重み（最大の重み + 1000）が割り当てられます。たとえば、既存のポリシーの最大の重みが 1200 の場合、新しいポリシーには重み 2200 が割り当てられます。

セキュリティ ポリシーはその重みに応じて適用されます。つまり、重みが大きいポリシーは重みが小さいポリシーよりも優先順位が高くなります。

- 7 作成しているポリシーで別のセキュリティ ポリシーからサービスを受け取るには、[指定したポリシーからセキュリティ ポリシーを継承] を選択します。親ポリシーを選択します。

新しいポリシーでは、親ポリシーからすべてのサービスが継承されます。

- 8 [次へ] をクリックします。

- 9 [ゲスト イントロスペクション サービス] ページで、[ゲスト イントロスペクション サービスの追加] () アイコンをクリックします。

- a [ゲスト イントロスペクション サービスの追加] ダイアログ ボックスで、サービスの名前と説明を入力します。

- b サービスを適用するか、ブロックするかを指定します。

セキュリティ ポリシーを継承する場合に、親ポリシーからのサービスをブロックするように選択することもできます。

サービスを適用する場合、サービスとサービス プロファイルを選択する必要があります。サービスをブロックする場合、ブロックするサービスのタイプを選択する必要があります。

- c サービスのブロックを選択する場合、サービスのタイプを選択します。

[Data Security] を選択した場合、データ セキュリティ ポリシーが設定されている必要があります。章 19 [「Data Security」](#) を参照してください。

- d ゲスト イントロスペクション サービスの適用を選択する場合、☐ サービス名を選択します。

選択したサービスのデフォルトのサービス プロファイルが表示されます。これには、関連付けられたベンダー テンプレートでサポートされているサービス機能タイプの情報が含まれます。

- e [状態] で、選択したゲスト イントロスペクション サービスを有効にするか、無効にするかを指定します。


ゲスト イントロスペクション サービスを、後で有効にするサービスのプレースホルダとして追加できます。これは、サービスをオンデマンドで追加する必要がある場合に（新しいアプリケーションなど）特に便利です。

- f ゲスト イントロスペクション サービスを適用するかどうかを選択します (オーバーライドできません)。選択したサービス プロファイルで複数のサービス機能タイプがサポートされている場合、これは、デフォルトで [強制] に設定されており、変更できません。


セキュリティ ポリシーで ゲスト イントロスペクション サービスを適用する場合、このセキュリティ ポリシーを継承する他のポリシーでは、他の子ポリシーより前にこのポリシーを適用する必要があります。このサービスが適用されていない場合、継承の選択により、子ポリシーが適用された後に親ポリシーが追加されます。

- g [OK] をクリックします。

上記の手順に従ってさらにゲスト イントロスペクションサービスを追加できます。ゲスト イントロスペクション サービスは、サービス テーブルの上にあるアイコンを使用して管理できます。

このページのサービスをエクスポートまたはコピーするには、[ゲスト イントロスペクション サービス] ページの右下にある  アイコンをクリックします。

- 10 [次へ] をクリックします。

- 11 [ファイアウォール] ページで、[ファイアウォール ルールの追加] () アイコンをクリックします。

ここで、このセキュリティ ポリシーが適用されるセキュリティ グループのファイアウォールルールを定義します。


- a 追加するファイアウォール ルールの名前と説明を入力します。
- b [許可] または [ブロック] を選択して、選択された送信先へのトラフィックをルールが許可するか、ブロックするかを示します。
- c ルールの送信元を選択します。デフォルトでは、ルールは、このポリシーが適用されるセキュリティ グループから受信するトラフィックに適用されます。デフォルトの送信元を変更するには、[変更] をクリックし、適切なセキュリティ グループを選択します。
- d ルールの送信先を選択します。

注: [ソース] または [ターゲット] (あるいはその両方) が、このポリシーの適用対象セキュリティ グループである必要があります。

たとえば、デフォルトの送信元でルールを作成し、[ターゲット] に Payroll を指定し、[ターゲットの無効化] を選択したとします。次に、このセキュリティ ポリシーを Engineering というセキュリティ グループに適用します。これにより、Engineering は Payroll サーバを除くすべてにアクセスできるようになります。

- e ルールを適用するサービスまたはサービス グループ、あるいはその両方を選択します。
- f [有効] または [無効] を選択してルールの状態を指定します。
- g このルールに一致するセッションをログに記録するには、[ログ] を選択します。
ログを有効にするとパフォーマンスに影響が出る場合があります。
- h [OK] をクリックします。

上記の手順に従ってさらにファイアウォール ルールを追加できます。ファイアウォール ルールは、ファイアウォール テーブルの上にあるアイコンを使用して管理できます。

このページのルールをエクスポートまたはコピーするには、[ファイアウォール] ページの右下にある  アイコンをクリックします。

ここで追加したファイアウォール ルールは、ファイアウォール テーブルに表示されます。ファイアウォール テーブルの Service Composer ルールは編集しないことをお勧めします。緊急のトラブルシューティングで編集が必要な場合は、[セキュリティ ポリシー] タブの [アクション] メニューから [ファイアウォールのルールを同期しますか?] を選択して、Service Composer ルールをファイアウォール ルールと再同期する必要があります。


12 [次へ] をクリックします。

[ネットワーク イントロスペクション サービス] ページには、VMware 仮想環境と統合した NetX サービスが表示されます。

13 [ネットワーク イントロスペクション サービスの追加] () アイコンをクリックします。

- a [ネットワーク イントロスペクション サービスの追加] ダイアログ ボックスで、追加するサービスの名前と説明を入力します。
- b サービスにリダイレクトするかどうかを選択します。
- c サービスの名前とプロファイルを選択します。
- d 転送元と転送先を選択します。
- e 追加するネットワーク サービスを選択します。
選択したサービスに基づいて追加の選択を行うことができます。
- f サービスを有効にするか、無効にするかを選択します。
- g このルールに一致するセッションをログに記録するには、[ログ] を選択します。
- h [OK] をクリックします。

上記の手順に従ってさらにネットワーク イントロスペクション サービスを追加できます。ネットワーク イントロスペクション サービスは、サービス テーブルの上にあるアイコンを使用して管理できます。

このページのサービスをエクスポートまたはコピーするには、[ネットワーク イントロスペクション サービス] ページの右下にある  アイコンをクリックします。

注: Service Composer ポリシーで使用されるサービス プロファイル用に手動で作成したバインドが上書きされます。

14 [終了] をクリックします。

セキュリティ ポリシーがポリシー テーブルに追加されます。ポリシーに関連付けられたサービスのサマリの表示、サービス エラーの表示、またはサービスの編集を行うには、ポリシー名をクリックし、適切なタブを選択します。

次のステップ

セキュリティ ポリシーをセキュリティ グループにマッピングします。

Service Composer ファイアウォールの適用先設定の編集

Service Composer から作成されたすべてのファイアウォール ルールの適用先を、分散ファイアウォールまたはポリシーのセキュリティ グループに設定できます。デフォルトでは、適用先は分散ファイアウォールに設定されています。

Service Composer ファイアウォール ルールの適用先が分散ファイアウォールに設定されているとき、ルールは分散ファイアウォールがインストールされているすべてのクラスタに適用されます。ファイアウォール ルールがポリシーのセキュリティ グループに適用されるように設定されている場合は、ファイアウォール ルールをより詳細に制御できます。ただし、場合によっては、複数のセキュリティ ポリシーまたはファイアウォール ルールが必要になります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] > [Service Composer] > [セキュリティ ポリシー (Security Policies)] タブの順にクリックします。
- 3 [アクション (Actions)] - [ファイアウォール ポリシー設定の編集 (Edit Firewall Policy Settings)] をクリックします。[適用先] のデフォルト設定を選択して、[OK] をクリックします。

オプション	説明
分散ファイアウォール	ファイアウォール ルールは、分散ファイアウォールがインストールされているすべてのクラスタに適用されます。
ポリシーのセキュリティ グループ	ファイアウォール ルールは、セキュリティ ポリシーが適用されているセキュリティ グループに適用されます。

適用先のデフォルト設定は、API を介して表示や変更ができます。『NSX API ガイド』を参照してください。

例：適用先の動作

ここに例として示すシナリオでは、ファイアウォール ルールのデフォルトのアクションが「ブロック」に設定されています。セキュリティ グループは「web-servers」と「app-servers」の2種類あり、それぞれ仮想マシンが含まれます。次のファイアウォール ルールを含むセキュリティ ポリシー allow-ssh-from-web を作成し、これをセキュリティ グループの「app-servers」に適用します。

- 名前：allow-ssh-from-web
- ソース：web-servers
- ターゲット：ポリシーのセキュリティ グループ
- サービス：ssh
- アクション：許可

ファイアウォール ルールが分散ファイアウォールに適用される場合は、セキュリティ グループ「web-servers」の仮想マシンからセキュリティ グループ「app-servers」の仮想マシンに対して SSL 通信を使用できます。

ファイアウォール ルールがポリシーのセキュリティ グループに適用される場合は、「app-servers」へのトラフィックがブロックされるため、SSL 通信を使用できません。「app-servers」への SSL 通信を許可するための追加のセキュリティ ポリシーを作成して、このポリシーをセキュリティ グループ「web-servers」に適用する必要があります。


- 名前：allow-ssh-to-app

- ソース：ポリシーのセキュリティ グループ
- ターゲット：app-servers
- サービス：ssh
- アクション：許可

セキュリティ グループへのセキュリティ ポリシーの適用

セキュリティ ポリシーをセキュリティ グループに適用して、仮想デスクトップ、ビジネス上重要なアプリケーション、およびその間の接続を保護することができます。適用されなかったサービスと適用に失敗した理由のリストも表示できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー (Security Policy)] タブをクリックします。
- 4 セキュリティ ポリシーを選択し、[セキュリティ ポリシーの適用 (Apply Security Policy)]  アイコンをクリックします。
- 5 ポリシーを適用するセキュリティ グループを選択します。

特定のセキュリティ タグが適用されている仮想マシンによって定義されるセキュリティ グループを選択した場合、動的または条件付きワークフローを作成できます。タグが仮想マシンに適用されるとすぐに、仮想マシンは自動的にそのセキュリティ グループに追加されます。

ポリシーに関連付けられた ネットワーク イントロスペクション ルールおよび Endpoint ルールは、IPSet および MacSet のメンバー（またはそのいずれか）を含むセキュリティ グループに対しては、有効になりません。

- 6 選択したセキュリティ グループに適用できないサービスと失敗した理由を表示するには、[サービス ステータスのプレビュー (Preview Service Status)] アイコンをクリックします。

たとえば、セキュリティ グループに含まれている仮想マシンが属するクラスタに、ポリシー サービスのいずれかがインストールされていない場合があります。セキュリティ ポリシーが目的どおりに機能するには、そのサービスを該当するクラスタにインストールする必要があります。

- 7 [OK] をクリックします。

Service Composer のグラフィック表示

Service Composer のキャンバス ビューでは、選択された NSX Manager 内のすべてのセキュリティ グループを表示できます。このビューにはまた、各セキュリティ グループのメンバーやセキュリティ グループに適用されているセキュリティ ポリシーなどの詳細も表示されます。

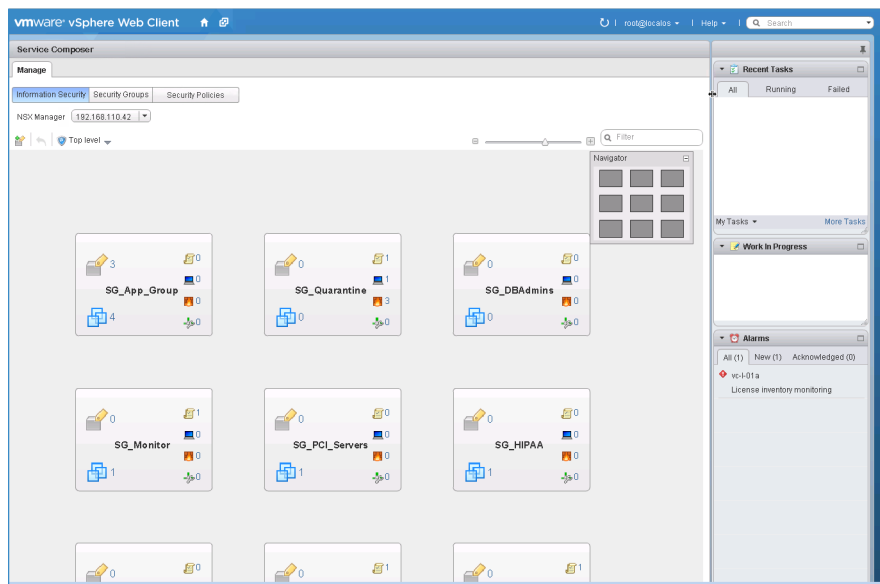
ここでは、部分的に設定されたシステムで Service Composer の手順を追うことで、キャンバス ビューから概要レベルでセキュリティ グループと Security Policy Object 間のマッピングを視覚的に理解する方法を説明します。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [キャンパス] タブをクリックします。

選択された NSX Manager 内のすべてのセキュリティ グループ（他のセキュリティ グループには含まれていないもの）が、適用されているポリシーとともに表示されます。[NSX Manager] ドロップダウン リストには、現在ログインしているユーザーにロールが割り当てられている NSX Manager がすべて表示されます。


図 17-3. Service Composer キャンパスの最上位レベル ビュー



キャンパスに表示される長方形のボックスはそれぞれセキュリティ グループを表し、ボックス内のアイコンはセキュリティ グループ メンバーとセキュリティ グループにマッピングされているセキュリティ ポリシーに関する詳細を表します。

図 17-4. セキュリティ グループ

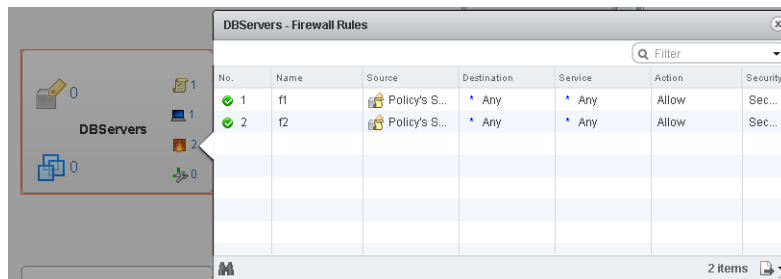


各アイコンの横にある数値は、インスタンス数を示します。たとえば、 1 は、そのセキュリティ グループに 1 個のセキュリティ ポリシーがマッピングされていることを示します。

アイコン	クリックして表示
	メインのセキュリティ グループ内にネストされているセキュリティ グループ。
	メインのセキュリティ グループとネストされているセキュリティ グループに現在含まれる仮想マシン。サービス エラーのある仮想マシンを表示するには、[エラー] タブをクリックします。
	セキュリティ グループにマッピングされた有効なセキュリティ ポリシー。 <ul style="list-style-type: none"> ■ 新しいセキュリティ ポリシーを作成するには、[Security Policy の作成] () アイコンをクリックします。新しく作成された Security Policy Object は、自動的にセキュリティ グループにマッピングされます。 ■ セキュリティ グループに追加のセキュリティ ポリシーをマッピングするには、[セキュリティ ポリシーの適用] () アイコンをクリックします。
	セキュリティ グループにマッピングされたセキュリティ ポリシーに関連付けられた有効な Endpoint サービス。2 つのポリシーがセキュリティ グループに適用されていて、どちらにも同じカテゴリの Endpoint サービスが設定されているとします。この場合、有効なサービス数は 1 です (2 つ目の優先度が低い方のサービスはオーバーライドされるため)。 Endpoint サービスの障害があった場合は、アラート アイコンで示されます。アイコンをクリックするとエラーが表示されます。
	セキュリティ グループにマッピングされたセキュリティ ポリシーに関連付けられた有効なファイアウォール ルール。 失敗したサービスがある場合、アラート アイコンで示されます。アイコンをクリックするとエラーが表示されます。
	セキュリティ グループにマッピングされたセキュリティ ポリシーに関連付けられた有効なネットワーク イントロスペクション サービス。 失敗したサービスがある場合、アラート アイコンで示されます。アイコンをクリックするとエラーが表示されます。

アイコンをクリックすると、適切な詳細がダイアログ ボックスに表示されます。

図 17-5. セキュリティ グループでアイコンをクリックすると表示される詳細



セキュリティ グループを名前で検索できます。たとえば、キャンパス ビューの右上隅にある検索フィールドに PCI と入力すると、名前に PCI が含まれるセキュリティ グループのみが表示されます。

セキュリティ グループ階層を表示するには、ウィンドウ左上部にある [トップ レベル] (▼) アイコンをクリックして、表示するセキュリティ グループを選択します。セキュリティ グループにネストされたセキュリティ グループが含まれる場合、▶ をクリックするとネストされているグループが表示されます。上部バーには親セキュリティ グループの名前が表示され、バーのアイコンには、親グループに適用されるセキュリティ ポリシー、Endpoint サービス、ファイアウォール サービス、およびネットワーク イントロスペクション サービスの総数が表示されます。元の最上位レベルに戻るには、ウィンドウの左上部分にある [1 つ上のレベルへ移動] (↶) アイコンをクリックします。

キャンバス ビューのズーム イン/アウトをスムーズに行うには、ウィンドウの右上隅にあるズーム スライダを動かします。[ナビゲータ] ボックスに、キャンバス全体のズームアウト ビューが表示されます。キャンバスが大きすぎて画面に収まらない場合、実際に表示されている領域の周囲にボックスが表示され、そのボックスを動かしてキャンバスの表示される部分を変更できます。

次のステップ

これでセキュリティ グループとセキュリティ ポリシー間のマッピングの仕組みを確認できたので、セキュリティ ポリシーの作成を開始して、セキュリティ グループに適用するセキュリティ サービスを定義できます。

セキュリティ ポリシーへのセキュリティ グループのマッピング

選択されたセキュリティ グループをセキュリティ ポリシーにマッピングできます。

手順

- 1 セキュリティ グループに適用するセキュリティ ポリシーを選択します。
- 2 新しいポリシーを作成するには、[新規セキュリティ グループ] を選択します。
[「セキュリティ ポリシーの作成」](#) を参照してください。
- 3 [保存 (Save)] をクリックします。

セキュリティ タグの操作

仮想マシンに適用されているセキュリティ タグを表示したり、ユーザー定義のセキュリティ タグを作成したりすることができます。

適用されているセキュリティ タグの表示

環境内の仮想マシンに適用されているセキュリティ タグを表示できます。

前提条件

データ セキュリティまたはアンチウイルスのスキャンが実行済みで、適切な仮想マシンにタグが適用済みである必要があります。

注: サードパーティのソリューションによって適用されたタグの詳細については、そのソリューションのドキュメントを参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 [セキュリティ タグ] タブをクリックします。

環境内で適用されたタグのリストが、タグを適用した仮想マシンの詳細とともに表示されます。特定のタグを使用する仮想マシンを含めるためにセキュリティ グループを追加する予定の場合は、正確なタグ名をメモしておいてください。

- 5 [仮想マシン数] 列の数値をクリックすると、その行でそのタグが適用された仮想マシンが表示されます。

セキュリティ タグの追加

セキュリティ タグを手動で追加し、仮想マシンに適用できます。これは、環境内で NETX 以外のソリューションを利用している場合に特に便利です。また、これによって、NSX Manager を使用したソリューション タグの登録ができなくなります。

前提条件

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 [セキュリティ タグ (Security Tags)] タブをクリックします。
- 5 [新規セキュリティ タグ (New Security Tag)] () アイコンをクリックします。
- 6 タグの名前と説明を入力し、[OK] をクリックします。

セキュリティ タグの割り当て

動的なメンバーシップ ベースのセキュリティ タグを使用して条件付きワークフローを作成するほか、仮想マシンに手動でセキュリティ タグを割り当てることができます。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 [セキュリティ タグ (Security Tags)] タブをクリックします。

- 5 セキュリティ タグを選択し、[セキュリティ タグの割り当て (Assign Security Tag)] ( アイコンをクリックします。
- 6 1 つ以上の仮想マシンを選択し、[OK] をクリックします。

セキュリティ タグの編集

ユーザー定義のセキュリティ タグを編集できます。編集するタグに特定の Security Group が基づいている場合、そのタグへの変更は Security Group メンバーシップに影響します。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 [セキュリティ タグ (Security Tags)] タブをクリックします。
- 5 セキュリティ タグを選択して [セキュリティ タグの編集 (Edit Security Tag)] () アイコンをクリックします。
- 6 必要な変更を行い、[OK] をクリックします。

セキュリティ タグの削除

ユーザー定義のセキュリティ タグを削除できます。特定のセキュリティ グループが削除するタグに基づいている場合、そのタグへの変更はセキュリティ グループ メンバーシップに影響します。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Manager (NSX Managers)] をクリックします。
- 3 [名前 (Name)] 列で NSX Manager をクリックし、[管理 (Manage)] タブをクリックします。
- 4 [セキュリティ タグ (Security Tags)] タブをクリックします。
- 5 セキュリティ タグを選択して [セキュリティ タグの削除 (Delete Security Tag)] () アイコンをクリックします。

有効なサービスの表示

Security Policy Object または仮想マシンで有効なサービスを表示できます。

セキュリティ ポリシーの有効なサービスの表示

セキュリティ ポリシーで有効なサービスを表示できます。このサービスには、親ポリシーから継承したサービスが含まれます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー (Security Policies)] タブをクリックします。
- 4 [名前 (Name)] 列のセキュリティ ポリシーをクリックします。
- 5 [管理 (Manage)] - [情報セキュリティ (Information Security)] タブが開かれていることを確認します。

3 つのタブ ([エンドポイント サービス (Endpoint Services)]、[ファイアウォール (Firewall)]、[ネットワーク イントロスペクション サービス (Network Introspection Services)]) それぞれに、対応するセキュリティ ポリシーのサービスが表示されます。

有効になっていないサービスは淡色表示されます。[オーバーライドされました (Overridden)] 列に実際にセキュリティ ポリシーに適用されているサービスが表示され、[継承元 (Inherited from)] 列にサービスの継承元のセキュリティ ポリシーが表示されます。

セキュリティ ポリシーのサービス障害の表示

セキュリティ ポリシーにマッピングされたセキュリティ グループへの適用で障害が発生した、セキュリティ ポリシーに関連付けられているサービスを表示できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー (Security Policies)] タブをクリックします。
- 4 [名前 (Name)] 列のセキュリティ ポリシーをクリックします。
- 5 [監視 (Monitor)] - [サービス エラー (Service Errors)] タブが開かれていることを確認します。

[ステータス (Status)] 列内のリンクをクリックすると [サービス デプロイ] ページが表示され、サービス エラーを修正できます。

仮想マシンでの有効なサービスの表示

仮想マシンで有効なサービスを表示できます。1 台の仮想マシンに複数のセキュリティ ポリシーが適用されている場合 (仮想マシンが、ポリシーがマッピングされた複数のセキュリティ グループに含まれる場合)、この表示には、これらのポリシーすべてで有効なすべてのサービスが、適用された順序で一覧表示されます。[サービス ステータス] 列には、各サービスのステータスが表示されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [vCenter] をクリックし、[仮想マシン (Virtual Machines)] をクリックします。
- 3 [名前 (Name)] 列の仮想マシンをクリックします。

4 [監視 (Monitor)] - [Service Composer] タブが開かれていることを確認します。

セキュリティ ポリシーの操作

セキュリティ ポリシーは、ネットワーク サービスとセキュリティ サービスのグループです。

次のネットワーク サービスとセキュリティ サービスは、セキュリティ ポリシーとしてグループ化できます。




- Endpoint サービス - データ セキュリティ、アンチウィルス、および脆弱性の管理
- Distributed Firewall ルール
- ネットワーク イントロスペクション サービス - ネットワーク IPS とネットワーク フォレンジック

セキュリティ ポリシーの優先順位の管理

セキュリティ ポリシーはその重みに応じて適用されます。つまり、重みが大きいポリシーほど、優先順位が高くなります。テーブル内でポリシーの位置を上下に移動すると、それに応じてポリシーの重みが調整されます。

仮想マシンを含むセキュリティ グループに複数のポリシーが関連付けられているか、異なるポリシーが関連付けられている複数のセキュリティ グループに仮想マシンが含まれているため、1 台の仮想マシンに複数のセキュリティ ポリシーが適用されることがあります。それぞれのポリシーを使用してグループ化されたサービスの間に競合がある場合は、ポリシーの重みによって、仮想マシンに適用されるサービスが決まります。たとえば、インターネット アクセスをブロックするポリシー 1 は重みの値が 1000 で、インターネット アクセスを許可するポリシー 2 は重みの値が 2000 であるとしてします。この場合は、ポリシー 2 の重みが大きいため、仮想マシンではインターネット アクセスが許可されます。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー (Security Policies)] タブをクリックします。
- 4 [優先順位の管理 (Manage Precedence)] () アイコンをクリックします。
- 5 [優先順位の管理] ダイアログ ボックスで、優先順位を変更するセキュリティ ポリシーを選択し、[上へ移動 (Move Up)] () または [下へ移動 (Move Down)] () アイコンをクリックします。
- 6 [OK] をクリックします。

セキュリティ ポリシーの編集

セキュリティ ポリシーの名前、説明、関連付けられているサービスおよびルールを編集できます。

手順


- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー (Security Policies)] タブをクリックします。

- 4 編集するセキュリティ ポリシーを選択し、[セキュリティ ポリシーの編集 (Edit Security Policy)] () アイコンをクリックします。
- 5 [セキュリティ ポリシーの編集] ダイアログ ボックスで必要な変更を行い、[終了 (Finish)] をクリックします。

セキュリティ ポリシーの削除

セキュリティ ポリシーを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ ポリシー (Security Policies)] タブをクリックします。
- 4 削除するセキュリティ ポリシーを選択し、[セキュリティ ポリシーの削除 (Delete Security Policy)] () アイコンをクリックします。

セキュリティ グループの編集

セキュリティ グループを編集できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ グループ] タブをクリックします。
- 4 編集するセキュリティ グループを選択し、[セキュリティ グループの編集] アイコンをクリックします。
- 5 必要な変更を行い、[OK] をクリックします。

Service Composer のシナリオ

このセクションでは、Service Composer の仮説シナリオをいくつか説明します。各使用事例では、Security Administrator ロールがすでに作成され、管理者に割り当てられていることが前提となっています。

感染しているマシンを隔離するシナリオ

Service Composer では、サードパーティのアンチウイルス ソリューションを使用して感染しているシステムをネットワークで識別し、感染の拡散を防止します。

サンプル シナリオでは、デスクトップを完全に保護する方法を示します。

図 17-6. Service Composer の設定

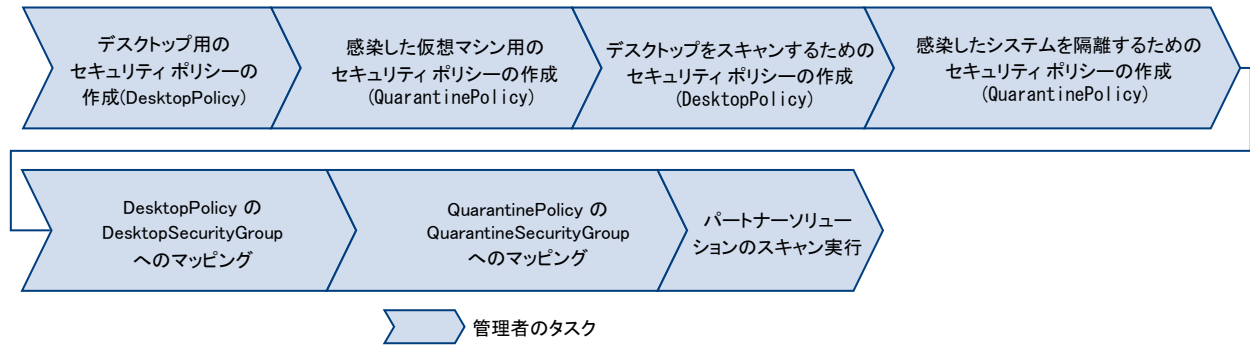
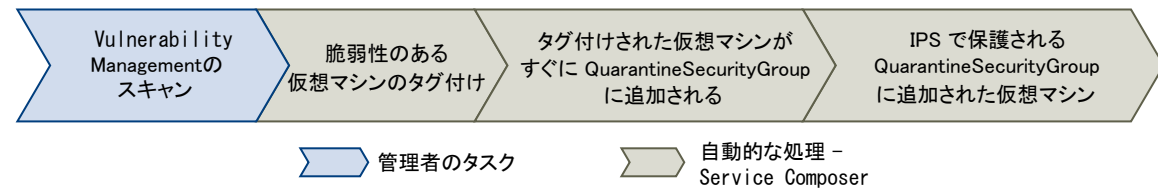


図 17-7. Service Composer の条件付きワークフロー




前提条件

Symantec によって、感染した仮想マシンに **AntiVirus.virusFound** というタグが付けられることがわかっています。


手順

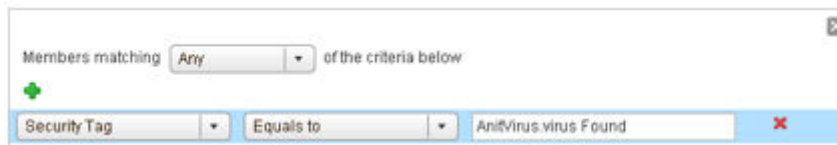
- 1 Symantec アンチマルウェア ソリューションをインストール、登録、デプロイします。
- 2 デスクトップにセキュリティ ポリシーを作成します。
 - a [セキュリティ ポリシー (Security Policies)] タブをクリックし、[セキュリティ ポリシーの追加 (Add Security Policy)] アイコンをクリックします。
 - b [名前 (Name)] に **DesktopPolicy** と入力します。
 - c [説明 (Description)] に、**Antivirus scan for all desktops** と入力します。
 - d 重みを 51000 に変更します。他のすべてのポリシーより常に優先されるようにするため、このポリシーの優先順位は非常に高く設定されています。
 - e [次へ (Next)] をクリックします。

- f [Endpoint サービスの追加] ページで、 をクリックし、次の値を入力します。

オプション	値
[アクション (Action)]	デフォルト値は変更しないでください
[サービス種別 (Service Type)]	Anti Virus
[サービス名 (Service Name)]	Symantec アンチマルウェア
[サービス設定 (Service Configuration)]	シルバー
[状態 (State)]	デフォルト値は変更しないでください
[強制 (Enforce)]	デフォルト値は変更しないでください
[名前 (Name)]	デスクトップ AV
[説明 (Description)]	すべてのデスクトップに適用する必須ポリシー

- g [OK] をクリックします。
- h ファイアウォールまたはネットワーク イントロスペクション サービスを追加せずに、[終了 (Finish)] をクリックします。
- 3 感染している仮想マシンにセキュリティ ポリシーを作成します。
- a [セキュリティ ポリシー (Security Policies)] タブをクリックし、[セキュリティ ポリシーの追加 (Add Security Policy)] アイコンをクリックします。
- b [名前] に **QuarantinePolicy** と入力します。
- c [説明] に、**Policy to be applied to all infected systems.** と入力します。
- d デフォルトの重みは変更しないでください。
- e [次へ (Next)] をクリックします。
- f [Endpoint サービスの追加] ページでは何も行わず、[次へ (Next)] をクリックします。
- g [ファイアウォール] で 3 つのルール (すべての送信トラフィックをブロックするルール、グループを使用してすべてのトラフィックをブロックするルール、修正ツールからの受信トラフィックのみ許可するルール) を追加します。
- h ネットワーク イントロスペクション サービスを追加せずに、[終了 (Finish)] をクリックします。
- 4 **QuarantinePolicy** をセキュリティ ポリシー テーブルの一番上に移動して、他のすべてのポリシーより確実に先に適用されるようにします。
- a [優先順位の管理 (Manage Priority)] アイコンをクリックします。
- b **QuarantinePolicy** を選択し、[上へ移動 (Move Up)] アイコンをクリックします。
- 5 環境内のすべてのデスクトップにセキュリティ グループを作成します。
- a vSphere Web Client にログインします。
- b [ネットワークとセキュリティ (Networking & Security)] をクリックし、[Service Composer] をクリックします。

- c [セキュリティ グループ (Security Groups)] タブをクリックし、[セキュリティ グループの追加 (Add Security Group)] アイコンをクリックします。
 - d [名前] に **DesktopSecurityGroup** と入力します。
 - e [説明] に、**All desktops** と入力します。
 - f 次の数ページで [次へ (Next)] をクリックします。
 - g [設定内容の確認] ページで選択内容を確認し、[終了 (Finish)] をクリックします。
- 6 感染している仮想マシンを配置する検疫セキュリティ グループを作成します。
- a [セキュリティ グループ (Security Groups)] タブをクリックし、[セキュリティ グループの追加 (Add Security Group)] アイコンをクリックします。
 - b [名前 (Name)] に **QuarantineSecurityGroup** と入力します。
 - c [説明 (Description)] に、
Dynamic group membership based on infected VMs identified by the antivirus scan と入力します。
 - d [メンバーシップ基準の定義] ページで、 をクリックし、次の基準を追加します。



- e [含めるオブジェクトの選択] ページおよび [除外するオブジェクトの選択] ページでは何も行わず、[次へ (Next)] をクリックします。
 - f [設定内容の確認] ページで選択内容を確認し、[終了 (Finish)] をクリックします。
- 7 **DesktopPolicy** ポリシーを **DesktopSecurityGroup** セキュリティ グループにマッピングします。
- a [セキュリティ ポリシー] タブで、**DesktopPolicy** ポリシーが選択されていることを確認します。
 - b [セキュリティ ポリシーの適用 (Apply Security Policy)]  アイコンをクリックし、SG_Desktops グループを選択します。
 - c [OK] をクリックします。
- このマッピングにより、アンチウイルス スキャンがトリガーされたときに、すべてのデスクトップ (**DesktopSecurityGroup** の一部) が確実にスキャンされます。
- 8 キャンバス ビューに移動して、**QuarantineSecurityGroup** に仮想マシンがまだ含まれていないことを確認します。
- a [情報セキュリティ (Information Security)] タブをクリックします。
 - b  グループ内の仮想マシンが 0 であることを確認します ()。

9 QuarantinePolicy を QuarantineSecurityGroup にマッピングします。

このマッピングにより、感染しているシステムにトラフィックが流れないようにします。

10 Symantec アンチマルウェア コンソールから、ネットワークでスキャンを起動します。

感染している仮想マシンがスキャンで検出され、セキュリティ タグ **AntiVirus.virusFound** が付けられます。タグが付けられた仮想マシンは、即座に **QuarantineSecurityGroup** に追加されます。

QuarantinePolicy では、感染しているシステムとの間のトラフィックは許可されません。

セキュリティ設定のバックアップ

Service Composer を使用すると、セキュリティをバックアップし、後からリストアする操作を効率的に行うことができます。

手順

- 1 Rapid 7 Vulnerability Management ソリューションをインストール、登録、デプロイします。
- 2 SharePoint アプリケーション (Web サーバ) の最初の階層にセキュリティ グループを作成します。
 - a vSphere Web Client にログインします。
 - b [Networking and Security] をクリックし、[Service Composer] をクリックします。
 - c [セキュリティ グループ] タブをクリックし、[セキュリティ グループの追加] アイコンをクリックします。
 - d [名前] に **SG_Web** と入力します。
 - e [説明] に **Security group for application tier** と入力します。
 - f [メンバーシップ基準の定義] ページでは何も行わず、[次へ] をクリックします。
 - g [含めるオブジェクトの選択] ページで、Web サーバの仮想マシンを選択します。
 - h [除外するオブジェクトの選択] ページでは何も行わず、[次へ] をクリックします。
 - i [設定内容の確認] ページで選択内容を確認し、[終了] をクリックします。
- 3 データベースおよび SharePoint Server にセキュリティ グループを作成し、それぞれ **SG_Database** および **SG_Server_SharePoint** という名前を付けます。各グループに適切なオブジェクトを含めます。
- 4 アプリケーション階層に最上位のセキュリティ グループを作成し、**SG_App_Group** という名前を付けます。このグループに SG_Web、SG_Database、SG_Server_SharePoint を追加します。
- 5 Web サーバにセキュリティ ポリシーを作成します。
 - a [セキュリティ ポリシー] タブをクリックし、[セキュリティ ポリシーの追加] アイコンをクリックします。
 - b [名前] に **SP_App** と入力します。
 - c [説明] に **アプリケーション Web サーバの SP** と入力します。
 - d 重みを 50000 に変更します。(検疫を除き) 他のほとんどのポリシーより常に優先されるようにするため、このポリシーの優先順位は非常に高く設定されています。
 - e [次へ] をクリックします。

- f [Endpoint サービス] ページで、 をクリックし、次の値を入力します。

オプション	値
[アクション]	デフォルト値は変更しないでください
[サービス種別]	Vulnerability Management
[サービス名]	Rapid 7
[サービス設定]	シルバー
[状態]	デフォルト値は変更しないでください
[強制]	デフォルト値は変更しないでください

- g ファイアウォールまたはネットワーク イントロスペクション サービスを追加せずに、[終了] をクリックします。
- 6 SP_App を SG_App_Group にマッピングします。
- 7 キャンバス ビューに移動し、SP_App が SG_App_Group にマッピングされたことを確認します。
- a [情報セキュリティ] タブをクリックします。
- b  アイコンの横にある数値をクリックして、SP_App がマッピングされていることを確認します。
- 8 SP_App ポリシーをエクスポートします。
- a [セキュリティ ポリシー] タブをクリックし、[Blueprint のエクスポート] () アイコンをクリックします。
- b [名前] に **Template_ App_** と入力し、[プリフィックス] に **FromAppArchitect** と入力します。
- c [次へ] をクリックします。
- d SP_App ポリシーを選択し、[次へ] をクリックします。
- e 選択内容を確認し、[終了] をクリックします。
- f エクスポートしたファイルのダウンロード先となるコンピュータのディレクトリを選択し、[保存] をクリックします。

セキュリティ ポリシーと、このポリシーが適用されたセキュリティ グループがエクスポートされます（この場合は、アプリケーションのセキュリティ グループと、そこにネストされた 3 つのセキュリティ グループ）。

- 9 エクスポートされたポリシーがどのように動作するかを示すには、SP_App ポリシーを削除します。
- 10 次に、手順 7 でエクスポートした Template_ App_ DevTest ポリシーをリストアします。
- a [アクション] をクリックし、[サービス設定のインポート] アイコンをクリックします。
- b デスクトップから **FromAppArtchitect_Template_App** ファイル（手順 7 で保存済み）を選択します。
- c [次へ] をクリックします。

- d [設定内容の確認] ページには、セキュリティ ポリシーとインポートする関連オブジェクト（セキュリティ ポリシーが適用されたセキュリティ グループ、Endpoint サービス、ファイアウォール ルール、ネットワーク イントロスペクション サービス）が表示されます。
- e [終了] をクリックします。

構成オブジェクトおよび関連オブジェクトが vCenter インベントリにインポートされ、キャンバス ビューに表示されます。

ゲスト イントロスペクション

ゲスト イントロスペクションは、VMware パートナーが提供する専用のセキュアな仮想アプライアンスに、アンチウイルスおよびアンチマルウェア エージェントの処理をオフロードします。ゲスト仮想マシンとは異なり、セキュアな仮想アプライアンスはオフラインにならないため、アンチウイルス シグネチャを継続的に更新することができ、ホスト上の仮想マシンに中断なく保護を提供できます。また、新しい仮想マシンやオフライン状態の既存の仮想マシンは、オンラインになった時点で、最も新しいアンチウイルス シグネチャにより即座に保護されます。

ゲスト イントロスペクション の健全性ステータスは、vCenter Server コンソールに赤で表示されるアラームを使用して示されます。さらに、イベント ログを見ることで詳しいステータス情報が得られます。

重要: ゲスト イントロスペクションのセキュリティ用に、vCenter Server を正しく設定する必要があります。

- すべてのゲスト オペレーティング システムがゲスト イントロスペクション によりサポートされているわけではありません。サポート外のオペレーティング システムを実行する仮想マシンは、セキュリティ ソリューションによって保護されません。
- リソース プール内のホストに保護対象の仮想マシンが含まれる場合は、そのすべてにゲスト イントロスペクション の準備を行っておく必要があります。これは、リソース プール内の仮想マシンが別の ESX ホストへ vMotion で移行した場合でも、継続して保護することができるためです。

この章には、次のトピックが含まれています。

- [ゲスト イントロスペクション のインストール](#)
- [ゲスト イントロスペクション のステータスの表示](#)
- [ゲスト イントロスペクションのアラーム](#)
- [ゲスト イントロスペクションのイベント](#)
- [ゲスト イントロスペクション の監査メッセージ](#)
- [ゲスト イントロスペクションのトラブルシューティング データの収集](#)
- [ゲスト イントロスペクション モジュールのアンインストール](#)

ゲスト イントロスペクション のインストール

ゲスト イントロスペクション をインストールすると、クラスタ内の各ホストに新しい VIB とサービス仮想マシンが自動的にインストールされます。ゲスト イントロスペクション は、NSX Data Security、アクティビティ モニタリング、およびいくつかのサードパーティ セキュリティ ソリューションで必要になります。

ステートレス ホストでの自動デプロイ セットアップの場合、ESXi ホストの再起動後に、VMware NSX for vSphere 6.x サービス仮想マシン (SVM) を手動で再起動する必要があります。詳細については、ナレッジベースの記事 <http://kb.vmware.com/kb/2120649> を参照してください。



警告: VMware NSX for vSphere 6.x の環境では、サービス仮想マシン (SVM) の移行時 (vMotion/SvMotion) に、次の問題が発生することがあります。

- サービス仮想マシン (SVM) のデータ提供先となるサービス (ワークロード仮想マシン) が中断する
- ESXi ホストに障害が発生し、診断画面に次のようなバクトレースを含むパープル スクリーンが表示される

```
@BlueScreen: #PF Exception 14 in world www:WorldName IP 0xffffffff addr 0x0
PTes:0xffffffff;0xffffffff;0x0;
0xffffffff:[0xffffffff]VmMemPin_DecCount@vmkernel#nover+0x1b
0xffffffff:[0xffffffff]VmMemPinUnpinPages@vmkernel#nover+0x65
0xffffffff:[0xffffffff]VmMemPin_ReleaseMainMemRange@vmkernel#nover+0x6
0xffffffff:[0xffffffff]P2MCache_ReleasePages@vmkernel#nover+0x2a
0xffffffff:[0xffffffff]DVFilterVmciUnmapGuestPage@com.vmware.vmkapi#v2_2_0_0+0x34
```

これは、VMware ESXi 5.5.x および 6.x のホストに影響する既知の問題です。この問題を回避するには、サービス仮想マシン (SVM) をクラスタ内の別の ESXi ホストに手動で移行 (vMotion/SvMotion) しないでください。SVM を別のデータストアに移行 (svMotion) する場合は、SVM をオフにしてから別のデータストアに移行するコールドマイグレーションを使用することをお勧めします。

前提条件

このインストール手順の前提条件として、下記のシステムが必要です。


- データセンター内のクラスタの各ホストに、サポート対象のバージョンの vCenter Server および ESXi がインストールされている
- クラスタ内のホストが vCenter Server バージョン 5.0 から 5.5 にアップグレードされた場合は、それらのホストでポート 80 とポート 443 が開かれている
- ゲスト イントロスペクションをインストールするクラスタのホストで、NSX の準備が完了している『NSX インストール ガイド』で、「NSX 用ホスト クラスタの準備」セクションを参照してください。ゲスト イントロスペクション はスタンドアローン ホストにはインストールできません。アンチウイルスのオフロード機能を使用する目的で、ゲスト イントロスペクションを展開および管理するために NSX を使用する場合、ホストで NSX の準備を行う必要はありません。また、NSX for vShield Endpoint ライセンスでは、このような使い方は許可されません。
- NSX Manager 6.2 がインストールおよび実行されていること。
- NSX Manager と、ゲスト イントロスペクション サービスを実行する準備済みホストが同じ NTP サーバにリンクされ、時刻が同期されていることを確認します。これを行わない場合、ゲスト イントロスペクションとサードパーティ サービスに対して、クラスタのステータスが問題がないことを示す緑で表示されているにもかかわらず、仮想マシンがアンチウイルス サービスによって保護されていないことがあります。

NTP サーバを追加した場合、ゲスト イントロスペクションとすべてのサードパーティ サービスを再デプロイすることをお勧めします。

NSX ゲスト イントロスペクション サービス仮想マシンに IP アドレス プールから IP アドレスを割り当てる場合は、NSX ゲスト イントロスペクション をインストールする前に IP アドレス プールを作成します。『NSX 管理ガイド』の「IP アドレス プールの操作」セクションを参照してください。

vSphere Fault Tolerance は、ゲスト イントロスペクション とは連携しません。

手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 [新しいサービスのデプロイ (New Service Deployment)] () アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログ ボックスで、[ゲスト イントロスペクション (Guest Introspection)] を選択します。
- 4 [スケジュールを指定する (Specify schedule)] (ダイアログ ボックス下部) で、[今すぐデプロイする (Deploy now)] を選択して ゲスト イントロスペクション がインストールされたらすぐにデプロイするか、またはデプロイの日付と時間を選択します。
- 5 [次へ (Next)] をクリックします。
- 6 ゲスト イントロスペクションをインストールするデータセンターおよびクラスタを選択し、[次へ (Next)] をクリックします。
- 7 [ストレージおよび管理ネットワークの選択] ページで、サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み (Specified on host)] を選択します。デプロイ ワークフローを自動化するためには、[ホスト上が選択済み] ではなく、共有のデータストアとネットワークを使用することをお勧めします。

選択したデータストアは、選択したクラスタ内のすべてのホストで利用可能である必要があります。

[ホスト上が指定済み (Specified on host)] を選択した場合は、クラスタ内の各ホストに対して次のステップを実行します。

- a vSphere Web Client のホーム ページで、[vCenter] をクリックし、[ホスト (Hosts)] をクリックします。
 - b [名前 (Name)] 列のホストをクリックし、[管理 (Manage)] タブをクリックします。
 - c [エージェント仮想マシンの設定 (Agent VM Settings)] をクリックし、[編集 (Edit)] をクリックします。
 - d データストアを選択し、[OK] をクリックします。
- 8 管理インターフェイスをホストする分散仮想ポート グループを選択します。データストアが [ホスト上が指定済み (Specified on host)] に設定されている場合は、ネットワークも [ホスト上が指定済み (Specified on host)] に設定する必要があります。

選択したポート グループは、NSX Manager のポート グループにアクセスできる必要があり、選択したクラスタ内のすべてのホストで利用できる必要があります。

[ホスト上が指定済み (Specified on host)] を選択した場合は、ステップ 7 のサブステップを実行してホスト上のネットワークを選択します。クラスタに 1 台以上のホストを追加する場合は、データストアおよびネットワークを設定してからクラスタに追加する必要があります。

9 [IP 割り当て] で、次のいずれかを選択します。

選択	宛先
DHCP	DHCP (Dynamic Host Configuration Protocol) を使用して NSX ゲスト イントロスペクション サービス仮想マシンに IP アドレスを割り当てます。ホストが異なるサブネット上にある場合に、このオプションを選択します。
IP アドレス プール	選択された IP アドレス プール内の IP アドレスを NSX ゲスト イントロスペクション サービス仮想マシンに割り当てます。

10 [次へ (Next)] をクリックし、[設定内容の確認] ページで [終了 (Finish)] をクリックします。

11 [インストールの状態 (Installation Status)] 列に [成功 (Succeeded)] と表示されるまで、状況を監視します。

12 [インストールの状態 (Installation Status)] 列に [失敗 (Failed)] と表示された場合は、[失敗] の横にあるアイコンをクリックします。すべてのデプロイ エラーが表示されます。[解決 (Resolve)] をクリックしてエラーを修正します。エラーを解決すると、別のエラーが表示されることがあります。必要な操作を行い、再度 [解決 (Resolve)] をクリックします。

次のステップ

ゲスト仮想マシンに VMware Tools をインストールします。

ゲスト仮想マシンへの VMware Tools のインストール

VMware Tools には、保護対象となるそれぞれのゲスト仮想マシンにインストールする必要がある NSX シン エージェントが含まれます。VMware Tools がインストールされた仮想マシンは、セキュリティ ソリューションがインストールされた ESX ホスト上で起動されるたびに自動的に保護されます。つまり、保護された仮想マシンは、終了と起動の間常に、また 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 ESX に移動した後でも、セキュリティ保護が保たれます。

前提条件

ゲスト仮想マシンに、ESX 5.1 以降と、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 Vista (32 ビット)
- Windows 7 (32 ビットまたは 64 ビット)
- Windows XP SP3 以降 (32 ビット)
- 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 8 (32 ビットまたは 64 ビット) -- vSphere 5.5 以降から
- Win2012 (64 ビット) -- vSphere 5.5 以降から

- Windows 8.1 (32 ビットまたは 64 ビット) -- vSphere 5.5 パッチ 2 以降から
- Win2012 R2 (64 ビット) -- vSphere 5.5 パッチ 2 以降から

手順

- 1 [Windows 仮想マシンでの VMware Tools の手動インストールまたはアップグレード](#)の手順に従ってください。
- 2 手順 7 で [カスタム (Custom)] セットアップを選択したら、[VMCI ドライバ (VMCI Driver)] セクションを展開し、[vShield ドライバ (vShield Drivers)] を選択して、[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 (This feature will be installed on the local hard drive)] を選択します。
- 3 残りの手順に従います。

ゲスト イントロスペクション のステータスの表示

ゲストイントロスペクションインスタンスの監視では、ゲストイントロスペクション コンポーネント (SVM (Security Virtual Machine)、ESX ホストに常駐する ゲスト イントロスペクション モジュール、保護された仮想マシンに常駐するシン エージェント) からのステータスのチェックが行われます。

手順

- 1 vSphere Web Client で、[vCenter] をクリックし、[データセンター (Datacenters)] をクリックします。
- 2 [名前 (Name)] 列で、データセンターをクリックします。
- 3 [監視 (Monitor)] をクリックし、[Endpoint] をクリックします。

ゲスト イントロスペクション の健全性およびアラームのページには、選択したデータセンターの下オブジェクトの健全性とアクティブなアラームが表示されます。健全性ステータスの変化は、その変化の原因となったイベントが実際に発生してから 1 分以内に反映されます。

ゲスト イントロスペクションのアラーム

注意が必要なゲスト イントロスペクション イベントは、vCenter Server 管理者にアラームで通知されます。アラームはその状態が解除されると自動的にキャンセルされます。

vCenter Server アラームはカスタム vSphere プラグインなしでも表示できます。イベントとアラームについては『vCenter Server 管理ガイド』を参照してください。

NSX Manager が vCenter Server の拡張として登録されると、NSX Manager は、SVM、ゲスト イントロスペクション モジュール、シン エージェントという 3 つのゲスト イントロスペクション コンポーネントからのイベントを基にしてアラームを作成および削除するルールを定義します。ルールはカスタマイズできます。アラームの新しいカスタム ルールを作成する方法については、vCenter Server のドキュメントを参照してください。いくつかのケースでは、アラームの発生には複数の原因があることがあります。下記の表では、可能性のある原因とそれに対応した改善のためのアクションがリストされています。

ホスト アラーム

ホスト アラームは ゲスト イントロスペクション モジュールの健全性ステータスに影響を及ぼすイベントにより生成されます。

表 18-1. エラー（赤で表示）

可能性のある原因	アクション
ゲスト イントロスペクション モジュールはホストにインストールされていますが、ステータスを NSX Manager に報告しなくなりました。	<ol style="list-style-type: none"> 1 ホストにログインし、<code>/etc/init.d/vShield-Endpoint-Mux start</code> コマンドを入力して、ゲスト イントロスペクション が動作していることを確認します。 2 ネットワークが適切に設定され、ゲスト イントロスペクション が NSX Manager に接続可能であることを確認します。 3 NSX Manager を再起動します。

SVM アラーム

SVM アラームは SVM の健全性ステータスに影響を及ぼすイベントによって生成されます。

表 18-2. SVM 赤アラーム

問題	アクション
ゲスト イントロスペクション モジュールと一致しないプロトコル バージョンがある。	ゲスト イントロスペクション モジュールと SVM に、互いに互換性のあるプロトコルが設定されていることを確認します。
ゲスト イントロスペクション が SVM への接続を確立できない。	SVM がパワーオン状態で、ネットワークが適切に設定されていることを確認します。
ゲストが接続されていても SVM がステータスを報告しない。	内部エラー。VMware のサポート担当者にお問い合わせください。

ゲスト イントロスペクションのイベント

イベントは、ゲスト イントロスペクション ベースのセキュリティ システム内で発生する状況のログや監査に使われます。

イベントはカスタム vSphere プラグインなしでも表示できます。イベントとアラームについては、『vCenter Server 管理ガイド』を参照してください。

イベントはアラーム生成の基となるものです。NSX Manager が vCenter Server の拡張として登録されると、NSX Manager はアラームを生成、解除するルールを定義します。

すべてのイベントに共通する引数は、イベントのタイム スタンプと NSX Manager `event_id` です。

次の表は、SVM および NSX Manager によって報告される ゲスト イントロスペクション のイベントのリストです。

表 18-3. ゲスト イントロスペクションのイベント

説明	重要度	VC 引数
ゲスト イントロスペクション ソリューション <SolutionName> が有効です。バージョン <versionNumber> の VFile プロトコルをサポートします。	情報	タイムスタンプ
ESX モジュールが有効になりました。	情報	タイムスタンプ
ESX モジュールがアンインストールされました。	情報	タイムスタンプ
NSX Manager と ESX モジュールとの接続が失われました。	情報	タイムスタンプ
ゲスト イントロスペクション ソリューション <SolutionName> が、互換性のないバージョンの ESX モジュールによって接続されました。	エラー	タイムスタンプ、ソリューションのバージョン、ESX モジュールのバージョン

表 18-3. ゲスト イントロスペクションのイベント (続き)

説明	重要度	VC 引数
ESX モジュールと <SolutionName> との接続が失敗しました。	エラー	タイムスタンプ、ESX モジュールのバージョン、ソリューションのバージョン
ゲスト イントロスペクション と SVM との接続が失敗しました。	エラー	タイムスタンプ
ゲスト イントロスペクション と SVM との接続が失われました。	エラー	タイムスタンプ

ゲスト イントロスペクション の監査メッセージ

致命的なエラーやその他の重要な監査メッセージは `vmware.log` にログされます。

以下の状態が AUDIT メッセージとしてログされます。

- シン エージェント初期化成功 (とバージョン情報)。
- シン エージェント初期化失敗。
- SVM との最初の接続確立。
- SVM との接続に失敗 (初めての失敗の時)。

生成されたログ メッセージには各ログ メッセージの先頭近くに以下の従属文字列が付いています。vf-AUDIT、vf-ERROR、vf-WARN、vf-INFO、vf-DEBUG

ゲスト イントロスペクションのトラブルシューティング データの収集

VMware のテクニカル サポートは、通常、サポート リクエストを受理する際に、診断情報やサポート バンドルの提供をお願いしています。この診断情報には、仮想マシンのログや構成ファイルが含まれます。

Identity Firewall のトラブルシューティング データ

ID ベースのファイアウォール環境でゲスト イントロスペクションを使用している場合は、ナレッジベースの記事「Troubleshooting vShield Endpoint / NSX Guest Introspection (<https://kb.vmware.com/kb/2094261>)」および「How to collect USVM logs in NSX for vSphere 6.x Guest Introspection (<https://kb.vmware.com/kb/2144624>)」で診断情報について確認できます。

ゲスト イントロスペクション モジュールのアンインストール

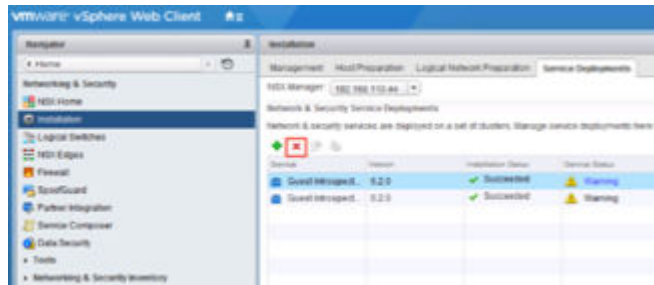
ゲスト イントロスペクション をアンインストールすると、VIB がクラスタ内のホストから削除され、サービス仮想マシンがクラスタ内の各ホストから削除されます。NSX Data Security、アクティビティ モニタリング、およびいくつかのサードパーティ製のセキュリティ ソリューションには、ゲスト イントロスペクション が必要です。ゲスト イントロスペクション をアンインストールすると、影響が広範囲に及ぶ可能性があります。



警告: クラスタから ゲスト イントロスペクション モジュールをアンインストールする前に、そのクラスタのホストから、ゲスト イントロスペクション を使用しているすべてのサードパーティ製品をアンインストールする必要があります。ソリューション プロバイダから提供される説明書を使用してください。

ゲスト イントロスペクション をアンインストールするには、次の操作を実行します。

- 1 vSphere Web Client で、[ホーム] > [Networking and Security] > [インストール手順] の順に移動し、[サービス デプロイ] タブを選択します。
- 2 ゲスト イントロスペクション インスタンスを選択し、[削除] アイコンをクリックします。
- 3 すぐに削除するか、後で削除するようにスケジュールを設定できます。



Data Security

NSX Data Security は、組織の仮想化されたクラウド環境内に格納されている機密データを表示できるようにします。NSX Data Security が提供するアクセス違反のレポートに基づいて、機密データを適切に保護し、世界の規制に準拠しているか評価できます。

注: NSX Data Security は、NSX 6.2.3 のリリースでは推奨されない機能です。NSX 6.2.3 では、ユーザーの判断でこの機能を引き続き使用できます。ただし、この機能は NSX の今後のリリースでは削除されることにご注意ください。

NSX Data Security の使用を開始するには、ポリシーを作成して、組織内のデータ セキュリティに適用される規制を定義し、スキャン対象になる環境の領域およびファイルを指定します。規制は、検出対象の機密コンテンツを特定するコンテンツ ブレードで設定します。NSX は、PCI、PHI、および PII に関連する規制のみをサポートします。

Data Security スキャンを開始すると、NSX が vSphere インベントリ内の仮想マシン上のデータを分析し、検出された違反の数とポリシーに違反するファイルをレポートします。

この章には、次のトピックが含まれています。

- [NSX Data Security のインストール](#)
- [NSX Data Security のユーザー ロール](#)
- [データ セキュリティ ポリシーの定義](#)
- [データ セキュリティ スキャンの実行](#)
- [レポートの表示とダウンロード](#)
- [正規表現の作成](#)
- [NSX Data Security のアンインストール](#)

NSX Data Security のインストール

注: NSX Data Security は、NSX 6.2.3 のリリースでは推奨されない機能です。NSX 6.2.3 では、ユーザーの判断でこの機能を引き続き使用できます。ただし、この機能は NSX の今後のリリースでは削除されることにご注意ください。

前提条件

Data Security をインストールするクラスタには、NSX ゲスト イントロスペクション がインストールされている必要があります。

Data Security サービス仮想マシンに IP プールから IP アドレスを割り当てる場合は、Data Security をインストールする前に IP プールを作成します。『NSX 管理ガイド』のグループ オブジェクトに関するページを参照してください。

手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 [新しいサービスの展開 (New Service Deployment)] () アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログ ボックスで、[Data Security] を選択し、[次へ (Next)] をクリックします。
- 4 [スケジュールを指定する (Specify schedule)] (ダイアログ ボックス下部) で、[今すぐデプロイする (Deploy now)] を選択して Data Security がインストールされたらすぐにデプロイするか、またはデプロイの日付と時間を選択します。
- 5 [次へ (Next)] をクリックします。
- 6 Data Security をインストールするデータセンターおよびクラスタを選択し、[次へ (Next)] をクリックします。
- 7 [ストレージおよび管理ネットワークの選択] ページで、サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み (Specified on host)] を選択します。

選択したデータストアは、選択したクラスタ内のすべてのホストで利用可能である必要があります。

[ホスト上が指定済み (Specified on host)] を選択した場合、そのホストの [エージェント仮想マシンの設定 (AgentVM Settings)] で ESX ホストのデータストアを指定してから、ホストをクラスタに追加する必要があります。vSphere API/SDK のドキュメントを参照してください。

- 8 管理インターフェイスをホストする分散仮想ポート グループを選択します。このポート グループには NSX Manager のポート グループへのアクセスが必要です。

データストアが [ホスト上が指定済み (Specified on host)] に設定されている場合、使用するネットワークは、クラスタの各ホストの [agentVmNetwork] プロパティで指定されている必要があります。vSphere API/SDK のドキュメントを参照してください。

クラスタにホストを追加するときは、ホストの [agentVmNetwork] プロパティを設定してからクラスタにホストを追加する必要があります。

選択したポート グループは、選択したクラスタのすべてのホストで利用できる必要があります。

- 9 [IP 割り当て] で、次のいずれかを選択します。

選択	宛先
DHCP	DHCP (Dynamic Host Configuration Protocol) を使用して Data Security サービス仮想マシンに IP アドレスを割り当てます。
IP アドレス プール	選択された IP プールから、Data Security サービス仮想マシンに IP アドレスを割り当てます。

固定 IP アドレスはサポートされていないことに注意してください。

- 10 [次へ (Next)] をクリックし、[設定内容の確認] ページで [終了 (Finish)] をクリックします。
- 11 [インストール ステータス (Installation Status)] 列に [成功 (Succeeded)] と表示されるまで、デプロイを監視します。
- 12 [インストール ステータス (Installation Status)] 列に [失敗 (Failed)] と表示された場合は、[失敗] の横にあるアイコンをクリックします。すべてのデプロイ エラーが表示されます。[解決法 (Resolve)] をクリックしてエラーを修正します。エラーを解決すると、別のエラーが表示されることがあります。必要な操作を行い、再度 [解決法 (Resolve)] をクリックします。

NSX Data Security のユーザー ロール

ユーザーのロールによって、そのユーザーが実行できる操作が決まります。

ロール	許可される操作
Security Administrator	ポリシーの作成および発行と、違反に関するレポートの表示。データ セキュリティ スキャンを開始または停止することはできません。
NSX Administrator	データ セキュリティ スキャンの開始および停止。
Auditor	設定済みポリシーと違反に関するレポートの表示。

データ セキュリティ ポリシーの定義

環境内の機密データを検出するには、データ セキュリティ ポリシーを作成する必要があります。ポリシーを作成するには、セキュリティ管理者でなければなりません。

ポリシーを定義するには、次の内容を指定する必要があります。

規制 規制とは、PCI (Payment Card Industry)、PHI (Protected Health Information)、および PII (Personally Identifiable Information) の情報を保護するためのデータ プライバシー法です。会社で順守する必要がある規制を選択できます。スキャンを実行すると、Data Security によって、ポリシーに指定された規制に違反する、慎重に扱う必要があるデータが特定されます。

ファイル フィルタ フィルタを作成して、スキャン対象となるデータを制限したり、機密データが含まれている可能性が低いファイルの種類をスキャンから除外したりすることができます。

規制の選択

企業データが準拠する必要がある規制を選択すると、それらの規制に違反する情報が含まれているファイルを NSX で確認できます。

前提条件

Security Administrator のロールを持っている必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、[Data Security] をクリックします。

- 3 [管理 (Manage)] タブをクリックします。
- 4 [編集 (Edit)] をクリックし、[すべて (All)] をクリックして、使用可能なすべての規制を表示します。
- 5 コンプライアンス状態の検出の対象となる規制を選択します。

注: 利用可能な規制については、『Data Security リファレンス ガイド』を参照してください。

規制によっては、NSX Data Security で機密データを認識できるようにするために、追加情報が必要です。団体保険番号、患者識別番号、医療記録番号、健康保険受給者番号、銀行口座番号、カスタム アカウント、または学生証番号を監視する規制を選択した場合は、そのデータを識別するための正規表現パターンを指定します。

- 6 正規表現が正確であることを確認してください。
正確でない正規表現を指定すると、検出プロセスの速度が低下する可能性があります。正規表現の詳細については、「[正規表現の作成](#)」を参照してください。
- 7 [次へ (Next)] をクリックします。
- 8 [終了 (Finish)] をクリックします。
- 9 [変更の発行 (Publish Changes)] をクリックしてポリシーを適用します。

ファイル フィルタの指定

サイズ、最終変更日、またはファイル拡張子に基づいて、監視対象にするファイルを制限することができます。

前提条件

Security Administrator のロールが自分に割り当てられている必要があります。

手順

- 1 Data Security パネルの [管理 (Manage)] タブで、[スキャンするファイル (Edit)] の横の [編集 (Files to scan)] をクリックします。
- 2 インベントリ内の仮想マシン上のすべてのファイルを監視するか、適用する制限を選択することができます。

オプション	説明
ゲスト仮想マシン上のすべてのファイルを監視	NSX Data Security ですべてのファイルがスキャンされます。
次の条件を満たすファイルのみを監視	<p>必要に応じて次のオプションを選択します。</p> <ul style="list-style-type: none"> ■ [サイズ (Size)] を選択すると、指定したサイズに満たないファイルだけが NSX Data Security でスキャンされます。 ■ [最終変更日 (Last Modified Date)] を選択すると、指定された日付までに変更されたファイルだけが NSX Data Security でスキャンされます。 ■ [タイプ (Types)] : スキャンするファイルのタイプを入力するには、[次の拡張子を持つファイルのみ (Only files with the following extensions)] を選択します。スキャンから除外するファイルのタイプを入力するには、[拡張子をもつこれらのファイルを除くすべてのファイル (All files, except those with extensions)] を選択します。

NSX Data Security が検出可能なファイル形式については、『Data Security リファレンス ガイド』を参照してください。

- 3 [保存 (Save)] をクリックします。

- 4 [変更の発行 (Publish Changes)] をクリックしてポリシーを適用します。

データ セキュリティ スキャンの実行

データ セキュリティ スキャンを実行すると、仮想環境内の、ポリシーに違反するデータが識別されます。

前提条件

データ セキュリティ スキャンを開始、一時停止、または停止するには、NSX Administrator である必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、[Data Security] をクリックします。
- 3 [管理 (Manage)] タブをクリックします。
- 4 スキャンの横にある [開始 (Start)] をクリックします。

注: 仮想マシンがパワーオフの場合、パワーオン状態になるまでスキャンは実行されません。

スキャンが進行中の場合、使用可能なオプションは [一時停止 (Pause)] と [停止 (Stop)] です。

Data Security が Service Composer ポリシーに含まれている場合は、その Service Composer ポリシーにマッピングされている Security Group 内の仮想マシンが、スキャン中に一度スキャンされます。スキャンの実行中にポリシーを編集して発行すると、スキャンが再度開始されます。この再スキャンによって、すべての仮想マシンが編集後のポリシーに確実に準拠するようになります。再スキャンは、仮想マシン上でのデータ更新ではなく、編集済みポリシーの発行によって起動されます。

データ セキュリティ スキャンの進行中に、スキャンから除外されたクラスタまたはリソース プールに仮想マシンが移動された場合、その仮想マシン上のファイルはスキャンされません。仮想マシンが vMotion によって別のホストに移動された場合、スキャンは 2 番目のホスト上で続行されます。仮想マシンが前のホスト上にあったときにスキャン済みだったファイルは、再スキャンされません。

Data Security エンジンが仮想マシンのスキャンを開始するときには、スキャンの開始時刻が記録されます。スキャンが終了すると、スキャンの終了が記録されます。[タスクとイベント (Tasks and Events)] タブで、クラスタ、ホスト、または仮想マシンのスキャン開始時刻とスキャン終了時刻を表示できます。

NSX Data Security は、パフォーマンスに与える影響を最小限に抑えるために、1 台のホスト上で同時にスキャンされる仮想マシンの数をスロットルします。VMware では、パフォーマンスのオーバーヘッドを避けるため、通常の営業時間中はスキャンを一時停止することをお勧めしています。

レポートの表示とダウンロード

セキュリティ スキャンを開始すると、NSX には各スキャンの開始時間と終了時間、スキャン対象の仮想マシンの数、および検出された違反の件数が表示されます。

前提条件

Security Administrator または Auditor のロールがあること。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、[Data Security] をクリックします。
- 3 [レポート (Reports)] タブをクリックします。
- 4 違反数または違反ファイルのレポートを指定します。

正規表現の作成

正規表現とは、文字列とも呼ばれるテキストの文字の特定の並びを記述するパターンです。正規表現は、テキスト本文内の特定の文字列または文字列のクラスを検索するため、またはマッチする項目を探すために使用します。

正規表現の使用方法はワイルドカード検索に似ていますが、それよりもはるかに強力です。非常にシンプルなものと、非常に複雑なものがあります。シンプルな正規表現の例としては、`<cat>` があります。

これは、適用するテキスト内でこの文字列が最初に表れる箇所を検索します。`<cat>` という語だけを見つけて、`<cats>` や `<hepcat>` を検索しないようにするには、もう少し複雑になった `<\bcat\b>` を使用します。

この表現には、`<cat>` という文字列の前後に単語区切りがある場合にのみマッチするように、特殊文字が含まれています。別の例としては、一般的なワイルドカード文字列 `<c+t>` による検索とほぼ同じ検索を行う `<\bc\w+t\b>` があります。

これは、単語区切り文字 (`\b`) に文字 `<c>`、1 文字以上のホワイトスペースや区切り文字以外の文字 (`\w+`)、文字 `<t>`、単語区切り文字 (`\b`) が続くということを意味しています。この表現は `<cot>`、`<cat>`、`<croat>` にマッチしますが、`<crate>` にはマッチしません。

表現は非常に複雑なものにすることもできます。次の表現は任意の有効な電子メール アドレスにマッチします。

```
\b[A-Za-z0-9._%~]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b
```

正規表現を作成する方法の詳細については、<http://userguide.icu-project.org/strings/regexp> を参照してください。

NSX Data Security のアンインストール

NSX Data Security を使用しなくなった、または NSX Manager をアップグレードする場合に、NSX Data Security をアンインストールします。NSX Data Security では直接アップグレードはサポートされていません。NSX Manager をアップグレードする前に、まず NSX Data Security をアンインストールすることが重要です。アップグレードが完了した後、NSX Data Security を再インストールします。

NSX Data Security は、NSX 6.2.3 のリリースでは推奨されない機能です。NSX 6.2.3 では、ユーザーの判断でこの機能を引き続き使用できます。ただし、この機能は NSX の今後のリリースでは削除されることにご注意ください。

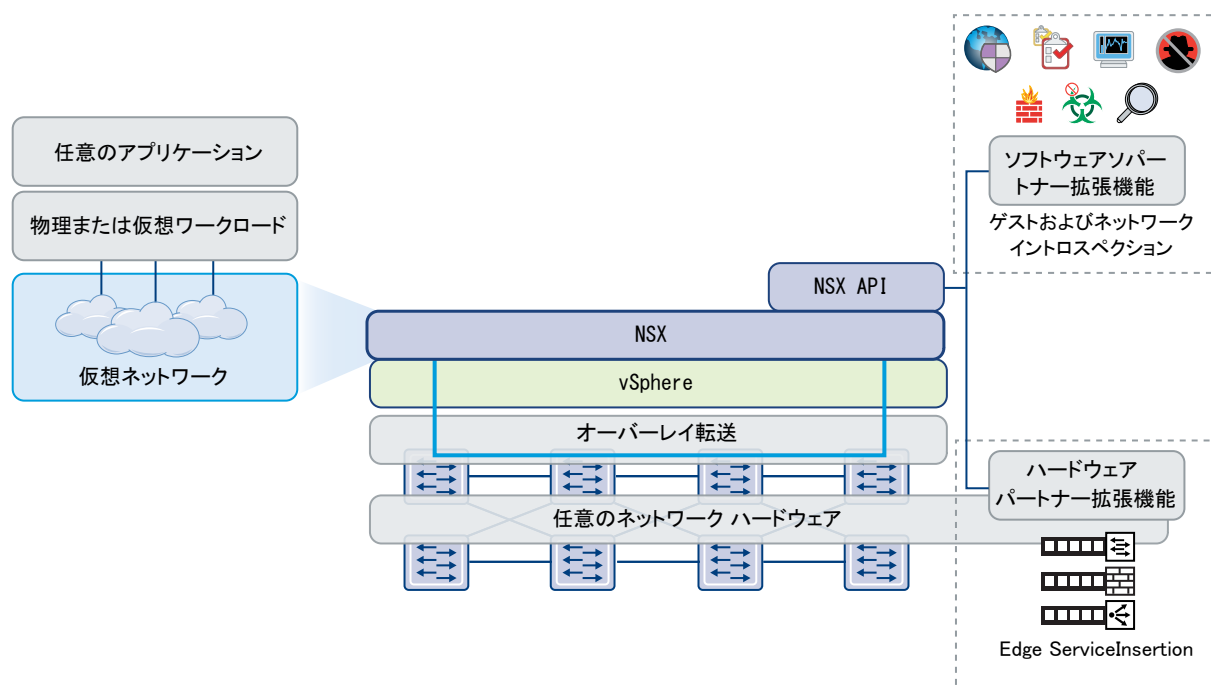
手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 NSX Data Security サービスを選択し、[サービス デプロイを削除します (Delete Service Deployment)] (✖) アイコンをクリックします。

- 3 [削除の確認] ダイアログ ボックスで、[今すぐ削除する (Delete now)] をクリックするか、または削除を有効にする日時を選択します。
- 4 [OK] をクリックします。

ネットワークの拡張性

データセンター ネットワークには通常、切り替え、ルーティング、ファイアウォール、ロード バランシングなどのさまざまなネットワーク サービスが関与しています。ほとんどの場合、これらのサービスはそれぞれ別のベンダーによって提供されます。物理環境のネットワークでこれらのサービスを接続するためには、物理ネットワーク デバイスのラックおよびスタック処理、物理的な接続の確立、各サービスの個別管理などの複雑な作業が必要になります。NSX を使用すると、適切なサービスを適切なトラフィック パスで接続するための手順が簡略化され、本番環境、テスト、開発などの目的で、単一の ESX Server ホストまたは複数の ESX Server ホストで複雑なネットワークを構築するために役立ちます。



NSX にサード パーティのサービスを挿入するための、さまざまなデプロイ方法があります。

この章には、次のトピックが含まれています。

- [分散サービス挿入](#)
- [Edge ベースのサービス挿入](#)
- [サードパーティのサービスの統合](#)
- [パートナー サービスの展開](#)

- [Service Composer を介したベンダー サービスの使用](#)
- [論理ファイアウォールを使用したベンダー ソリューションへのトラフィックのリダイレクト](#)
- [パートナーのロード バランサの使用](#)
- [サードパーティ統合の削除](#)

分散サービス挿入

分散サービス挿入では、単一のホストが、すべてのサービス モジュール、カーネル モジュール、および仮想マシンを単一の物理マシンで実装します。システムのすべてのコンポーネントが、物理ホスト内のコンポーネントと連携します。これにより、モジュール間の通信が高速化し、デプロイ モデルがコンパクトになります。拡張性を高めるために、サービス モジュールを宛先とする、またはサービス モジュールから `vmkernel` に送られるコントロールやデータ プレーンのトラフィックを物理システム上に置いたままにして、同じをネットワーク内の各物理システムにレプリケートすることができます。保護対象の仮想マシンに vMotion を実行している間に、パートナー セキュリティ マシンが仮想マシンの状態を送信元から宛先のホストに移動します。

このような種類のサービス挿入を利用するベンダー ソリューションに、侵入防止サービス (IPS)/侵入検知サービス (IDS)、ファイアウォール、Anti Virus、ファイル ID 監視 (FIM)、および脆弱性管理があります。

Edge ベースのサービス挿入

NSX Edge は、Edge サービス クラスタ内で、他のネットワーク サービスと一緒に仮想マシンとしてデプロイされます。NSX Edge には、特定のトラフィックをサードパーティのネットワーク サービスにリダイレクトする機能があります。

このような種類のサービス挿入を利用するベンダー ソリューションに、ADC デバイスやロード バランサ デバイスがあります。

サードパーティのサービスの統合

これは、サードパーティのサービスを NSX プラットフォームに挿入するための、一般的な高レベルのワークフローです。

手順

- 1 ベンダーのコンソール上の NSX Manager を使用して、サードパーティのサービスを登録します。

サービスの登録には、NSX のログイン認証情報が必要です。詳細については、ベンダーのドキュメントを参照してください。

- 2 NSX にサービスをデプロイします。[「パートナー サービスの展開」](#)を参照してください。

デプロイされたサードパーティのサービスは、NSX の [サービス定義] ウィンドウに表示され、使用する準備が整います。NSX でのサービスの使用手順は、挿入されたサービスの種類によって異なります。

たとえば、ホストベースのファイアウォール サービスは、Service Composer でセキュリティ ポリシーを作成するか、トラフィックをそのサービスにリダイレクトするファイアウォール ルールを作成することで有効にできます。[「Service Composer を介したベンダー サービスの使用」](#)または[「論理ファイアウォールを使用したベンダー ソリューションへのトラフィックのリダイレクト」](#)を参照してください。Edge ベース サービスの使用の詳細については、[「パートナーのロード バランサの使用」](#)を参照してください。

パートナー サービスの展開


パートナー ソリューションにホスト常駐型の仮想アプライアンスが含まれる場合は、ソリューションを NSX Manager で登録した後にサービスを展開できます。

前提条件

次のように設定されていることを確認します。

- パートナー ソリューションは、NSX Manager を使用して登録されます。
- NSX Manager から、パートナー ソリューションの管理コンソールにアクセスできます。

手順

- 1 [Networking and Security] をクリックし、[インストール手順] をクリックします。
- 2 [サービス デプロイ] タブをクリックし、[新しいサービスのデプロイ] () アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログ ボックスで、適切なソリューションを選択します。
- 4 [スケジュールを指定する] (ダイアログ ボックス下部) で、[今すぐデプロイする] を選択してソリューションをすぐにデプロイするか、デプロイの日付と時間を選択します。
- 5 [次へ] をクリックします。
- 6 ソリューションをデプロイするデータセンターおよびクラスタを選択し、[次へ] をクリックします。
- 7 ソリューション サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み] を選択します。

選択したデータストアは、選択したクラスタ内のすべてのホストで利用可能である必要があります。

[ホスト上が指定済み] を選択した場合、そのホストの [エージェント仮想マシンの設定] で ESX ホストのデータストアを指定してから、ホストをクラスタに追加する必要があります。vSphere API/SDK のドキュメントを参照してください。

- 8 管理インターフェイスをホストする分散仮想ポート グループを選択します。このポート グループには NSX Manager のポート グループへのアクセスが必要です。

ネットワークが [ホスト上が指定済み] に設定されている場合、使用するネットワークは、クラスタの各ホストの [エージェント仮想マシンの設定] > [ネットワーク] プロパティで指定されている必要があります。vSphere API/SDK のドキュメントを参照してください。

エージェント仮想マシンをクラスタに追加する前に、ホストでエージェント仮想マシンのネットワーク プロパティを設定する必要があります。[管理] - [設定] - [エージェント仮想マシン設定] - [ネットワーク] の順に移動し、[編集] をクリックして、エージェント仮想マシンのネットワークを設定します。

選択したポート グループは、選択したクラスタのすべてのホストで利用できる必要があります。

- 9 [IP 割り当て] で、次のいずれかを選択します。

選択	宛先
DHCP	DHCP (Dynamic Host Configuration Protocol) を使用してサービス仮想マシンに IP アドレスを割り当てます。
IP アドレス プール	選択された IP アドレス プールの IP アドレスをサービス仮想マシンに割り当てます。

- 10 [次へ] をクリックし、[設定内容の確認] ページで [終了] をクリックします。

- 11 [インストールの状態] に [成功] と表示されるまで、デプロイを監視します。ステータスに [失敗] と表示された場合は、[失敗] の横にあるアイコンをクリックして、エラーを解決するための操作を実行します。

次のステップ

NSX ユーザー インターフェイスまたは NSX API を介してパートナー サービスを使用できるようになりました。

Service Composer を介したベンダー サービスの使用

サードパーティ ベンダー サービスには、トラフィックのリダイレクト、ロード バランサ、およびデータ損失防止や Anti Virus などのゲスト セキュリティ サービスなどがあります。Service Composer を使用すると、これらのサービスを一連の vCenter Server オブジェクトに適用できます。

セキュリティ グループは vCenter Server オブジェクトのセットであり、これにはクラスタ、仮想マシン、vNIC、および論理スイッチが含まれます。セキュリティ ポリシーは ゲスト イントロスペクション サービス、ファイアウォール ルール、およびネットワーク イントロスペクション サービスのセットです。

セキュリティ ポリシーをセキュリティ グループにマッピングするときに、該当するサードパーティ ベンダー サービス プロファイルにリダイレクション ルールが作成されます。そのセキュリティ グループに属する仮想マシンからのトラフィックが流れるときは、このトラフィックのリダイレクト先は、登録済み サードパーティ ベンダー サービスになり、このサービスによって、トラフィックの処理方法が決定されます。Service Composer の詳細については、[\[Service Composer の使用\]](#) を参照してください。




論理ファイアウォールを使用したベンダー ソリューションへのトラフィックのリダイレクト

登録済みのベンダー ソリューションにトラフィックをリダイレクトするファイアウォール ルールを追加できます。リダイレクトされたトラフィックは、ベンダー サービスによって処理されます。

前提条件

- サードパーティのサービスは、NSX Manager に登録する必要があり、サービスは NSX 内にデプロイされている必要があります。
- デフォルトのファイアウォール ルール アクションがブロックに設定されている場合、ルールを追加することで、トラフィックのリダイレクトを許可する必要があります。

手順

- 1 vSphere Web Client で、[ネットワークとセキュリティ (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動します。
- 2 [パートナー セキュリティ サービス (Partner security services)] タブをクリックします。
- 3 ルールを追加するセクションで、[ルールの追加 (Add rule)] () アイコンをクリックします。
セクションの一番上に新しい許可ルールが追加されます。
- 4 新しいルールの [名前 (Name)] セルをポイントし、 をクリックし、ルールの名前を入力します。
- 5 ルールの [送信元 (Source)]、[宛先 (Destination)]、[サービス (Service)] を指定します。詳細については、[「ファイアウォール ルールの追加」](#) を参照してください。
- 6 新しいルールの [アクション (Action)] セルをポイントし、 をクリックします。
 - a [操作 (Action)] で、[リダイレクト (Redirect.)] を選択します。
 - b [リダイレクト先 (Redirect To)] で、サービス プロファイルおよび論理スイッチ、またはサービス プロファイルをバインドするセキュリティ グループを選択します。

このサービス プロファイルは、接続先の仮想マシンに適用されるか、選択した論理スイッチまたはセキュリティ グループに格納されます。
 - c リダイレクトされたトラフィックをログに記録するかどうかを示し、コメントがある場合は入力します。
 - d [OK] をクリックします。

選択したサービス プロファイルは、[操作 (Action)] 列にリンクとして表示されます。サービス プロファイル リンクをクリックすると、サービス プロファイルのバインドが表示されます。
- 7 [変更の発行 (Publish Changes)] をクリックします。

パートナーのロード バランサの使用

サードパーティのロード バランサを使用し、特定の NSX Edge のトラフィックを分散できます

前提条件

サードパーティのロード バランサは、NSX Manager に登録する必要があり、NSX 内でデプロイする必要があります。

手順

- 1 vSphere Web Client で、[ネットワークとセキュリティ (Networking & Security)] - [NSX Edge (NSX Edges)] の順に移動します。
- 2 [NSX Edge] をダブルクリックします。
- 3 [管理 (Manage)] > [ロード バランサ (Load Balancer)] タブの順にクリックします。
- 4 [ロード バランサのグローバル設定] の横にある [編集 (Edit)] をクリックします。
- 5 [ロード バランサの有効化 (Enable Load Balancer)] および [サービス挿入の有効化 (Enable Service Insertion)] を選択します。

- 6 [サービス定義 (Service Definition)] で、該当するパートナー ロード バランサを選択します。
- 7 [サービス設定 (Service Configuration)] で、該当するサービス設定を選択します。
- 8 その他のフィールドを入力し、サービス監視、サーバ プール、アプリケーション プロファイル、アプリケーション ルール、仮想サーバを追加することによって、ロード バランサを設定します。仮想サーバを追加するときは、ベンダーが提供するテンプレートを選択します。詳細については、「[ロード バランシングの設定](#)」を参照してください。

指定した Edge のトラフィックの負荷は、サードパーティ ベンダーの管理コンソールによって分散されます。

サードパーティ統合の削除

この例では、NSX からサードパーティ統合ソリューションを削除する方法について説明します。

サードパーティ ソフトウェア ソリューションを削除する場合、ソフトウェアについての正しい順序があります。

手順

- 1 Sphere Web Client で、[Networking and Security (Networking & Security)] > [Service Composer] の順に移動し、サードパーティ ソリューションにトラフィックをリダイレクトするルール（またはセキュリティ ポリシー）を削除します。
- 2 [サービス定義 (Service Definitions)] に移動し、サードパーティ ソリューションの名前をダブルクリックします。
- 3 [関連オブジェクト (Related Objects)] をクリックし、関連オブジェクトを削除します。
- 4 [インストール手順 (Installation)] > [サービス デプロイ (Service Deployments)] の順に移動し、サードパーティ デプロイを削除します。

この操作により、関連付けられた仮想マシンがアンインストールされます。

- 5 [サービス定義 (Service Definitions)] に戻り、定義のサブコンポーネントを削除します。
- 6 サービス インスタンスで、サービス プロファイルを削除します。
- 7 サービス インスタンスを削除します。
- 8 サービス定義を削除します。

サードパーティ統合ソリューションが NSX から削除されます。

次のステップ

構成設定をメモしてから、NSX をサードパーティ ソリューションから削除します。たとえば、他のオブジェクトを参照するルールを削除してからオブジェクトを削除する必要がある場合もあります。

ユーザー管理

多くの組織では、ネットワークとセキュリティの作業は複数のチームまたはメンバーが対処します。このような組織では、ある作業を特定のユーザーに限定する必要が生じることがあります。このトピックでは、このようなアクセスコントロールを設定するために使用できる NSX のオプションについて説明します。

NSX は Single Sign-On (SSO) もサポートしています。SSO により NSX は、Active Directory、NIS、LDAP などの他の ID サービスからユーザーを認証できます。

vSphere Web Client のユーザー管理は、NSX コンポーネントの CLI でのユーザー管理とは異なります。

この章には、次のトピックが含まれています。

- [機能別の NSX ユーザーおよび権限](#)
- [Single Sign-On の設定](#)
- [ユーザー権限の管理](#)
- [デフォルト ユーザー アカウントの管理](#)
- [vCenter Server ユーザーへのロールの割り当て](#)
- [ユーザー アカウントの編集](#)
- [ユーザー ロールの変更](#)
- [ユーザー アカウントを無効または有効にする](#)
- [ユーザー アカウントの削除](#)

機能別の NSX ユーザーおよび権限

NSX をデプロイして管理するには、vCenter Server の特定の権限が必要です。NSX によって、各種ユーザーおよびロールの読み取りおよび読み取り/書き込みの拡張権限が提供されます。

ロール定義

有効なロールは次のとおりです。

roles = system_write, system_urm, super_user, vshield_admin, security_admin, auditor, dlp_svm, epsec_host, enterprise_admin, component_manager_user, replicator


```
local_user_roles = system_write, system_urm, super_user, security_admin, auditor, dlp_svm, epsec_host,
component_manager_user, replicator

system_roles = system_write, system_urm, dlp_svm, epsec_host, replicator
```

権限タイプ

権限タイプには読み取りと書き込みがあります。

ロール アクセス定義

ロール アクセス定義によって、ロールに読み取り権限 (read) または読み取り/書き込み権限 (read/write) があるかどうかが決まります。

```
super_user.object_permission = read, write
vshield_admin.object_permission = read, write
security_admin.object_permission = read, write
auditor.object_permission = read
system_write.object_permission = read, write
system_urm.object_permission = read
dlp_svm.object_permission = read, write
epsec_host.object_permission = read, write
enterprise_admin.object_permission = read, write
replicator.object_permission = read, write
```

ルート定義

ルート定義には、スーパーユーザー ロールが記述されます。

```
super_user.superuser = true
system_write.superuser = true
```

グローバル スコープ用オブジェクト アクセスのためのロール

```
vshield_admin.object_access_scope.global = true
super_user.object_access_scope.global = true
system_write.object_access_scope.global = true
system_urm.object_access_scope.global = true
dlp_svm.object_access_scope.global = true
epsec_host.object_access_scope.global = true
enterprise_admin.object_access_scope.global = true
```

ユニバーサル スコープ用オブジェクト アクセスのためのロール

`replicator.object_access_scope.universal=true`

`system_write.object_access_scope.universal=true`

サービス

次のサービスが NSX で使用できます。

administration、urm、edge、app、namespace、spoofguard、dlp、epsec、library、install、vdn、eam、si、truststore、component_manager、ipam、secfabric、security_policy、messaging、replicator

機能定義

各サービス内の機能定義は次のとおりです。

`administration.featurelist = administration.configuration, administration.update, administration.system_events, administration.audit_logs, administration.debug`

`urm.featurelist = urm.user_account_management, urm.object_access_control, urm.feature_access_control`

`edge.featurelist = edge.system, edge.nat, edge.firewall, edge.dhcp, edge.loadbalancer, edge.vpn, edge.syslog, edge.support, edge.routing, edge.certificate, edge.appliance, edge.highavailability, edge.dns, edge.vnic, edge.ssh, edge.autoplumbing, edge.statistics, edge.bridging, edge.systemcontrol`

`app.featurelist = app.config, app.firewall, app.flow, app.forcesync, app.syslog, app.techsupport`

`pgi.featurelist = pgi.switch, pgi.portgroup, pgi.lkm`

`namespace.featurelist = namespace.config`

`spoofguard.featurelist = spoofguard.config`

`dlp.featurelist = dlp.scan_scheduling, dlp.reports, dlp.policy, dlp.svm_interaction`

`epsec.featurelist = epsec.registration, epsec.health_monitoring, epsec.manager, epsec.policy, epsec.svm_priv, epsec.scan, epsec.reports`

`library.featurelist = library.grouping, library.host_preparation, library.tagging`

`install.featurelist = install.app, install.epsec, install.dlp`

`vdn.featurelist = vdn.config_nsm, vdn.provision`

`eam.featurelist = eam.install`

`si.featurelist = si.service, si.serviceprofile`

`truststore.featurelist = truststore.trustentity_management`

`component_manager.featurelist = healthstatus`

`ipam.featurelist = ipam.configuration, ipam.ipallocation`

```

secfabric.featurelist = secfabric.deploy, secfabric.alarms
security_policy.featurelist = security_policy.configuration, security_policy.security_group_binding
blueprint_sam.featurelist = blueprint_sam.reports, blueprint_sam.ad_config,
blueprint_sam.control_data_collection, blueprint_sam.techsupport, blueprint_sam.db_maintain
messaging.featurelist = messaging.messaging
replicator.featurelist = replicator.configuration

```

機能アクセス定義

各機能とロールの組み合わせについては、ユーザーに読み取り専用権限と読み取り/書き込み権限のどちらがあるのが機能アクセス定義に示されます。

機能とロールの組み合わせが列挙されていない場合、そのロールを持つユーザーには、この機能に対するアクセス許可がないことを意味します。

次はその例です。

```

auditor.app.firewall = read
security_admin.app.firewall = read, write

```

これは、app.firewall 機能に対して auditor ロールには読み取り専用アクセス許可があり、security_admin ロールには読み取り/書き込みアクセス許可があることを意味します。

機能アクセス定義 - system_urm

```

system_urm.urm.user_account_management = read

```

機能アクセス定義 - vshield_admin

```

vshield_admin.administration.configuration = read, write
vshield_admin.administration.update = read, write
vshield_admin.administration.system_events = read, write
vshield_admin.administration.audit_logs = read
vshield_admin.urm.user_account_management = read, write
vshield_admin.urm.object_access_control = read
vshield_admin.urm.feature_access_control = read
vshield_admin.edge.system = read, write
vshield_admin.edge.appliance = read, write
vshield_admin.edge.highavailability = read, write
vshield_admin.edge.vnic = read, write
vshield_admin.edge.dns = read

```

vshield_admin.edge.ssh = read, write
vshield_admin.edge.autoplumbing = read
vshield_admin.edge.statistics = read
vshield_admin.edge.nat = read
vshield_admin.edge.dhcp = read
vshield_admin.edge.loadbalancer = read
vshield_admin.edge.vpn = read
vshield_admin.edge.syslog = read, write
vshield_admin.edge.support = read, write
vshield_admin.edge.routing = read
vshield_admin.edge.firewall = read
vshield_admin.edge.bridging = read
vshield_admin.edge.certificate = read
vshield_admin.edge.systemcontrol = read, write
vshield_admin.library.grouping = read
vshield_admin.app.config = read, write
vshield_admin.app.forcesync = read, write
vshield_admin.app.syslog = read, write
vshield_admin.app.techsupport = read, write
vshield_admin.namespace.config = read, write
vshield_admin.dlp.scan_scheduling = read, write
vshield_admin.epsec.reports = read, write
vshield_admin.epsec.registration = read, write
vshield_admin.epsec.health_monitoring = read
vshield_admin.epsec.policy = read, write
vshield_admin.epsec.scan_scheduling = read, write
vshield_admin.library.host_preparation = read, write
vshield_admin.library.tagging = read
vshield_admin.install.app = read, write
vshield_admin.install.epsec = read, write
vshield_admin.install.dlp = read, write
vshield_admin.vdn.config_nsm = read, write

vshield_admin.vdn.provision = read, write
vshield_admin.eam.install = read, write
vshield_admin.si.service = read, write
vshield_admin.si.serviceprofile = read, write
vshield_admin.truststore.trustentity_management = read, write
vshield_admin.ipam.configuration = read, write
vshield_admin.ipam.ipallocation = read, write
vshield_admin.secfabric.deploy = read, write
vshield_admin.secfabric.alarms = read_write
vshield_admin.blueprint_sam.ad_config = read, write
vshield_admin.blueprint_sam.control_data_collection = read, write
vshield_admin.blueprint_sam.techsupport = read, write
vshield_admin.blueprint_sam.db_maintain = read, write
vshield_admin.messaging.messaging = read, write
vshield_admin.replicator.configuration = read, write

機能アクセス定義 - security_admin

security_admin.administration.system_events = read, write
security_admin.administration.audit_logs = read
security_admin.edge.system = read
security_admin.edge.appliance = read
security_admin.edge.highavailability = read
security_admin.edge.vnic = read, write
security_admin.edge.dns = read, write
security_admin.edge.ssh = read, write
security_admin.edge.autoplumbing = read, write
security_admin.edge.statistics = read
security_admin.edge.nat = read, write
security_admin.edge.dhcp = read, write
security_admin.edge.loadbalancer = read, write
security_admin.edge.vpn = read, write
security_admin.edge.syslog = read, write

security_admin.edge.support = read, write
security_admin.edge.routing = read, write
security_admin.edge.firewall = read, write
security_admin.edge.bridging = read, write
security_admin.edge.certificate = read, write
security_admin.edge.systemcontrol = read, write
security_admin.app.firewall = read, write
security_admin.app.flow = read, write
security_admin.app.forcesync = read
security_admin.app.syslog = read
security_admin.namespace.config = read
security_admin.spoofguard.config = read, write
security_admin.dlp.reports = read, write
security_admin.dlp.policy = read, write
security_admin.epsec.policy = read, write
security_admin.epsec.reports = read
security_admin.epsec.health_monitoring = read
security_admin.library.grouping = read, write
security_admin.library.tagging = read, write
security_admin.install.app = read
security_admin.install.epsec = read
security_admin.install.dlp = read
security_admin.vdn.config_nsm = read
security_admin.vdn.provision = read
security_admin.eam.install = read
security_admin.si.service = read, write
security_admin.si.serviceprofile = read
security_admin.truststore.trustentity_management = read, write
security_admin.ipam.configuration = read, write
security_admin.ipam.ipallocation = read, write
security_admin.secfabric.alarms = read
security_admin.secfabric.deploy = read

security_admin.security_policy.configuration = read, write
security_admin.security_policy.security_group_binding = read, write
security_admin.blueprint_sam.reports = read
security_admin.blueprint_sam.ad_config = read
security_admin.blueprint_sam.control_data_collection = read
security_admin.blueprint_sam.db_maintain = read
security_admin.messaging.messaging = read, write
security_admin.replicator.configuration = read

機能アクセス定義 - auditor

auditor.administration.system_events = read
auditor.administration.audit_logs = read
auditor.edge.appliance = read
auditor.edge.highavailability = read
auditor.edge.vnic = read
auditor.edge.dns = read
auditor.edge.ssh = read
auditor.edge.autoplumbing = read
auditor.edge.statistics = read
auditor.edge.nat = read
auditor.edge.dhcp = read
auditor.edge.loadbalancer = read
auditor.edge.vpn = read
auditor.edge.syslog = read
auditor.edge.routing = read
auditor.edge.firewall = read
auditor.edge.bridging = read
auditor.edge.system = read
auditor.edge.certificate = read
auditor.edge.systemcontrol = read
auditor.app.firewall = read
auditor.app.flow = read

auditor.app.forcesync = read
auditor.app.syslog = read
auditor.namespace.config = read
auditor.spoofguard.config = read
auditor.dlp.scan_scheduling = read
auditor.dlp.policy = read
auditor.dlp.reports = read
auditor.library.grouping = read
auditor.epsec_host.health_monitoring = read
auditor.epsec.policy = read
auditor.epsec.reports = read
auditor.epsec.registration = read
auditor.vdn.config_nsm = read
auditor.epsec.scan_scheduling = read
auditor.vdn.provision = read
auditor.si.service = read
auditor.si.serviceprofile = read
auditor.truststore.trustentity_management = read
auditor.secfabric.alarms = read
auditor.secfabric.deploy = read
auditor.security_policy.configuration = read
auditor.security_policy.security_group_binding = read
auditor.blueprint_sam.reports = read
auditor.blueprint_sam.ad_config = read
auditor.blueprint_sam.control_data_collection = read
auditor.blueprint_sam.db_maintain = read
auditor.library.tagging = read
auditor.ipam.configuration = read
auditor.ipam.ipallocation = read
auditor.messaging.messaging = read
auditor.replicator.configuration = read

機能アクセス定義 - dlp_svm

dlp_svm.dlp.svm_interaction = read, write
dlp_svm.epsec.svm_priv = read, write
dlp_svm.epsec.registration = read
dlp_svm.epsec.policy = read
dlp_svm.epsec.scan_scheduling = read
dlp_svm.library.host_preparation = read, write
dlp_svm.library.tagging = read, write

機能アクセス定義 - epsec_host

epsec_host.epsec.registration = read
epsec_host.epsec.health_monitoring = write

機能アクセス定義 - enterprise_admin

enterprise_admin.administration.configuration = read, write
enterprise_admin.administration.update = read, write
enterprise_admin.administration.system_events = read, write
enterprise_admin.administration.audit_logs = read
enterprise_admin.urm.user_account_management = read, write
enterprise_admin.urm.object_access_control = read
enterprise_admin.urm.feature_access_control = read
enterprise_admin.edge.system = read, write
enterprise_admin.edge.appliance = read, write
enterprise_admin.edge.highavailability = read, write
enterprise_admin.edge.vnic = read, write
enterprise_admin.edge.dns = read, write
enterprise_admin.edge.ssh = read, write
enterprise_admin.edge.autoplumbing = read, write
enterprise_admin.edge.statistics = read, write
enterprise_admin.edge.nat = read, write
enterprise_admin.edge.dhcp = read, write

enterprise_admin.edge.loadbalancer = read, write
enterprise_admin.edge.vpn = read, write
enterprise_admin.edge.syslog = read, write
enterprise_admin.edge.support = read, write
enterprise_admin.edge.routing = read, write
enterprise_admin.edge.firewall = read, write
enterprise_admin.edge.bridging = read, write
enterprise_admin.edge.certificate = read, write
enterprise_admin.edge.systemcontrol = read, write
enterprise_admin.library.grouping = read, write
enterprise_admin.library.host_preparation = read, write
enterprise_admin.library.tagging = read, write
enterprise_admin.app.config = read, write
enterprise_admin.app.forcesync = read, write
enterprise_admin.app.syslog = read, write
enterprise_admin.app.techsupport = read, write
enterprise_admin.app.firewall = read, write
enterprise_admin.app.flow = read, write
enterprise_admin.namespace.config = read, write
enterprise_admin.dlp.scan_scheduling = read, write
enterprise_admin.dlp.reports = read, write
enterprise_admin.dlp.policy = read, write
enterprise_admin.epsec.registration = read, write
enterprise_admin.epsec.health_monitoring = read
enterprise_admin.epsec.scan_scheduling = read, write
enterprise_admin.epsec.reports = read, write
enterprise_admin.epsec.policy = read, write
enterprise_admin.install.app = read, write
enterprise_admin.install.epsec = read, write
enterprise_admin.install.dlp = read, write
enterprise_admin.eam.install = read, write
enterprise_admin.spoofguard.config = read, write

enterprise_admin.vdn.config_nsm = read, write
enterprise_admin.vdn.provision = read, write
enterprise_admin.si.service = read, write
enterprise_admin.si.serviceprofile = read, write
enterprise_admin.truststore.trustentity_management = read, write
enterprise_admin.ipam.configuration = read, write
enterprise_admin.ipam.ipallocation = read, write
enterprise_admin.secfabric.deploy = read, write
enterprise_admin.secfabric.alarms = read, write
enterprise_admin.security_policy.configuration = read, write
enterprise_admin.security_policy.security_group_binding = read, write
enterprise_admin.blueprint_sam.reports = read
enterprise_admin.blueprint_sam.ad_config = read, write
enterprise_admin.blueprint_sam.control_data_collection = read, write
enterprise_admin.blueprint_sam.techsupport = read, write
enterprise_admin.blueprint_sam.db_maintain = read, write
enterprise_admin.messaging.messaging = read, write
enterprise_admin.replicator.configuration = read, write

機能アクセス定義 - component_manager_user

component_manager_user.component_manager.healthstatus = read

機能アクセス定義 - replicator

replicator.administration.configuration = read, write
replicator.administration.update = read, write
replicator.administration.system_events = read, write
replicator.administration.audit_logs = read
replicator.urm.user_account_management = read, write
replicator.urm.object_access_control = read
replicator.urm.feature_access_control = read
replicator.edge.system = read, write
replicator.edge.appliance = read, write

replicator.edge.highavailability = read
replicator.edge.vnic = read, write
replicator.edge.dns = read
replicator.edge.ssh = read
replicator.edge.autoplumbing = read, write
replicator.edge.statistics = read
replicator.edge.nat = read
replicator.edge.dhcp = read, write
replicator.edge.loadbalancer = read
replicator.edge.vpn = read
replicator.edge.syslog = read
replicator.edge.support = read
replicator.edge.routing = read, write
replicator.edge.firewall = read
replicator.edge.bridging = read
replicator.edge.certificate = read
replicator.edge.systemcontrol = read
replicator.library.grouping = read, write
replicator.library.host_preparation = read, write
replicator.library.tagging = read, write
replicator.app.config = read, write
replicator.app.forcesync = read, write
replicator.app.syslog = read, write
replicator.app.techsupport = read, write
replicator.app.firewall = read, write
replicator.app.flow = read, write
replicator.namespace.config = read, write
replicator.dlp.scan_scheduling = read, write
replicator.dlp.reports = read, write
replicator.dlp.policy = read, write
replicator.epsec.registration = read, write
replicator.epsec.health_monitoring = read

replicator.epsec.scan_scheduling = read, write
replicator.epsec.reports = read, write
replicator.epsec.policy = read, write
replicator.install.app = read, write
replicator.install.epsec = read, write
replicator.install.dlp = read, write
replicator.eam.install = read, write
replicator.spoofguard.config = read, write
replicator.vdn.config_nsm = read, write
replicator.vdn.provision = read, write
replicator.si.service = read, write
replicator.si.serviceprofile = read, write
replicator.truststore.trustentity_management = read, write
replicator.ipam.configuration = read, write
replicator.ipam.ipallocation = read, write
replicator.secfabric.deploy = read, write
replicator.secfabric.alarms = read, write
replicator.security_policy.configuration = read, write
replicator.security_policy.security_group_binding = read, write
replicator.blueprint_sam.reports = read
replicator.blueprint_sam.ad_config = read, write
replicator.blueprint_sam.control_data_collection = read, write
replicator.blueprint_sam.techsupport = read, write
replicator.blueprint_sam.db_maintain = read, write
replicator.messaging.messaging = read, write
replicator.replicator.configuration = read, write

ユニバーサル オブジェクトのセカンダリ ノードに対するロールの上書き機能権限

secondary.super_user.edge.highavailability = read, write
secondary.enterprise_admin.edge.highavailability = read, write
secondary.vshield_admin.edge.highavailability = read, write
secondary.super_user.edge.ssh = read, write

secondary.enterprise_admin.edge.ssh = read, write
secondary.security_admin.edge.ssh = read, write
secondary.vshield_admin.edge.ssh = read, write
secondary.super_user.edge.syslog = read, write
secondary.enterprise_admin.edge.syslog = read, write
secondary.security_admin.edge.syslog = read, write
secondary.vshield_admin.edge.syslog = read, write
secondary.super_user.edge.support = read, write
secondary.enterprise_admin.edge.support = read, write
secondary.security_admin.edge.support = read, write
secondary.vshield_admin.edge.support = read, write
secondary.super_user.edge.routing = read, write
secondary.security_admin.edge.routing = read, write
secondary.enterprise_admin.edge.routing = read, write
secondary.super_user.edge.appliance = read, write
secondary.vshield_admin.edge.appliance = read, write
secondary.enterprise_admin.edge.appliance = read, write
secondary.super_user.edge.vnic = read, write
secondary.vshield_admin.edge.vnic = read, write
secondary.enterprise_admin.edge.vnic = read, write
secondary.super_user.edge.firewall = read, write
secondary.vshield_admin.edge.firewall = read, write
secondary.enterprise_admin.edge.firewall = read, write

Single Sign-On の設定

SSO を使用することで、さまざまなコンポーネントがセキュアなトークン交換メカニズムを介した相互通信を行えるため、各コンポーネントが個別にユーザーを認証する必要がなく、vSphere と NSX のセキュリティを高めることができます。NSX Manager で Lookup Service を設定し、SSO 管理者の認証情報を入力して、NSX 管理サービスを SSO ユーザーとして登録することができます。Single Sign On (SSO) サービスを NSX に統合すると、vCenter ユーザーに対するユーザー認証のセキュリティが強化され、NSX が AD、NIS、LDAP など他の ID サービスからユーザーを認証できるようになります。

SSO により NSX は、REST API 呼び出しを介して、信頼されるソースからの認証済み Security Assertion Markup Language (SAML) トークンを使用する認証をサポートします。また NSX Manager では、他の VMware ソリューションで使用する認証 SAML トークンを取得できます。

NSX は、SSO ユーザーのグループ情報をキャッシュします。グループ メンバーシップを変更すると、ID プロバイダ (Active Directory など) から NSX への伝達に最大 60 分かかります。

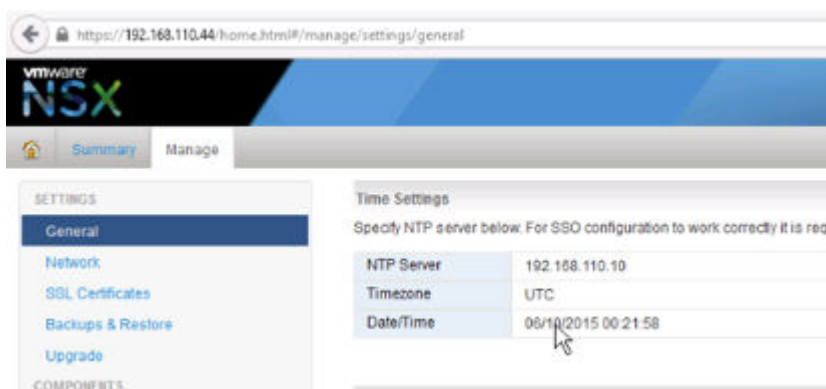
前提条件

- NSX Manager で SSO を使用するには、vCenter Server 5.5 以降が必要であり、vCenter Server に Single Sign-On (SSO) 認証サービスがインストールされている必要があります。これは組み込みの SSO が対象であることに注意してください。代わりに、デプロイで、外部の一元化された SSO サーバが使用される場合があります。

vSphere が提供する SSO サービスの詳細については、<http://kb.vmware.com/kb/2072435> および <http://kb.vmware.com/kb/2113115> を参照してください。

- SSO サーバの時間と NSX Manager の時間が同期するよう、NTP サーバを指定する必要があります。

次はその例です。



手順

- 1 NSX Manager 仮想アプライアンスにログインします。

Web ブラウザで、NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>> または <https://<nsx-manager-hostname>>) に移動し、NSX Manager のインストール時に設定したパスワードを使用して admin としてログインします。

- 2 [管理 (Manage)] タブをクリックして、[NSX 管理サービス (NSX Management Service)] をクリックします。

- 3 Lookup Service が実行されるホストの名前または IP アドレスを入力します。

vCenter Server を使用して Lookup Service を実行する場合は、vCenter Server の IP アドレスまたはホスト名を入力し、vCenter Server のユーザー名とパスワードを入力します。

4 ポート番号を入力します。

vSphere 6.0 を使用している場合はポート 443 を入力し、vSphere 5.5 を使用している場合はポート 7444 を使用します。

Lookup Service の URL は、指定されたホストおよびポートに基づいて表示されます。

次はその例です。

Lookup Service

For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service IP: 192.168.110.26

Lookup Service Port: 443

Lookup Service: https://192.168.110.26:443/lookupservice/sdk

SSO Administrator User Name: administrator@vsphere.local

Password: *****

OK Cancel

5 証明書のサム プリントが vCenter Server の証明書と一致することを確認します。

CA サーバに CA 署名付き証明書をインストールした場合は、CA 署名付き証明書のサムプリントが表示されます。CA 署名付き証明書をインストールしていない場合は、自己署名証明書が表示されます。

6 Lookup Service のステータスが [接続中 (Connected)] になっていることを確認します。

次はその例です。

Lookup Service

For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service: https://192.168.110.26:443/lookupservice/sdk

SSO Administrator User Name: administrator@vsphere.local

Status: ● Connected

次のステップ

SSO ユーザーにロールを割り当てます。

ユーザー権限の管理

ユーザーのロールによって、指定されたリソースに対してユーザーが実行できるアクションが定義されます。ユーザーのロールに応じて、指定されたリソースのアクティビティへのアクセスが許可されます。また、ユーザーがアクセスできるのは、該当する操作を完了するために必要な機能のみです。これにより、特定のリソースに対するドメインの管理が可能になります。また、権限に制限がない場合は、システム全体を管理できます。

次のルールが適用されます。

- 1 名のユーザーには 1 つのロールのみ割り当てることができます。

- ユーザーにロールを追加したり、ユーザーに割り当てられたロールを削除することはできません。ただし、ユーザーに対するロールの割り当てを変更することはできます。

表 21-1. NSX Manager のユーザー ロール

権限	許可される処理
Enterprise Administrator	NSX の操作およびセキュリティ。
NSX Administrator	NSX の操作のみ：たとえば、仮想アプライアンスのインストール、ポート グループの設定などが可能です。
Security Administrator	NSX のセキュリティのみ：たとえば、データ セキュリティ ポリシーの定義、ポート グループの作成、NSX モジュール用のレポート作成などが可能です。
Auditor	読み取り専用。

Enterprise Administrator ロールと NSX Administrator ロールは vCenter Server のユーザーにのみ割り当てることができます。

デフォルト ユーザー アカウントの管理

NSX Manager ユーザー インターフェイスには、すべてのリソースへのアクセス権限が付与されたユーザー アカウントがあります。このユーザーの権限を編集したり、削除したりすることはできません。デフォルトのユーザー名は **admin** で、デフォルトのパスワードは **default** または NSX Manager のインストール時に指定したパスワードです。

NSX Manager アプライアンスの **admin** ユーザーは、CLI コマンドでのみ管理できます。

vCenter Server ユーザーへのロールの割り当て

SSO ユーザーにロールを割り当てると、vCenter Server はその SSO サーバで設定されている ID サービスを使用してユーザーを認証します。SSO サーバが構成されていないか使用不可の場合、ユーザーは vCenter Server の設定に基づいてローカルに、または Active Directory によって認証されます。

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、[NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックして、[管理] タブをクリックします。
- 4 [ユーザー] をクリックします。
- 5 [追加] をクリックします。
[ロールの割り当て] ウィンドウが開きます。
- 6 [vCenter ユーザーを指定する] または [vCenter グループを指定する] をクリックします。
- 7 vCenter Server の [ユーザー] 名、またはユーザーの [グループ] 名を入力します。

詳細については、次の例を参照してください。

ドメイン名 : corp.vmware.com

エイリアス : corp

グループ名 : group1@corp.vmware.com

ユーザー名 : user1@corp.vmware.com

グループに NSX Manager のロールを割り当てると、そのグループのユーザーは NSX Manager のユーザー インターフェイスにログインできます。

ロールをユーザーに割り当てる場合、ユーザーのエイリアスを入力します。たとえば、user1@corp と入力します。

- 8 [次へ] をクリックします。
- 9 このユーザーのロールを選択し、[次へ] をクリックします。使用可能なロールの詳細については、[「ユーザー権限の管理」](#)を参照してください。
- 10 [終了] をクリックします。

作成したユーザー アカウントが Users テーブルに表示されます。

グループ ベースのロール割り当てについて

組織は、ユーザーを適切に管理するためにユーザー グループを作成します。SSO との統合後、NSX Manager はユーザーが属するグループの詳細情報を取得できます。同じグループに属する可能性がある個々のユーザーにロールを割り当てる代わりに、NSX Manager はグループにロールを割り当てます。NSX Manager がロールをどのように割り当てるかについて、次のシナリオで説明します。

例：ロール ベースのアクセス制御のシナリオ

このシナリオでは、IT ネットワーク エンジニア (Sally Moore) に、次の環境内の NSX コンポーネントへのアクセス権を与えます。

Active Directory ドメイン : corp.local、vCenter グループ : neteng@corp.local、ユーザー名 : smoore@corp.local

前提条件 : vCenter Server が NSX Manager に登録されており、SSO が構成されている。

- 1 ロールを Sally に割り当てます。
 - a vSphere Web Client にログインします。
 - b [Networking and Security] をクリックし、[NSX Manager] をクリックします。
 - c [名前] 列で NSX Manager をクリックして、[管理] タブをクリックします。
 - d [ユーザー] をクリックし、[追加] をクリックします。
[ロールの割り当て] ウィンドウが開きます。
 - e [vCenter グループを指定する] をクリックし、[グループ] に **neteng@corp.local** と入力します。
 - f [次へ] をクリックします。
 - g [ロールの選択] で [NSX Administrator] をクリックし、[次へ] をクリックします。
- 2 データセンターに対する権限を Sally に付与します。
 - a [ホーム] アイコンをクリックして、[vCenter ホーム] - [データセンター] をクリックします。

- b データセンターを選択し、[アクション] - [すべての vCenter アクション] - [権限の追加] をクリックします。
- c [追加] をクリックし、ドメイン CORP を選択します。
- d [ユーザーとグループ] で [最初にグループを表示] を選択します。
- e NetEng を選択し、[OK] をクリックします。
- f [割り当てられたロール] で、[読み取り専用] を選択し、[子へ伝達] を選択解除して、[OK] をクリックします。

3 vSphere Web Client からログアウトし、smoore@corp.local として再度ログインします。

Sally は NSX 操作のみを実行できます。たとえば、仮想アプライアンスのインストール、論理スイッチの作成などが可能です。

例：ユーザー グループのメンバーシップ経由で権限を継承するシナリオ

グループ オプション	値
名前	G1
割り当てられたロール	Auditor (読み取り専用)
リソース	グローバル ルート

ユーザー オプション	値
名前	John
属するグループ	G1
割り当てられたロール	なし

John は、Auditor ロールが割り当てられているグループ G1 に属しています。John は、グループ ロールとリソース権限を継承します。

例：複数グループに属するユーザー メンバーのシナリオ

グループ オプション	値
名前	G1
割り当てられたロール	Auditor (読み取り専用)
リソース	グローバル ルート

グループ オプション	値
名前	G2
割り当てられたロール	Security Administrator (読み取りと書き込み)
リソース	Datacenter1

ユーザー オプション	値
名前	Joseph
属するグループ	G1、G2
割り当てられたロール	なし

Joseph はグループ G1 と G2 に属しており、Auditor ロールと Security Administrator ロールの権利と権限の組み合わせを継承します。たとえば、John には次の権限があります。

- Datacenter1 の読み取り、書き込み (Security Administrator ロール)
- グローバル ルートの読み取り専用 (Auditor)

例：複数ロールを持つユーザー メンバーのシナリオ

グループ オプション	値
名前	G1
割り当てられたロール	Enterprise Administrator
リソース	グローバル ルート

ユーザー オプション	値
名前	Bob
属するグループ	G1
割り当てられたロール	Security Administrator (読み取りと書き込み)
リソース	Datacenter1

Bob には Security Administrator ロールが割り当てられているため、グループ ロールの権限を継承しません。Bob には次の権限があります。

- Datacenter1 とその子リソースの読み取り、書き込み (Security Administrator ロール)
- Datacenter1 での Enterprise Administrator ロール

ユーザー アカウントの編集

ユーザー アカウントを編集して、ロールまたはスコープを変更することができます。**admin** アカウントは編集できません。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前 ()] 列で NSX Manager をクリックして、[管理 (Manage)] タブをクリックします。
- 4 [ユーザー (Users)] をクリックします。
- 5 編集するユーザーを選択します。
- 6 [編集 (Edit)] をクリックします。
- 7 必要な変更を実行します。
- 8 [終了 (Finish)] をクリックして、変更内容を保存します。

ユーザー ロールの変更

admin ユーザーを除くすべてのユーザーについて、ロールの割り当てを変更できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックして、[管理 (Manage)] タブをクリックします。
- 4 [ユーザー (Users)] をクリックします。
- 5 ロールを変更するユーザーを選択します。
- 6 [ロールの変更 (Change Role)] をクリックします。
- 7 必要な変更を実行します。
- 8 [終了 (Finish)] をクリックして、変更内容を保存します。

ユーザー アカウントを無効または有効にする

ユーザー アカウントを無効にして、そのユーザーが NSX Manager にログインできないようにすることができます。

admin ユーザーまたは現在 NSX Manager にログインしているユーザーを無効にできません。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前 ()] 列で NSX Manager をクリックして、[管理 (Manage)] タブをクリックします。
- 4 [ユーザー (Users)] をクリックします。
- 5 ユーザー アカウントを選択します。
- 6 [有効化 (Enable)] または [無効化 (Disable)] アイコンをクリックします。

ユーザー アカウントの削除

作成したユーザー アカウントは削除できます。**admin** アカウントは削除できません。削除されたユーザーに対する監査レコードは、データベースに保持され、監査ログ レポートで参照できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。

- 3 [名前 ()] 列で NSX Manager をクリックして、[管理 (Manage)] タブをクリックします。
- 4 [ユーザー (Users)] をクリックします。
- 5 ユーザー アカウントを選択します。
- 6 [削除 (Delete)] をクリックします。
- 7 [OK] をクリックして削除を確認します。

vCenter Server のユーザー アカウントを削除する場合、NSX Manager 用のロール割り当てだけが削除されます。vCenter Server 上のユーザー アカウントは削除されません。

ネットワークおよびセキュリティ オブジェクト

22

このセクションでは、カスタム ネットワークとセキュリティ コンテナについて説明します。これらのコンテナは、Distributed Firewall と Service Composer で使用できます。Cross-vCenter NSX 環境では、ユニバーサル Distributed Firewall ルールで使用するユニバーサル ネットワークとセキュリティ コンテナを作成できます。ユニバーサル ネットワークおよびセキュリティ オブジェクトを Service Composer で使用することはできません。

この章には、次のトピックが含まれています。


- IP アドレス グループの操作
- MAC アドレス グループの操作
- IP アドレス プールの操作
- Security Groups の操作
- サービスおよびサービス グループの操作

IP アドレス グループの操作

IP アドレス グループの作成

IP アドレス グループを作成してから、このグループを送信元または送信先としてファイアウォール ルールに追加できます。そのようなルールにより、仮想マシンから物理マシンを、またはその逆方向でマシンを保護することができます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル IP アドレス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループオブジェクト] タブをクリックして、[IP セット] をクリックします。
- 5 [追加] () アイコンをクリックします。
- 6 アドレス グループの名前を入力します。

- 7 (オプション) アドレス グループの説明を入力します。
- 8 アドレス グループに含める IP アドレスを入力します。
- 9 (オプション) [継承を有効にして、基礎となるスコープで表示できるようにします] を選択します。
- 10 (オプション) ユニバーサル IP アドレス グループを作成する場合は、[このオブジェクトをユニバーサル同期の対象としてマーク] を選択します。
- 11 [OK] をクリックします。

IP アドレス グループの編集

前提条件

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル IP アドレス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト] タブをクリックして、[IP セット] をクリックします。
- 5 編集するグループを選択して、[編集 (Edit)] (✎) アイコンをクリックします。
- 6 [IP セットの編集] ダイアログ ボックスで、必要な変更を行います。
- 7 [OK] をクリックします。

IP アドレス グループの削除

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル IP アドレス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[IP セット (IP Sets)] をクリックします。
- 5 削除するグループを選択し、[削除 (Delete)] (✖) アイコンをクリックします。

MAC アドレス グループの操作

MAC アドレス グループの作成

一定範囲の MAC アドレスで設定される MAC アドレス グループを作成してから、そのグループを分散ファイアウォール ルールにソースまたはターゲットとして追加できます。このルールにより、仮想マシンから物理マシンを、または物理マシンから仮想マシンを保護することができます。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル MAC アドレス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[MAC セット (MAC Sets)] をクリックします。
- 5 [追加] (+) アイコンをクリックします。
- 6 アドレス グループの名前を入力します。
- 7 (オプション) アドレス グループの説明を入力します。
- 8 グループに含める MAC アドレスを入力します。
- 9 (オプション) [継承を有効にして、基礎となるスコープで表示できるようにします] を選択します。
- 10 (オプション) ユニバーサル MAC アドレス グループを作成する場合は、[このオブジェクトをユニバーサル同期の対象としてマーク] を選択します。
- 11 [OK] をクリックします。

MAC アドレス グループの編集


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル MAC アドレス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[MAC セット (MAC Sets)] をクリックします。

- 5 編集するグループを選択して、[編集 (Edit)] () アイコンをクリックします。
- 6 [MAC セットの編集] ダイアログ ボックスで、必要な変更を行います。
- 7 [OK] をクリックします。

MAC アドレス グループの削除

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル MAC アドレス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[MAC セット (MAC Sets)] をクリックします。
- 5 削除するグループを選択し、[削除 (Delete)] () アイコンをクリックします。

IP アドレス プールの操作

IP アドレス プールを編集または削除できます。

IP アドレス プール追加の詳細については、[「ネットワーク アクセス SSL VPN-Plus の設定」](#) または [「Web Access SSL VPN-Plus の設定」](#) を参照してください。

IP アドレス プールの作成

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[IP アドレス プール (IP Pool)] をクリックします。
- 5 [新規 IP アドレス プールの追加 (Add New IP Pool)] アイコンをクリックします。
- 6 IP アドレス プールの名前を入力し、デフォルト ゲートウェイとプリフィックスの長さを入力します。
- 7 (オプション) プライマリおよびセカンダリ DNS と、DNS サフィックスを入力します。
- 8 プールに含める IP アドレス範囲を入力し、[OK] をクリックします。

IP アドレス プールの編集

IP アドレス プールを編集できます (CIDR およびゲートウェイは編集できません)。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
- 4 [グループオブジェクト (Grouping Objects)] タブをクリックして、[IP アドレス プール (IP Pools)] をクリックします。
- 5 IP アドレス プールを選択し、[編集 (Edit)] アイコンをクリックします。
- 6 必要な変更を行い、[OK] をクリックします。

IP アドレス プールの削除

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
- 4 [グループオブジェクト (Grouping Objects)] タブをクリックして、[IP アドレス プール (IP Pool)] をクリックします。
- 5 削除する IP アドレス プールを選択し、[削除 (Delete)] アイコンをクリックします。

Security Groups の操作

Security Groups は、vSphere インベントリの資産またはグループ オブジェクトの集合体です。

Security Group の作成

NSX Manager レベルで Security Group を作成できます。

前提条件

Active Directory グループ オブジェクトに基づいて Security Group を作成する場合、1 つ以上のドメインが NSX Manager に登録されていることを確認します。NSX Manager は、グループ、ユーザー情報、およびこれらの間の関係を登録先の各ドメインから取得します。[\[NSX Manager への Windows ドメインの登録\]](#) を参照してください。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサルセキュリティ グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループオブジェクト (Grouping Objects)] タブをクリックし、[Security Group]、[Security Group の追加 (Add Security Group)] アイコンの順にクリックします。
- 5 Security Group の名前と説明（説明は任意）を入力します。
- 6 (オプション) ユニバーサル Security Group を作成する必要がある場合、[このオブジェクトをユニバーサル同期の対象としてマーク (Mark this object for universal synchronization)] を選択します。
- 7 [次へ (Next)] をクリックします。
- 8 [動的メンバーシップ] ページで、作成中の Security Group に追加するオブジェクトが満たす必要のある基準を定義します。これにより、フィルタ基準を定義して検索基準を満たす仮想マシンを含めることができます。フィルタ基準では、多数のパラメータがサポートされています。

注: ユニバーサル Security Group を作成する場合、[動的メンバーシップの定義] の手順は利用できません。

たとえば、指定したセキュリティ タグ (AntiVirus.virusFound など) でタグ付けされた仮想マシンのすべてを Security Group に追加するための基準を含めることができます。セキュリティ タグでは大文字と小文字が区別されます。

または、**W2008** という名前を含むすべての仮想マシンや、論理スイッチ **global_wire** に含まれる仮想マシンを Security Group に追加することもできます。

- 9 [次へ (Next)] をクリックします。

- 10 [含めるオブジェクトの選択] ページで、追加するリソースのタブを選択し、Security Group に追加するリソースを 1 つ以上選択します。Security Group には次のオブジェクトを含めることができます。

表 22-1. Security Group およびユニバーサル Security Group に含めることができるオブジェクト。

Security Group	ユニバーサル Security Group
<ul style="list-style-type: none"> ■ 作成中の Security Group 内にネストされた他の Security Group。 ■ クラスタ ■ 論理スイッチ ■ ネットワーク ■ 仮想 App ■ データセンター ■ IP セット ■ ディレクトリ グループ 	<ul style="list-style-type: none"> ■ 作成中のユニバーサル Security Group 内にネストされた他のユニバーサル Security Group。 ■ ユニバーサル IP セット ■ ユニバーサル MAC セット
<p>注: NSX Security Group の Active Directory の設定は、vSphere SSO の Active Directory 構成とは異なります。NSX Active Directory グループの設定はゲスト仮想マシンにアクセスするエンド ユーザー用であり、vSphere SSO は vSphere および NSX を使用する管理者用です。これらのディレクトリ グループを使用するには、Active Directory との同期が必要です。章 11 「Identity Firewall の概要」 を参照してください。</p>	
<ul style="list-style-type: none"> ■ MAC セット ■ セキュリティ タグ ■ vNIC ■ 仮想マシン ■ リソース プール ■ 分散仮想ポート グループ 	

ここで選択したオブジェクトは、[手順 8](#) の基準を満たすかどうかにかかわらず、常に Security Group に含まれます。

Security Group に 1 つのリソースを追加すると、関連するすべてのリソースも自動的に追加されます。たとえば、仮想マシンを選択すると、関連する vNIC が自動的にその Security Group に追加されます。

- 11 [次へ (Next)] をクリックして、Security Group から除外するオブジェクトを選択します。

注: ユニバーサル Security Group を作成する場合、[\[除外するオブジェクトの選択\]](#) の手順は使用できません。

ここで選択したオブジェクトは、動的基準を満たすかどうかにかかわらず、常に Security Group から除外されます。

- 12 [終了 (Finish)] をクリックします。

Security Group のメンバーシップは、次のように決まります。

{式の結果 ([手順 8](#) で生成) + 含まれるアイテム ([手順 10](#) で指定)} - 除外されるアイテム ([手順 11](#) で指定)

つまり、含まれるアイテムが最初に式の結果に追加されます。次に、除外されるアイテムが、結合された結果から差し引かれます。

セキュリティ グループの編集

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサルセキュリティ グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループオブジェクト] タブをクリックして、[セキュリティ グループ] をクリックします。
- 5 編集するグループを選択して、[編集] (✎) アイコンをクリックします。
- 6 [セキュリティ グループの編集] ダイアログ ボックスで、必要な変更を行います。
- 7 [OK] をクリックします。

セキュリティ グループの削除

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサルセキュリティ グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループオブジェクト (Grouping Objects)] タブをクリックして、[セキュリティ グループ (Security Group)] をクリックします。
- 5 削除するグループを選択し、[削除 (Delete)] (✖) アイコンをクリックします。

サービスおよびサービス グループの操作


サービスはプロトコルとポートの組み合わせで、サービス グループはサービスや他のサービス グループの集合です。

サービスの作成

サービスを作成してから、そのサービスに適用するルールを定義できます。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル サービスの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[サービス (Service)] をクリックします。
- 5 [追加] () アイコンをクリックします。
- 6 サービスを識別する [名前 (Name)] を入力します。
- 7 (オプション) サービスの [説明 (Description)] を入力します。
- 8 [プロトコル (Protocol)] を選択します。
 - a 選択したプロトコルによっては、ターゲット ポートなどのその他の情報の入力を求められる場合があります。
- 9 (オプション) [継承を有効にして、基礎となるスコープで表示できるようにします] を選択します。
- 10 (オプション) ユニバーサル サービスを作成する場合は、[このオブジェクトをユニバーサル同期の対象としてマーク] を選択します。
- 11 [OK] をクリックします。

サービスが [サービス] テーブルに表示されます。

サービス グループの作成

サービス グループを作成して、そのサービス グループに適用するルールを定義できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル サービス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[セキュリティ グループ (Service Groups)] をクリックします。
- 5 [追加 (Add)] アイコンをクリックします。
- 6 サービス グループを識別する [名前 (Name)] を入力します。
- 7 (オプション) サービス グループの [説明 (Description)] を入力します。
- 8 (オプション) ユニバーサル サービス グループを作成する場合は、[このオブジェクトをユニバーサル同期の対象としてマーク] を選択します。
- 9 [メンバー] で、グループに追加するサービスまたはサービス グループを選択します。


10 (オプション) [継承を有効にして、基礎となるスコープで表示できるようにします] を選択します。

11 [OK] をクリックします。

サービスまたはサービス グループの編集

サービスおよびサービス グループを編集できます。


手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル サービスまたはサービス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[サービス (Service)] または [サービス グループ (Service Groups)] をクリックします。
- 5 カスタム サービスまたはサービス グループを選択し、[編集 (Edit)] () アイコンをクリックします。
- 6 適切に変更します。
- 7 [OK] をクリックします。

サービスまたはサービス グループの削除

サービスまたはサービス グループを削除できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[管理] タブをクリックします。
 - ◆ ユニバーサル サービスまたはサービス グループの管理が必要な場合は、プライマリ NSX Manager を選択する必要があります。
- 4 [グループ オブジェクト (Grouping Objects)] タブをクリックして、[サービス (Service)] または [サービス グループ (Service Groups)] をクリックします。
- 5 カスタム サービスまたはサービス グループを選択し、[削除 (Delete)] () アイコンをクリックします。
- 6 [はい (Yes)] をクリックします。

サービスまたはサービス グループが削除されます。

操作と管理

この章には、次のトピックが含まれています。

- [コントローラ パスワードの変更](#)
- [NSX コントローラ障害からのリカバリ](#)
- [VXLAN ポートの変更](#)
- [通信チャネルの健全性の確認](#)
- [カスタマ エクスペリエンス改善プログラム](#)
- [システム イベントと監査ログ](#)
- [システム設定の管理](#)
- [SNMP トラップの操作](#)
- [NSX のバックアップとリストア](#)
- [フロー モニタリング](#)
- [アクティビティ モニタリング](#)
- [トレースフロー](#)

コントローラ パスワードの変更

データ セキュリティを確保するために、NSX Controller のパスワードを変更できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、[インストール手順] をクリックします。
- 3 [管理] で、パスワードを変更するコントローラを選択します。
- 4 [アクション] をクリックし、[コントローラ クラスタのパスワードの変更] をクリックします。
- 5 新しいパスワードを入力し、[OK] をクリックします。

これで、コントローラ パスワードが変更されました。

NSX コントローラ障害からのリカバリ

NSX コントローラ障害が発生した場合でも、2 つのコントローラがまだ機能している可能性があります。クラスタの過半数が維持されているため、制御プレーンは機能し続けます。その場合でも、3 つのコントローラをすべて削除してからすべてのコントローラを追加し直すようにしてください。それによって、完全に機能する 3 ノード クラスタが維持されます。

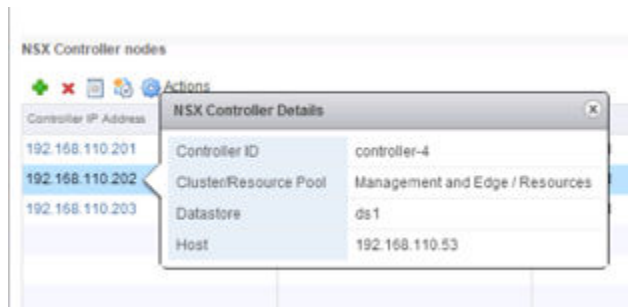
1 つ以上のコントローラで致命的なリカバリ不能エラーが発生した場合、または 1 つ以上のコントローラ仮想マシンがアクセス不能で修復できない状態になった場合は、コントローラ クラスタを削除することをお勧めします。

一部のコントローラが健全に動作していると思われる場合でも、すべてのコントローラを削除することをお勧めします。新しいコントローラを作成してから NSX Manager の [コントローラ状態の更新] メカニズムを使用して、2 つのコントローラの状態を同期させる方法をお勧めします。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] で、[インストール手順] > [管理] の順にクリックします。
- 3 [NSX コントローラ ノード] セクションで、各コントローラをクリックして、画面のスクリーンショットを作成するか、画面を印刷します。または、後で参照できるように設定情報をメモします。

次はその例です。



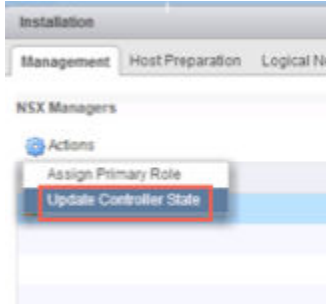
- 4 [NSX コントローラ ノード] セクションで、各コントローラを選択し、[ノードの削除 (x)] アイコンをクリックして、3 つのコントローラをすべて削除します。

システムにコントローラが存在しなくなると、ホストはいわゆる「ヘッドレス」モードで動作します。新しい仮想マシンまたは vMotion で移動された仮想マシンは、新しいコントローラがデプロイされ同期が完了するまで、ネットワークの問題が発生した状態になります。

- 5 [ノードの追加 (+)] アイコンをクリックして、3 台の新しい NSX コントローラ ノードをデプロイします。
- 6 [コントローラの追加] ダイアログ ボックスで、ノードを追加するデータセンターを選択し、コントローラを設定します。
 - a 適切なクラスタを選択します。
 - b クラスタおよびストレージでホストを選択します。
 - c 分散ポートグループを選択します。

- d ノードに割り当てられる IP アドレス プールを選択します。
- e [OK] をクリックして、インストールが完了するまで待ち、すべてのノードのステータスが [標準] になっていることを確認します。

7 [アクション] > [コントローラ状態の更新] の順にクリックして、コントローラの状態を再同期します。



コントローラ状態の更新によって、最新の VXLAN および分散論理ルーター設定（Cross-vCenter NSX 環境内のユニバーサル オブジェクトを含む）が、NSX Manager からコントローラ クラスタにプッシュされます。

VXLAN ポートの変更

VXLAN トラフィックに使用するポートを変更できます。

NSX 6.2.3 からは、デフォルトの VXLAN ポートは 4789 となり、標準ポートは IANA により割り当てられます。NSX 6.2.3 より前では、デフォルトの VXLAN UDP ポート番号は 8472 でした。

すべての新しい NSX インストール環境では、VXLAN に UDP ポート 4789 が使用されます。

NSX 6.2.3 にアップグレードする場合、アップグレード前の NSX で以前のデフォルト (8472) またはカスタム ポート番号 (8888 など) が使用されていた場合は、アップグレード後も、ユーザーが変更しない限り、引き続きそのポートが使用されます。

アップグレードされた NSX でハードウェア VTEP ゲートウェイ (ToR ゲートウェイ) が使用されている、またはその予定がある場合は、VXLAN ポート 4789 に切り替える必要があります。

Cross-vCenter NSX では、VXLAN ポートに 4789 を使用する必要はありませんが、同じ VXLAN ポートを使用するように Cross-vCenter NSX 環境にあるすべてのホストを設定する必要があります。ポート 4789 に切り替えると、Cross-vCenter NSX に追加される新しいすべての NSX インストール環境では、既存の NSX 環境と同じポートが使用されます。

VXLAN ポートの変更は 3 つのプロセスで行われ、処理中に VXLAN のトラフィックが中断されることはありません。Cross-vCenter NSX 環境では、この変更はすべての NSX Manager アプライアンスとすべてのホストに適用されます。

前提条件

- VXLAN に使用するポートがファイアウォールによってブロックされていないことを確認します。
- VXLAN ポートの変更時にホストの準備が実行されないことを確認します。

手順

- 1 [論理ネットワークの準備 (Logical Network Preparation)] タブをクリックし、次に [VXLAN 転送 (VXLAN Transport)] をクリックします。

- 2 [VXLAN ポート] パネルの [変更 (Change)] ボタンをクリックします。切り替え先のポートを入力します。4789 は、IANA が VXLAN 用に割り当てているポート番号です。

すべてのホストにポートの変更が適用されるまで、少し時間がかかります。

- 3 (オプション) ポート変更の進捗状況を確認するには、API 要求 `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` を使用します。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TW0</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

通信チャネルの健全性の確認

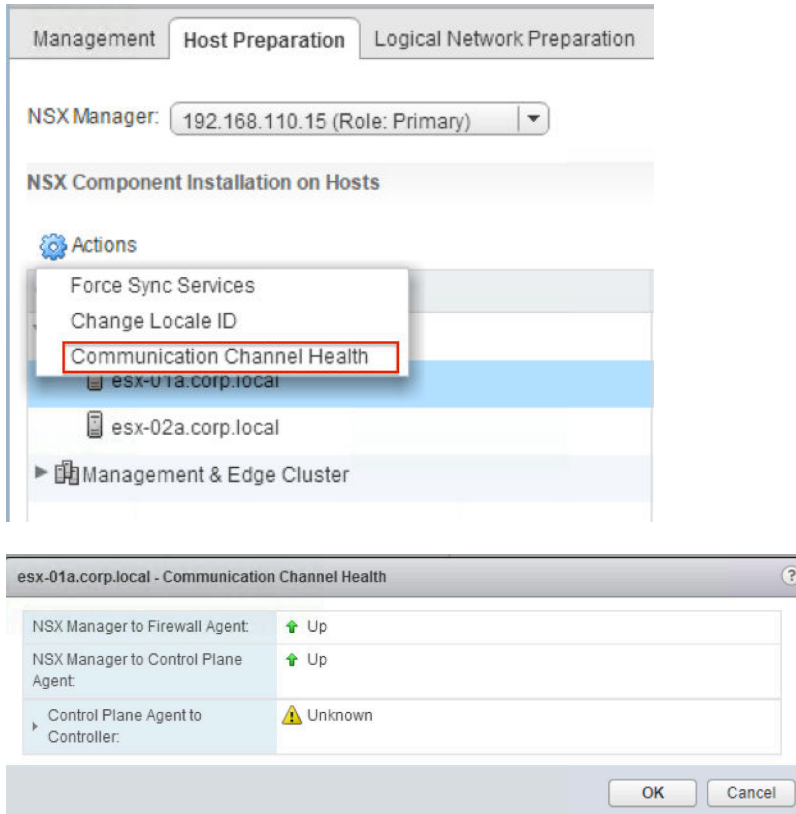
NSX は、NSX Manager とファイアウォール エージェント間、NSX Manager と制御プレーン エージェント間、および制御プレーン エージェントとコントローラ間の通信の状態を確認します。

手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [ホストの準備 (Host Preparation)] の順に移動します。

- 2 クラスタを選択するか、クラスタを展開してホストを選択します。[アクション (Actions)] (⚙️) をクリックし、[通信チャネルの健全性 (Communication Channel Health)] をクリックします。

通信チャネルの健全性情報が表示されます。



カスタマ エクスペリエンス改善プログラム

NSX は、VMware のカスタマ エクスペリエンス改善プログラム (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 (<http://www.vmware.com/trustvmware/ceip.html>) に記載されています。

NSX の CEIP への参加/参加中止、またはプログラム設定の編集を操作するには、「[カスタマ エクスペリエンス改善プログラムのオプションの編集](#)」を参照してください。

カスタマ エクスペリエンス改善プログラムのオプションの編集

NSX Manager をインストールまたはアップグレードするときに、CEIP への参加を選択できます。後で CEIP に参加したり、参加を中止することも可能です。また、情報の収集頻度や収集日も指定できます。

前提条件

- NSX Manager が接続されていて、vCenter Server と同期可能である。
- NSX Manager で DNS が設定されている。
- データのアップロードのために、NSX がパブリック ネットワークに接続されている。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] を選択します。
- 3 [ネットワークとセキュリティのインベントリ] の下で、[NSX Manager (NSX Managers)] を選択します。
- 4 変更する NSX Manager をダブルクリックします。
- 5 [サマリ (Summary)] タブをクリックします。
- 6 [カスタム エクスペリエンス改善プログラム] ダイアログ ボックスの [編集 (Edit)] をクリックします。
- 7 [VMware カスタム エクスペリエンス改善プログラムに参加する (Join the VMware Customer Experience Improvement Program)] オプションを選択または選択解除します。
- 8 (オプション) スケジュールを設定します。
- 9 [OK] をクリックします。

システム イベントと監査ログ

システム イベントは NSX の操作に関連したイベントです。すべての操作イベントの詳細を通知するために発行されます。イベントは基本操作（情報）に関連するものと、クリティカル エラー（重大）に関連するものがあります。

NSX チケット ロガー機能を使用して、行った変更をチケット ID で追跡できます。チケットによって追跡された操作の監査ログにはチケット ID が含まれます。

NSX ログについて

このセクションでは、Syslog サーバを設定し、各 NSX コンポーネントのテクニカル サポート ログを表示する方法を説明します。管理プレーン ログは NSX Manager から、データ プレーン ログは vCenter Server を通じて提供されます。そのため、Syslog サーバで環境全体のログが記録できるように、NSX コンポーネントと vCenter Server で同じ Syslog サーバを指定することが推奨されます。

vCenter Server で管理されるホストの Syslog の設定については、VMware vSphere ESXi および vCenter Server 5.5 のドキュメントを参照してください。

注: ログの収集や NSX 分散論理ルーター (DLR) 制御仮想マシンへのアクセスに使用する Syslog サーバまたはジャンプサーバは、分散論理ルータの論理インターフェイスに直接接続された論理スイッチ上に配置することはできません。

NSX Manager

Syslog サーバを指定するには、[「Syslog サーバの指定」](#)を参照してください。

テクニカル サポート ログをダウンロードするには、[「NSX のテクニカル サポート ログのダウンロード」](#)を参照してください。

NSX Edge

Syslog サーバを指定するには、「[リモート Syslog サーバの設定](#)」を参照してください。

テクニカル サポート ログをダウンロードするには、「[NSX Edge のテクニカル サポート ログのダウンロード](#)」を参照してください。

ファイアウォール

ファイアウォールが有効になっている各クラスタに対して、リモート Syslog サーバを構成する必要があります。リモート Syslog サーバは **Syslog.global.logHost** 属性で指定されます。ESXi および vCenter Server 5.5 のドキュメントを参照してください。

ホスト ログ ファイルのサンプル行は次のとおりです。

```
2013-10-02T05:41:12.670Z cpu11:1000046503)vsip_pkt: INET, match, PASS, Rule 0/3, Ruleset domain-c7, Rule ID 100, OUT, Len 60, SRC 10.24.106.96, DST 10.24.106.52, TCP SPORT 59692, DPORT 22 S
```

これは次の 3 つで構成されています。

表 23-1. ログ ファイル エントリのコンポーネント

	サンプル内の値
日付、時間、CPU、WorldID から構成される VMKernel の共通ログ部分	2013-10-02T05:41:12.670Z cpu11:1000046503)
識別子	vsip_pkt
ファイアウォール固有の部分	INET, match, PASS, Rule 0/3, Ruleset domain-c7, Rule ID 100, OUT, Len 60, SRC 10.24.106.96, DST 10.24.106.52, TCP SPORT 59692, DPORT 22 S

表 23-2. ログ ファイル エントリのファイアウォール固有の部分

エンティティ	利用可能な値
AF 値	INET、INET6
原因	利用可能な値 : match、bad-offset、fragment、short、normalize、memory、bad-timestamp、congestion、ip-option、proto-cksum、state-mismatch、state-insert、state-limit、src-limit、synproxy、spoofguard
アクション	PASS、DROP、SCRUB、NOSCRUB、NAT、NONAT、BINAT、NOBINAT、RDR、NORDR、SYNPROXY_DROP、PUNT、REDIRECT、COPY
ルール識別子	<Identifier>
ルールの値	ルールセット ID およびルールの位置 (内部詳細)
ルール セット識別子	<Identifier>
ルール セットの値	ルールセット名
ルール ID 識別子	<Identifier>
ルール ID	一致する ID
方向	ROUT、IN
長さの識別子	Len + 変数

表 23-2. ログ ファイル エントリのファイアウォール固有の部分 (続き)

エンティティ	利用可能な値
長さの値	パケットの長さ
ソース識別子	SRC
ソース IP アドレス	<IP address>
ターゲット識別子	<IP address>
プロトコル	TCP、UDP、PROTO
ソース ポート識別子	SPORT
ソース ポート	TDP および UDP のソース ポート番号
ソース ポート識別子	送信先ポート識別子
送信先ポート	TDP および UDP の送信先ポート番号
フラグ	TCP のフラグ

NSX チケット ロガーの使用

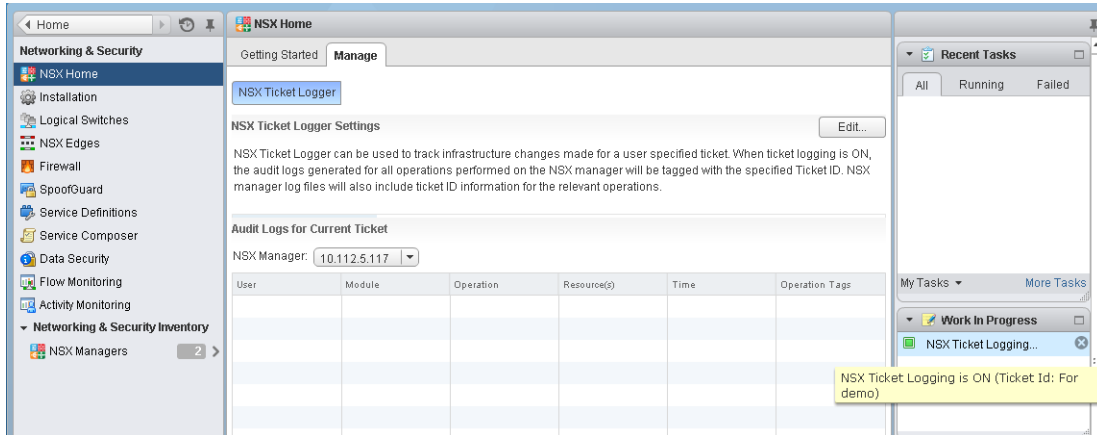
NSX チケット ロガーを使用すると、インフラストラクチャに行った変更を追跡できます。すべての操作に指定したチケット ID がタグ付けされ、これらの操作の監査ログにもチケット ID が記載されます。また、これらの操作のログ ファイルにも同じチケット ID がタグ付けされます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[管理 (Manage)] タブをクリックします。
- 3 [NSX チケット ロガー設定 (NSX Ticket Logger Settings)] の横にある [編集 (Edit)] をクリックします。
- 4 チケット ID を入力して、[オンにする (Turn On)] をクリックします。

[vSphere Web Client] ウィンドウの右側に [NSX チケット ログ] ペインが表示されます。監査ログの [操作タグ (Operation Tags)] 列に、現在のユーザー インターフェース セッションで実行した操作のチケット ID が記載されます。

図 23-1. [NSX チケット ロガー] ペイン



vSphere Web Client で複数の vCenter Server を管理している場合は、適用可能なすべての NSX Manager のログにチケット ID が使用されます。

次のステップ

チケット ログはセッションに基づきます。チケット ログがオンのままユーザーがログアウトした場合、またはセッションが失われた場合、デフォルトではユーザーがユーザー インターフェイスに再度ログインしたときにチケット ログがオフになります。チケットの操作が完了したら、手順 2 および 3 を繰り返して [オフにする (Turn Off)] をクリックし、ログをオフにします。

システム イベントのレポートの表示

vSphere Web Client では、NSX Manager が管理しているすべてのコンポーネントのシステム イベントを確認できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[監視] タブをクリックします。
- 4 [システム イベント] タブをクリックします。

列ヘッダーの矢印をクリックすると、イベントを並べ替えることができます。また、[フィルタ] テキスト ボックスを使用すると、イベントをフィルタリングできます。

NSX Manager 仮想アプライアンスのイベント

次のイベントは、NSX Manager 仮想アプライアンスに固有のイベントです。

表 23-3. NSX Manager 仮想アプライアンスのイベント

	パワーオフ	パワーオン	インターフェイスの切断	インターフェイスの接続中
ローカル CLI	<code>show log follow</code> コマンドを実行	<code>show log follow</code> コマンドを実行	<code>show log follow</code> コマンドを実行	<code>show log follow</code> コマンドを実行
GUI	NA	NA	NA	NA

表 23-4. NSX Manager 仮想アプライアンスのイベント

	CPU	メモリ	ストレージ
ローカル CLI	<code>show process monitor</code> コマンドを実行	<code>show system memory</code> コマンドを実行	<code>show filesystem</code> コマンドを実行
GUI	NA	NA	NA

Syslog の形式について

システム イベントのメッセージは、次の構造で syslog に記録されます。

```

syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter ':' (double colons)
Each name/value pair separated by delimiter ';' (double semi-colons)

```

システム イベントのフィールドおよびタイプには、次の情報が含まれます。

```

Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer (possible values: 10007 10016 10043 20019)
Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)
Message ::

```

監査ログの表示

[監査ログ] タブには、すべての NSX Manager ユーザーが実行したアクションが表示されます。NSX Manager では、最大 100 万件の監査ログが保持されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で、NSX サーバをクリックし、[監視] タブをクリックします。
- 4 [監査ログ] タブをクリックします。

- 5 監査ログに関する詳細情報がある場合は、そのログの [操作] 列のテキストがクリック可能になります。監査ログの詳細を表示するには、[操作] 列のテキストをクリックします。
- 6 [監査ログ変更の詳細] で、[変更された行] を選択すると、この監査ログ操作で値が変更されたプロパティのみが表示されます。

システム設定の管理

初期ログイン時に指定した、vCenter Server、DNS と NTP サーバ、および Lookup サーバを編集できます。NSX Manager では、VMware Infrastructure インベントリの詳細を取得するためには、vCenter Server および DNS や NTP などのサービスと通信する必要があります。

NSX Manager 仮想アプライアンスへのログイン

NSX Manager 仮想マシンのインストールと構成が済んだら、NSX Manager 仮想アプライアンスへログインし、インストール中に指定した設定を確認します。

手順

- 1 Web ブラウザ ウィンドウを開き、NSX Manager に割り当てた IP アドレスを入力します。たとえば、**https://192.168.110.42** と入力します。

NSX Manager ユーザー インターフェイスが、SSL を使用して Web ブラウザ ウィンドウで開きます。

- 2 セキュリティ証明書を受け入れます。

注: SSL 証明書を認証に使用できます。

NSX Manager のログイン画面が表示されます。

- 3 ユーザー名 **admin** とインストール時に設定したパスワードを使用して、NSX Manager 仮想アプライアンスにログインします。
- 4 [ログイン (Log In)] をクリックします。

NSX Manager の日時の編集

最初のログインのときに指定した NTP サーバは変更することができます。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [[Appliance Management] (Appliance Management)] で、[[Manage Appliance Settings] (Manage Appliance Settings)] をクリックします。
- 3 [時間設定 (Time Settings)] の横にある [編集 (Edit)] をクリックします。
- 4 適切に変更します。
- 5 [OK] をクリックします。
- 6 NSX Manager を再起動します。

Syslog サーバの指定

Syslog サーバを指定すると、NSX Manager は、その Syslog サーバにすべての監査ログとシステム イベントを送信します。

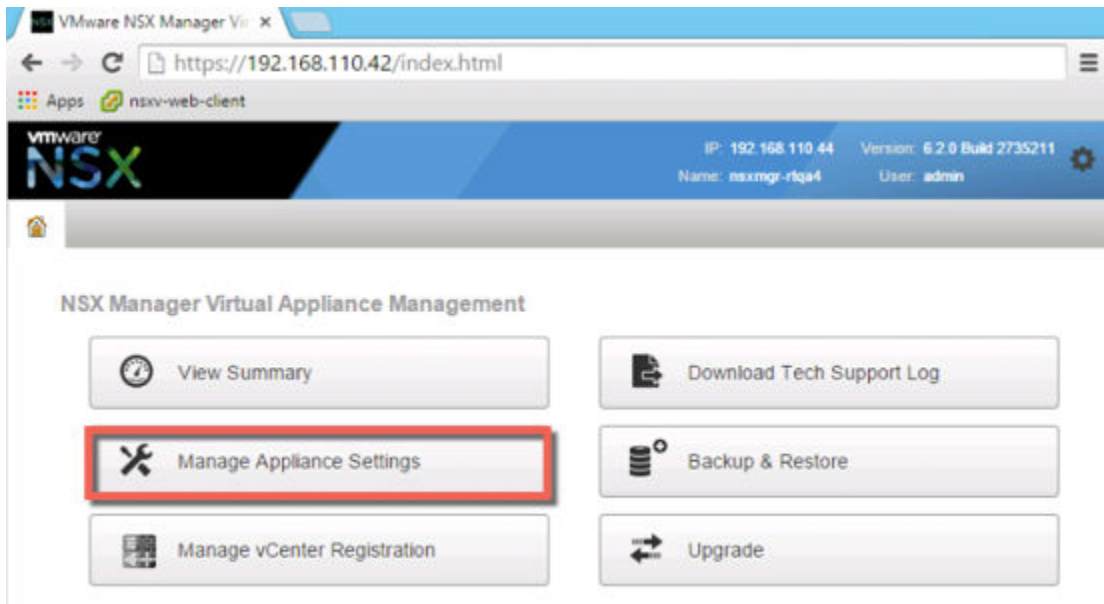
Syslog データは、トラブルシューティングや、インストールおよび構成中、ログに記録されたデータを確認する際に役立ちます。

NSX Edge は 2 台の Syslog サーバをサポートします。NSX Manager と NSX コントローラは 1 台の Syslog サーバをサポートします。

手順

- 1 Web ブラウザで、NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>> または <https://<nsx-manager-hostname>>) の順に移動します。
- 2 NSX Manager のインストール時に設定したパスワードを使用して admin としてログインします。
- 3 [アプライアンス設定の管理 (Manage Appliance Settings)] をクリックします。

次はその例です。

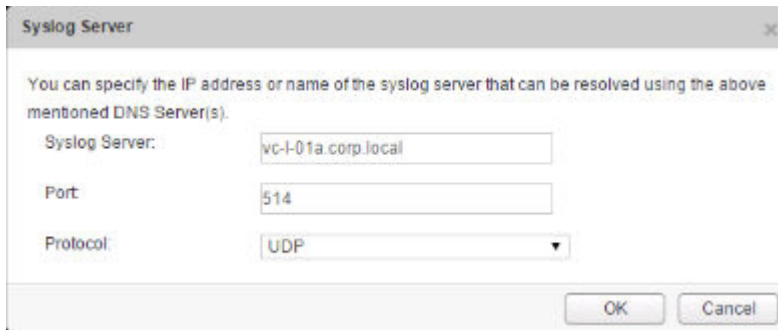


- 4 [設定] パネルから [全般 (General)] をクリックします。
- 5 [Syslog サーバ (Edit)] の横にある [編集 (Syslog Server)] をクリックします。

- 6 Syslog サーバの IP アドレス/ホスト名、ポート、およびプロトコルを入力します。

ポートを指定しないと、Syslog サーバの IP アドレス/ホスト名用のデフォルトの UDP ポートが使用されます。

次はその例です。



- 7 [OK] をクリックします。

vCenter Server のリモート ログが有効になり、ログがスタンドアロンの Syslog サーバに格納されます。

DNS サーバの編集

Manager のインストール時に指定した DNS サーバは変更することができます。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [[Appliance Management] (Appliance Management)]で、[[Manage Appliance Settings] (Manage Appliance Settings)] をクリックします。
- 3 [SETTINGS] パネルで、[[Network] (Network)] をクリックします。
- 4 [DNS サーバ (DNS Servers)] の横にある [編集 (Edit)] をクリックします。
- 5 適切に変更します。
- 6 [OK] をクリックします。

Lookup Service の詳細の編集

最初のログインのときに指定した Lookup Service の詳細は変更することができます。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [[Appliance Management] (Appliance Management)]で、[[Manage Appliance Settings] (Manage Appliance Settings)] をクリックします。
- 3 [設定] パネルで、[NSX 管理サービス (NSX Management Service)] をクリックします。
- 4 [Lookup Service] の横にある [編集 (Edit)] をクリックします。
- 5 適切に変更します。

- 6 [OK] をクリックします。

vCenter Server の編集

インストール時に NSX Manager を登録した vCenter Server を変更できます。この変更は、現在の vCenter Server の IP アドレスを変更する場合にのみ行ってください。


手順

- 1 vSphere Web Client にログインしている場合は、ログアウトします。
- 2 NSX Manager 仮想アプライアンスにログインします。
- 3 [[Appliance Management] (Appliance Management)] で、[[Manage Appliance Settings] (Manage Appliance Settings)] をクリックします。
- 4 [設定] パネルで、[NSX 管理サービス (NSX Management Service)] をクリックします。
- 5 [vCenter Server (Edit)] の横にある [編集 (vCenter Server)] をクリックします。
- 6 適切に変更します。
- 7 [OK] をクリックします。

NSX のテクニカル サポート ログのダウンロード

自分のデスクトップに NSX Manager のシステム ログと Web Manager のログをダウンロードできます。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [アプライアンス管理] で、[アプライアンス設定の管理] をクリックします。
- 3  をクリックし、[テクニカル サポート ログのダウンロード] をクリックします。
- 4 [ダウンロード] をクリックします。
- 5 ログの準備ができたなら、[保存] をクリックして、デスクトップにログをダウンロードします。
ログは圧縮され、ファイル拡張子 **.gz** が付加されます。

次のステップ

解凍ユーティリティを使用して、ファイルを保存したディレクトリの [すべてのファイル] を参照してログを開くことができます。

NSX Manager の SSL 証明書

NSX Manager では、NSX Manager の Web サービスの ID を認証して NSX Manager の Web サーバに送信される情報を暗号化するために、署名付き証明書が必要です。このプロセスでは、証明書署名要求 (CSR) を生成し、CA に署名してもらい、署名付き SSL 署名書を NSX Manager にインポートする必要があります。セキュリティのベストプラクティスとしては、プライベート キーと公開鍵を生成し、NSX Manager にプライベート キーが保存されるという証明書発行オプションを使用することを推奨します。

NSX Manager の証明書を取得するには、NSX Manager のビルトイン CSR ジェネレータを使用するか、OpenSSL などの別のツールを使用します。

NSX Manager のビルトイン証明書署名要求ジェネレータを使用して生成された CSR には、サブジェクトの代替名 (SAN) などの拡張属性を含めることができません。拡張属性を含める場合、別の証明書署名要求生成ツールを使用する必要があります。OpenSSL などの別のツールを使用して証明書署名要求を生成する場合、このプロセスは 1) 証明書署名要求を生成する、2) 署名してもらう、3) [「NSX Manager 証明書ファイルの PKCS#12 形式への変換」](#)のセクションに進む、となります。

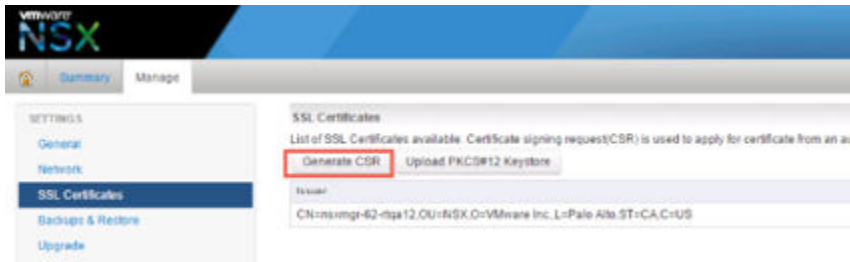
ビルトイン証明書署名要求 (CSR) ジェネレータの使用

NSX Manager 用の SSL 証明書を取得する方法の 1 つとして、ビルトイン証明書署名要求ジェネレータを使用する方法があります。

この方法には、証明書署名要求にサブジェクトの代替名 (SAN) などの拡張属性を含めることができないという制約があります。拡張属性を含める場合、別の証明書署名要求生成ツールを使用する必要があります。別の証明書署名要求生成ツールを使用している場合、この手順はスキップします。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [アプライアンス設定の管理 (Manage Appliance Settings)] をクリックします。
- 3 [設定] パネルで、[SSL 証明書 (SSL Certificates)] をクリックします。
- 4 [CSR の生成 (Generate CSR)] をクリックします。



- 5 次のフィールドに入力してフォームを完成させます。

オプション	アクション
[キーのサイズ (Key Size)]	選択したアルゴリズムで使用される鍵の長さを選択します。
[共通名 (Common Name)]	NSX Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。FQDN を入力することをお勧めします。
[組織単位 (Organization Unit)]	証明書を注文する会社・組織の部署名を記入します。
[組織名 (Organization Name)]	法人名を登記通りに記入します。
[市区町村名 (City Name)]	組織の所在地 (市) を記入します。
[都道府県名 (State Name)]	組織の所在地 (都道府県) を記入します。
[国コード (Country Code)]	アルファベット 2 文字の国識別コードを記入します。たとえば米国の場合、 US となります。

- 6 [OK] をクリックします。

7 証明書署名要求を CA に送信して署名してもらいます。

- a [CSR のダウンロード (Download CSR)] をクリックして、生成された要求をダウンロードします。
この方法を使用すると、プライベート キーが NSX Manager の外部には出ません。
- b この要求を CA に送信します。
- c PEM 形式の署名付き証明書、ルート CA、中間 CA 証明書を取得します。
- d CER/DER 形式の証明書を PEM に変換するには、次の OpenSSL コマンドを使用します。

```
openssl x509 -inform der -in Cert.cer -out 4-nsx_signed.pem
```

- e すべての証明書（サーバ、中間、ルート証明書）をテキスト ファイルで連結します。
- f NSX Manager ユーザー インターフェースで [インポート (Import)] をクリックし、すべての証明書が含まれるテキスト ファイルを参照します。
- g インポートに成功すると、サーバ証明書とすべての CA 証明書が [SSL 証明書] ページに表示されます。

次のステップ

署名付き SSL 証明書を NSX Manager にインポートします。

NSX Manager 証明書ファイルの PKCS#12 形式への変換

OpenSSL などの他のツールを使用して NSX Manager 証明書を取得した場合、証明書とプライベート キーが PKCS#12 形式であることを確認してください。NSX Manager 証明書とプライベート キーが PKCS#12 形式でない場合、変換しないと NSX Manager にインポートできません。

前提条件

OpenSSL がシステムにインストールされていることを確認します。OpenSSL は <http://www.openssl.org> からダウンロードできます。

手順

- ◆ 承認済み署名者から署名付き証明書を受け取った後で、OpenSSL を使用して PKCS#12 (.pfx または .p12) キーストア ファイルを証明書ファイルとプライベート キーから生成します。

次はその例です。

```
openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile CACert.crt
```

この例では、CACert.crt が認証局によって返されたルート証明書の名前です。

次のステップ

署名付き SSL 証明書を NSX Manager にインポートします。

SSL 証明書のインポート

以前から存在するか CA 署名の SSL 証明書をインポートして NSX Manager で使用することができます。

前提条件

証明書を NSX Manager にインストールする場合、PKCS#12 キーストア形式のみがサポートされ、1 つのプライベート キーと対応する署名付き証明書または証明書チェーンが含まれている必要があります。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [アプライアンス設定の管理 (Manage Appliance Settings)] をクリックします。
- 3 [設定] パネルで、[SSL 証明書 (SSL Certificates)] をクリックします。
- 4 [PKCS#12 キーストアのアップロード (Upload PKCS#12 Keystore)] をクリックします。



- 5 [ファイルの選択 (Choose File)] をクリックしてファイルを見つけます。
- 6 [インポート (Import)] をクリックします。
- 7 証明書を適用するには、NSX Manager アプライアンスを再起動します。

証明書が NSX Manager に保存されます。

SNMP トラップの操作

NSX Manager は、NSX Edge やハイパーバイザーなどから、「情報」、「警告」、および「重大」のシステム イベントを受信します。SNMP エージェントは、OID を含む SNMP トラップを SNMP レシーバに転送します。

SNMP トラップは SNMPv2c バージョンを使用する必要があります。SNMP レシーバがオブジェクト識別子 (OID) を含むトラップを処理できるように、トラップが管理情報ベース (MIB) に関連付けられている必要があります。

デフォルトでは、SNMP トラップのメカニズムは無効に設定されています。SNMP トラップを有効にすると、SNMP マネージャが膨大な数の通知を受け取ることがないように、重大な通知および重要度の高い通知のみが有効になります。IP アドレスまたはホスト名により、トラップのターゲットが指定されます。ホスト名がトラップのターゲット用として機能するには、Domain Name System (DNS) サーバに対してクエリを実行するようにデバイスが設定されている必要があります。

SNMP サービスを有効にすると、OID 1.3.6.1.6.3.1.1.5.1 を含む coldStart トラップが最初に送信されます。その後は、停止と開始が実行されるたびに、OID 1.3.6.1.6.3.1.1.5.2 を含む warmStart トラップが、設定されている SNMP レシーバに送信されます。

SNMP サービスが引き続き有効になっている場合は、OID 1.3.6.1.4.1.6876.4.190.0.401 を含むハートビート トラップの vmwHbHeartbeat が 5 分ごとに送信されます。サービスを無効にすると、OID 1.3.6.1.4.1.6876.90.1.2.1.0.1 を含む vmwNsxMSnmpDisabled トラップが送信されます。このプロセスは、vmwHbHeartbeat トラップがサービスを実行したり無効にしたりしないように抑制します。

SNMP レシーバの値を追加、変更、または削除すると、OID 1.3.6.1.6.3.1.1.5.2 を含む warmStart トラップ、および OID 1.3.6.1.4.1.6876.90.1.2.1.0.2 を含む vmwNsxMSnmpManagerConfigUpdated トラップが、SNMP レシーバの新規セットまたは更新されたセットに対して送信されます。

注: SNMP のポーリングはサポートされません。

SNMP の設定

SNMP 設定を有効にして、重要度が「重大」、「高」、または「情報」のトラップをターゲット レシーバが送信するようにします。

前提条件

- SNMP トラップのメカニズムについての知識を深めていただくことをお勧めします。[\[SNMP トラップの操作\]](#) を参照してください。
- SNMP レシーバがされていることを確認します。
- SNMP レシーバが OID を含むトラップを処理できるように、NSX Manager の MIB モジュールをダウンロードしてインストールします。<http://kb.vmware.com/kb/1013445> を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] - [ネットワークとセキュリティのインベントリ (Networking & Security Inventory)] - [NSX Manager (NSX Managers)] の順に選択します。
- 3 NSX Manager の IP アドレスを選択します。
- 4 [管理 (Manage)] - [システム イベント (System Events)] タブの順に選択します。
- 5 [編集 (Edit)] をクリックして、SNMP を設定します。

オプション	説明
サービス	SNMP トラップを送信します。 デフォルトでは、このオプションは無効です。
グループ通知	システム イベント用グループの事前定義セットで、発生したイベントをグループ化します。 このオプションはデフォルトで有効です。 たとえば、システム イベントが特定のグループに属する場合、これらのグループ化したイベントについてはトラップが保留になります。5 分ごとに、NSX Manager から受信したシステム イベント数の詳細を含むトラップが送信されます。送信されるトラップ数を減らすことで、SNMP レシーバのリソースを節約することができます。
レシーバ	トラップの宛先のレシーバを最大 4 つ設定できます。 SNMP レシーバを追加するときには、次のセクションを設定する必要があります。 [レシーバ アドレス]: レシーバ ホストの IP アドレスまたは完全修飾ドメイン名です。 [レシーバ ポート]: SNMP レシーバのデフォルトの UDP ポートは 162 です。 [コミュニティ スtring]: 通知トラップの一部として送信される情報です。 [有効]: このレシーバがトラップを送信することを示します。

- 6 [OK] をクリックします。

SNMP サービスが有効になり、トラップがレシーバに送信されます。

次のステップ

SNMP 設定が機能するかどうかを確認します。[「SNMP トラップ設定の確認」](#)を参照してください。

SNMP トラップ設定の確認

既存のシステムトラップを編集する前に、新たに有効にした SNMP サービスや更新した SNMP が適切に動作しているかどうかを確認する必要があります。

前提条件

SNMP が設定済みであることを確認します。[「SNMP の設定」](#)を参照してください。

手順

- 1 SNMP の設定とレシーバの接続を確認します。
 - a [管理 (Manage)] - [システム イベント (System Events)] タブの順に選択します。
 - b [編集 (Edit)] をクリックして、SNMP を設定します。
ダイアログ ボックスの設定は変更しないでください。
 - c [OK] をクリックします。
OID 1.3.6.1.6.3.1.1.5.2 を含む warmStart トラップが、すべての SNMP レシーバに送信されます。
- 2 SNMP の設定またはレシーバの問題のデバッグを実行します。
 - a SNMP レシーバがトラップを受信しない場合は、設定したポートで SNMP レシーバが実行されていることを確認します。
 - b SNMP 設定セクションで、レシーバの情報が正しいことを確認します。
 - c SNMP レシーバが OID 1.3.6.1.4.1.6876.4.190.0.401 を含む vmwHbHeartbeat トラップを 5 分おきに受信しなくなった場合は、NSX Manager アプライアンスまたは NSX Manager SNMP エージェントが動作していることを確認します。
 - d ハートビートトラップが停止した場合は、SNMP サービスが無効になっていないかを確認し、NSX Manager と SNMP レシーバの間のネットワーク接続が動作しているかどうかをテストします。

システムトラップの編集

システムトラップを編集してトラップの重要度や有効/無効設定を変更し、これによってトラップがレシーバに送信されるか抑制されるかを指定できます。

モジュール、SNMP OID、または SNMP のトラップが有効になっている列で、値が -- と表示されている場合は、トラップの OID がこれらのイベントに割り当てられていないことを意味します。したがって、これらのイベントのトラップは送信されません。





システムトラップには、システムイベントのさまざまな側面について示す複数の列が含まれます。

オプション	説明
イベント コード	イベントに関連付けられている固定のイベント コードです。
説明	イベントの概要説明です。
モジュール	イベントをトリガーするサブコンポーネント。
重要度	イベントのレベルは、「情報」、「低」、「中」、「メジャー」、「重大」、「高」のいずれかとなります。 デフォルトでは、SNMP サービスが有効になっているとき、即座に対応する必要があるトラップを強調するため、重要度が「重大」と「高」のイベントについてのみトラップが送信されます。
SNMP OID	個別の OID を示します。この OID は、システム イベントが発せられた場合に送信されます。 グループ通知はデフォルトで有効になっています。グループ通知が有効な場合、このグループの下位のイベントまたはトラップには、イベントまたはトラップが属するグループの OID が表示されます。 たとえば、構成グループの下に分類されたグループ通知の OID は、1.3.6.1.4.1.6876.90.1.2.0.1.0.1 となります。
有効な SNMP トラップ	このイベントについてのトラップの送信が有効か無効かを示します アイコンを使用して、イベントまたはトラップの有効/無効設定を個別に切り替えることができます。グループ通知が有効になっているとき、トラップの有効/無効設定を切り替えることはできません。
フィルタ	キーワードを検索して、システム トラップをフィルタリングします。

前提条件

SNMP 設定を使用できることを確認します。[「SNMP の設定」](#)を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] - [ネットワークとセキュリティのインベントリ (Networking & Security Inventory)] - [NSX Manager (NSX Managers)] の順に選択します。
- 3 NSX Manager の IP アドレスを選択します。
- 4 [管理 (Manage)] - [システム イベント (System Events)] タブの順に選択します。
- 5 [システム トラップ] セクションの下で、システム イベントを選択します。
- 6 [編集 (Edit)] () アイコンをクリックします。
グループ通知が有効になっているときは、トラップの有効/無効設定を編集できません。グループに属さないトラップの有効/無効設定は変更できます。
- 7 システム イベントの重要度を、ドロップダウン メニューから選択して変更します。
- 8 重要度を「情報」から「重大」へ変更する場合は、[SNMP トラップとして有効にする (Enable as SNMP Trap)] チェックボックスを選択します。
- 9 [OK] をクリックします。
- 10 (オプション) システム トラップの送信を有効または無効に指定するには、ヘッダーの [有効 (Enable)] () アイコンまたは [無効 (Disable)] () アイコンをクリックします。
- 11 (オプション) 1 つ以上のイベント行をクリップボードにコピーするには、[コピー (Copy)] () アイコンをクリックします。

NSX のバックアップとリストア

すべての NSX コンポーネントを正しくバックアップすることは、障害が発生した場合にシステムを正常動作の状態にリストアするために重要です。

NSX Manager のバックアップには、コントローラ、論理スイッチ、ルーティング エンティティ、セキュリティ、ファイアウォール ルール、および NSX Manager ユーザー インターフェイスや API でユーザーが設定したその他のすべてを含む、あらゆる NSX 設定が含まれます。vCenter データベースと仮想スイッチのような関連要素は、別々にバックアップする必要があります。

少なくとも、定期的に NSX Manager と vCenter Server のバックアップを作成することをお勧めします。バックアップの頻度とスケジュールは、ビジネス上のニーズと操作手順によって異なる場合があります。設定の変更を何度も行う場合は、頻繁に NSX バックアップを作成することをお勧めします。

NSX Manager のバックアップは、オンデマンドで作成することも、時間単位、日単位、または週単位で作成することもできます。

次の場合にバックアップを作成することをお勧めします。

- NSX または vCenter Server をアップグレードする前。
- NSX または vCenter Server をアップグレードした後。
- NSX Controller、論理スイッチ、分散論理ルーター、Edge Services Gateway、セキュリティおよびファイアウォール ポリシーを作成した後など、0 日目に NSX コンポーネントをデプロイして初期設定を行った後。
- インフラストラクチャまたはトポロジを変更した後。
- 2 日目に大きな変更を行った後。

任意の時点でシステム全体をロールバックできるように、NSX コンポーネント（NSX Manager など）のバックアップを vCenter Server、クラウド管理システム、操作ツールなどの他の連携コンポーネントのバックアップと同時に行うことをお勧めします。

NSX Manager データのバックアップ

NSX Manager データは、オンデマンド バックアップまたはスケジュール設定したバックアップを実行してバックアップできます。

NSX Manager のバックアップおよびリストアは、NSX Manager 仮想アプライアンス Web インターフェイスから、または NSX Manager API を使用して設定できます。バックアップは時間単位、日単位、週単位でスケジュール設定できます。

バックアップ ファイルは、NSX Manager が FTP または SFTP でアクセスできるリモートの格納場所に保存されます。NSX Manager データには、構成テーブル、イベント テーブル、監査ログ テーブルが含まれます。構成テーブルは、すべてのバックアップに含まれます。

リストアは、バックアップ バージョンと同じ NSX Manager バージョンでのみサポートされます。そのため、NSX アップグレードを実行する前と後に新規のバックアップ ファイルを作成し、古いバージョンと新しいバージョンのそれぞれにバックアップを作成することが重要です。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [アプライアンス管理] で、[バックアップとリストア] をクリックします。
- 3 バックアップ先を指定するには、[FTP サーバ設定] の横の [変更] をクリックします。
 - a バックアップシステムの IP アドレスまたはホスト名を入力します。
 - b 送信先でサポートされるプロトコルに応じて、[転送プロトコル] ドロップダウン メニューから [SFTP] または [FTP] を選択します。
 - c 必要に応じてデフォルトのポートを編集します。
 - d バックアップシステムにログインするために必要なユーザー名とパスワードを入力します。
 - e [バックアップディレクトリ] フィールドに、バックアップの保存先の絶対パスを入力します。

絶対パスを確認するには、FTP サーバにログインし、使用するディレクトリに移動して、現在のディレクトリのフルパスを表示するコマンド (**pwd**) を実行します。次はその例です。

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f [ファイル名のプリフィックス] に文字列を入力します。

このテキストがそれぞれのバックアップ ファイル名の前に追加され、バックアップシステムで容易に認識されるようになります。たとえば **ppdb** と入力すると、バックアップ ファイル名は **ppdbHH_MM_SS_DayDDMonYYYY** となります。

- g パス フレーズを入力してバックアップを保護します。

このパス フレーズはバックアップをリストアするために必要となります。

- h [OK] をクリックします。

次はその例です。

- 4 オンデマンド バックアップの場合、[バックアップ] をクリックします。

新しいファイルが [バックアップ履歴] に追加されます。

- 5 スケジュール設定されたバックアップの場合、スケジュールの横にある [変更] をクリックします。

- a [バックアップ頻度] ドロップダウン メニューで、[時間単位]、[日単位]、または [週単位] を選択します。選択したバックアップ頻度によっては、[曜日]、[時間]、および [分] ドロップダウン メニューが無効になります。たとえば、[日単位] を選択すると、[曜日] ドロップダウン メニューは日次バックアップには適用されないため、無効になります。
 - b 週単位バックアップの場合、データをバックアップする曜日を選択します。
 - c 週単位バックアップまたは日単位バックアップの場合、バックアップを開始する時間を選択します。
 - d 開始する分数を選択して、[スケジュール設定] をクリックします。
- 6 ログおよびフロー データをバックアップから除外するには、[除外] の横の [変更] をクリックします。
- a バックアップから除外する項目を選択します。
 - b [OK] をクリックします。
- 7 FTP サーバの IP アドレス/ホスト名、認証情報、ディレクトリの詳細、パス フレーズを保存します。この情報は、バックアップをリストアするために必要です。

NSX Manager バックアップのリストア

NSX Manager をリストアすると、バックアップ ファイルが NSX Manager アプライアンスでロードされます。バックアップ ファイルは、NSX Manager がアクセスできるリモート FTP または SFTP の場所に保存する必要があります。NSX Manager データには、構成テーブル、イベント テーブル、監査ログ テーブルが含まれます。

重要: バックアップ ファイルをリストアする前に、現在のデータをバックアップしてください。

前提条件

NSX Manager データをリストアする前に、NSX Manager アプライアンスを再インストールすることをお勧めします。既存の NSX Manager アプライアンスでリストア操作を実行しても機能する可能性はありますが、公式にはサポートされていません。既存の NSX Manager で障害が発生した場合は、新規の NSX Manager アプライアンスをデプロイすることが想定されています。

ベスト プラクティスとしては、新規でデプロイする NSX Manager アプライアンスの IP 情報およびバックアップ場所の情報の指定に使用できるように、既存の NSX Manager アプライアンスの現在の設定のスクリーンショットを取るか、メモを取ります。

手順

1 既存の NSX Manager アプライアンスのすべての設定のスクリーンショットを取るか、メモを取ります。

2 NSX Manager アプライアンスを新規にデプロイします。

バージョンはバックアップした NSX Manager アプライアンスと同じである必要があります。

3 新規の NSX Manager アプライアンスにログインします。

4 [アプライアンス管理] で、[バックアップとリストア (Backups & Restore)] をクリックします。

5 [FTP サーバ設定] で、[変更 (Change)] をクリックして設定を追加します。

バックアップ先画面の [ホスト IP アドレス (Host IP Address)]、[ユーザー名 (User Name)]、[パスワード (Password)]、[バックアップディレクトリ (Backup Directory)]、[ファイル名の接頭辞 (Filename Prefix)]、[パスフレーズ (Pass Phrase)] の各フィールドで、リストアするバックアップの場所を識別する必要があります。

6 [バックアップ履歴] セクションで、リストアするバックアップのチェック ボックスを選択し、[リストア (Restore)] をクリックします。

NSX Edge のバックアップ

すべての NSX Edge 設定（分散論理ルーターおよび Edge Services Gateway）は、NSX Manager データ バックアップの一環としてバックアップされます。

NSX Manager の設定が変更されていない場合、NSX Edge を再デプロイする（vSphere Web Client で [NSX Edge の再デプロイ] アイコンをクリックする）ことで、アクセス不能または障害が発生した Edge Appliance 仮想マシンを再作成できます。

NSX Edge のバックアップを個別に作成することは、サポートされていません。

vSphere Distributed Switch のバックアップ

vSphere Distributed Switch (VDS) および分散ポート グループの設定をファイルにエクスポートできます。

有効なネットワーク設定がファイルに保存され、ほかのデプロイ環境で利用できるようになります。

この機能は、vSphere Web Client 5.1 以降でのみ使用できます。VDS 設定およびポートグループ設定は、インポートの一環としてインポートされます。

ベスト プラクティスとして、VXLAN のクラスタを準備する前に、VDS 設定をエクスポートします。詳細な手順については、<http://kb.vmware.com/kb/2034602> を参照してください。

vCenter Server のバックアップ

NSX デプロイを保護するには、vCenter Server データベースをバックアップして仮想マシンのスナップショットを作成することが重要です。

vCenter Server のバックアップとリストアの手順、およびベスト プラクティスについては、お使いのバージョンの vCenter Server ドキュメントを参照してください。

仮想マシンのスナップショットについては、<http://kb.vmware.com/kb/1015180> を参照してください。

vCenter Server 5.5 に役立つリンク：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

vCenter Server 6.0 に役立つリンク：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

フロー モニタリング

フロー モニタリングは、保護対象の仮想マシンへのトラフィックおよび保護対象の仮想マシンからのトラフィックの詳細情報を提供する、トラフィック解析ツールです。フロー モニタリングが有効な場合、その出力では、どのマシンが、どのアプリケーションを使用してデータを交換しているかが定義されます。このデータにはセッション数やセッションごとのパケット転送数などが含まれます。セッションの詳細には、使用されている転送元、転送先、アプリケーション、ポートなどの情報が含まれます。セッションの詳細は、ファイアウォールの作成や、ルールの許可またはブロックで使用できます。

TCP、UDP、ARP、ICMP など、さまざまなプロトコル タイプのフロー データを表示できます。選択した vNIC（接続元または接続先）との TCP 接続および UDP 接続をライブで監視できます。また、フィルタを指定してフローを除外することもできます。

このように、フロー モニタリングは、不正なサービスを検出したり、送信セッションを調査したりするためのフォレンジック ツールとして使用できます。

フロー モニタリングデータの表示

指定した期間内の仮想マシンのトラフィック セッションを表示できます。デフォルトでは過去 24 時間のデータが表示されます。最小時間範囲は 1 時間、最大時間は 2 週間です。

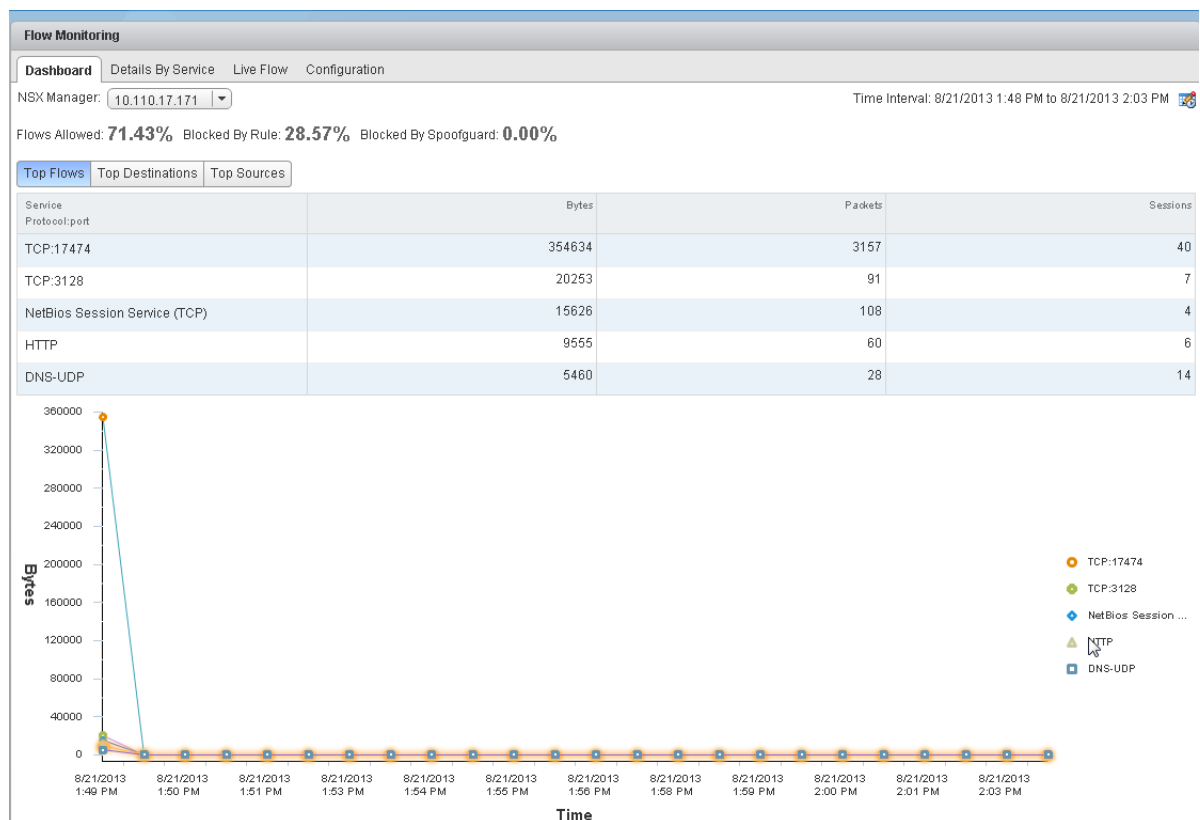
前提条件

フロー モニタリング データは、ネットワーク仮想化コンポーネントがインストールされ、ファイアウォールが有効になっているクラスタの仮想マシンでのみ利用できます。『NSX インストール ガイド』を参照してください。

手順

- 1 vSphere Web Client にログインします。
- 2 左側のナビゲーション ペインで [Networking and Security (Networking & Security)] を選択し、[フロー モニタリング (Flow Monitoring)] を選択します。
- 3 [ダッシュボード (Dashboard)] タブを表示していることを確認します。
- 4 [フロー モニタリング (Flow Monitoring)] をクリックします。

このページのロードに数秒かかることがあります。ページの上部に、許可されたトラフィックの割合、ファイアウォール ルールでブロックされたトラフィック、SpoofGuard でブロックされたトラフィックが表示されます。環境内の各サービスのデータ フローが複数の折れ線グラフで表示されます。凡例の 1 つのサービスをポイントすると、そのサービスの各点が強調表示されます。



トラフィック統計は次の 3 つのタブに表示されます。

- [トップ フロー (Top Flows)] には、(セッション/パケットではなく) 合計バイト数の値に基づいて、指定された時間におけるサービスあたりの受信トラフィックと送信トラフィックの合計が表示されます。上位 5 つのサービスが表示されます。トップ フローの計算時には、ブロックされたフローは考慮されません。
- [トップ ターゲット (Top Destinations)] には、指定された時間におけるターゲットあたりの受信トラフィックが表示されます。上位 5 つのターゲットが表示されます。
- [トップ ソース (Top Sources)] には、指定された時間におけるソースあたりの送信トラフィックが表示されます。上位 5 つのソースが表示されます。

5 [サービス別の詳細 (Details by Service)] タブをクリックします。

選択したサービスのすべてのトラフィックの詳細が表示されます。[許可されたフロー (Allowed Flows)] タブには許可されたトラフィック セッションが表示され、[ブロックされたフロー (Blocked Flows)] タブにはブロックされたトラフィックが表示されます。

サービス名で検索できます。

Flow Monitoring

Dashboard **Details By Service** Live Flow Configuration

NSX Manager: 10.110.17.171 Time Interval: 8/23/2013 6:10 AM to 8/23/2013 6:25 AM

Allowed Flows Blocked Flows

Type	Service	Bytes	Sessions
UDP	DHCP-Server	4954	6
TCP	TCP:17474	2224	1
OTHER	IPv6-ICMP:0	1872	18
OTHER	ARP	1196	26
OTHER	0xffff	162	2
UDP	NTP Time Server	152	1

6 items

Rule Id	Time Stamp	Source	Source User(s)	Destination	Packets	Actions
1021	8/23/2013 6:15 AM	10.112.243.233	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:15 AM	DB_server	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:15 AM	win32rdclone	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:14 AM	10.112.243.214	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:12 AM	win32rdclone	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:11 AM	10.112.243.229	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:13 AM	win32rdclone	Unknown	10.113.60.150	12	Add Rule Edit Rule

6 そのトラフィック フローを許可またはブロックしたルールを表示するには、テーブルで項目をクリックします。


7 ルール詳細を表示するルールの [ルール ID (Rule Id)] をクリックします。

フロー モニタリング チャートの日付範囲の変更

フロー モニタリング データの日付範囲は、[ダッシュボード] タブと [詳細] タブの両方で変更できます。

手順

1 vSphere Web Client にログインします。

- 2 左側のナビゲーション ペインで [Networking and Security (Networking & Security)] を選択し、[フロー モニタリング (Flow Monitoring)] を選択します。
- 3 [時間間隔 (Time interval)] の横にある  をクリックします。
- 4 期間を選択するか、新しい開始日および終了日を入力します。
トラフィック フロー データを表示できる最長期間は、過去 2 週間です。
- 5 [OK] をクリックします。

フロー モニタリング レポートからのファイアウォール ルールの追加または編集

トラフィック データにドリル ダウンすると、リソースの使用について評価し、セッション情報を分散ファイアウォールに送信して、任意のレベルで新しい許可/拒否ルールを作成できます。

手順

- 1 vSphere Web Client にログインします。
- 2 左側のナビゲーション ペインで [Networking and Security (Networking & Security)] を選択し、[フロー モニタリング (Flow Monitoring)] を選択します。
- 3 [サービス別の詳細 (Details by Service)] タブをクリックします。
- 4 トラフィック フローを表示するサービスをクリックします。
選択したタブに応じて、このサービスのトラフィックを許可または拒否したルールが表示されます。
- 5 ルールの詳細を表示するには、ルール ID をクリックします。
- 6 次のいずれかを実行します。
 - ルールを編集するには：
 - 1 [アクション (Actions)] 列の [ルールの編集 (Edit Rule)] をクリックします。
 - 2 ルールの名前、アクション、またはコメントを変更します。
 - 3 [OK] をクリックします。
 - ルールを追加するには：
 - 1 [アクション (Actions)] 列の [ルールの追加 (Add Rule)] をクリックします。
 - 2 フォームに入力し、ルールを追加します。ファイアウォール ルールのフォームの記入については、[「ファイアウォール ルールの追加」](#)を参照してください。
 - 3 [OK] をクリックします。

ルールは、ファイアウォール ルール セクションの最上部に追加されます。

ライブ フローの表示

選択した vNIC（接続先または接続元）との UDP 接続および TCP 接続を表示できます。2 台の仮想マシン間のトラフィックを表示するために、1 台のコンピュータ上にある一方の仮想マシンと、2 台目のコンピュータ上にあるもう一方の仮想マシンのライブ トラフィックを表示できます。ホストごとに最大 2 つの vNIC と、インフラストラクチャごとに最大 5 つの vNIC のトラフィックを表示できます。

ライブフローを表示すると、NSX Manager や対応する仮想マシンのパフォーマンスに影響することがあります。

手順

- 1 vSphere Web Client にログインします。
- 2 左側のナビゲーション ペインで [Networking and Security (Networking & Security)] を選択し、[フロー モニタリング (Flow Monitoring)] を選択します。
- 3 [ライブ フロー (Live Flow)] タブをクリックします。
- 4 [参照 (Browse)] をクリックして、vNIC を選択します。
- 5 [開始 (Start)] をクリックしてライブ フローの表示を開始します。

このページは 5 秒ごとに更新されます。[更新速度 (Refresh Rate)] ドロップダウンから別の頻度を選択することも可能です。

Flow Monitoring

Dashboard


Details By Service

Live Flow

Configuration

NSX Manager: 10.24.130.213

Live Flow will be shown for the selected vNic. Please select a vNic and press start to see the live flows

vNic:  app-sv-t2 - Network adapter 1 [Browse](#)

Start

Stop

Refresh Rate: 5 Seconds

New active flows

Flows with state change

Terminated flows

RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	state	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets
1026	OUT	Active	TCP	172.16.40.121	49099	172.16.40.131	3306	FINWAIT2	747	11	2077	9
1026	OUT	Inactive	TCP	172.16.40.121	49098	172.16.40.131	3306	FINWAIT2	747	11	2077	9

- 6 デバッグやトラブルシューティングが終了したら [停止 (Stop)] をクリックして、NSX Manager や選択した仮想マシンのパフォーマンスに影響が及ばないようにします。

フロー モニタリング データ収集の設定

収集する フロー モニタリング データを確認してフィルタリングした後で、データ収集を設定できます。除外基準を指定すると、表示されるデータをフィルタできます。たとえば、重複するフローが表示されないようにプロキシ サーバを除外することができます。また、インベントリの仮想マシンで Nessus スキャンを実行している場合に、スキャン フローを収集から除外しないことができます。特定のフローの情報がファイアウォールからフロー コレクタに直接エクスポートされるように、IPFix を設定できます。フロー モニタリング のグラフには IPFix フローは含まれません。IPFix フローは、IPFix コレクタのインターフェイスに表示されます。

手順

- 1 vSphere Web Client にログインします。
- 2 左側のナビゲーション ペインで [Networking and Security (Networking & Security)] を選択し、[フロー モニタリング (Flow Monitoring)] を選択します。
- 3 [設定 (Configuration)] タブを選択します。
- 4 [グローバル フロー収集構成ステータス (Global Flow Collection Status)] が [有効 (Enabled)] になっていることを確認します。

[除外設定 (Exclusion Settings)] で指定されているオブジェクトを除いて、インベントリ全体ですべてのファイアウォール関連フローが収集されます。

5 フィルタリング基準を指定するには、[フロー除外 (Flow Exclusion)] をクリックして、次の手順を実行します。

a 除外するフローに対応するタブをクリックします。

Flow Monitoring

Dashboard Details By Service Live Flow **Configuration**

NSX Manager: 10.110.8.93

Global Flow Collection Status: **Enabled** **Disable**

Flow Exclusion IPFix

Exclusion Settings
System will not collect flows that match the specified condition

Filter	
Collect Blocked Flows	Yes
Collect Layer2 Flows	Yes
Source	
Destination	system-generated-broadcast-macset, 224.0.0.0/24, 255.255.255.255
Destination ports	138, 137
Service	

System is configured to collect all firewall related flows except those that match the conditions specified below

Detail Collection Policy: (Click Save to commit changes to settings)

Collect Blocked Flows:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Collect Layer2 Flows:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Save

b 必要な情報を指定します。

次の項目を選択した場合は	次の情報を指定
ブロックされたフローの収集	[いいえ] を選択するとブロックされたフローが除外されます。
レイヤー 2 フローの収集	[いいえ] を選択するとレイヤー 2 のフローが除外されます。
ソース	指定したソースのフローが収集されません。 1 [追加 (Add)] アイコンをクリックします。 2 [ビュー] で、適切なコンテナを選択します。 3 除外するオブジェクトを選択します。
ターゲット	指定したターゲットのフローが収集されません。 1 [追加 (Add)] アイコンをクリックします。 2 [ビュー] で、適切なコンテナを選択します。 3 除外するオブジェクトを選択します。
ターゲット ポート	指定したポートへのフローを除外します。 除外するポート番号を入力します。
サービス	指定したサービスおよびサービス グループへのフローを除外します。 1 [追加 (Add)] アイコンをクリックします。 2 適切なサービスやサービス グループを選択します。

c [保存 (Save)] をクリックします。

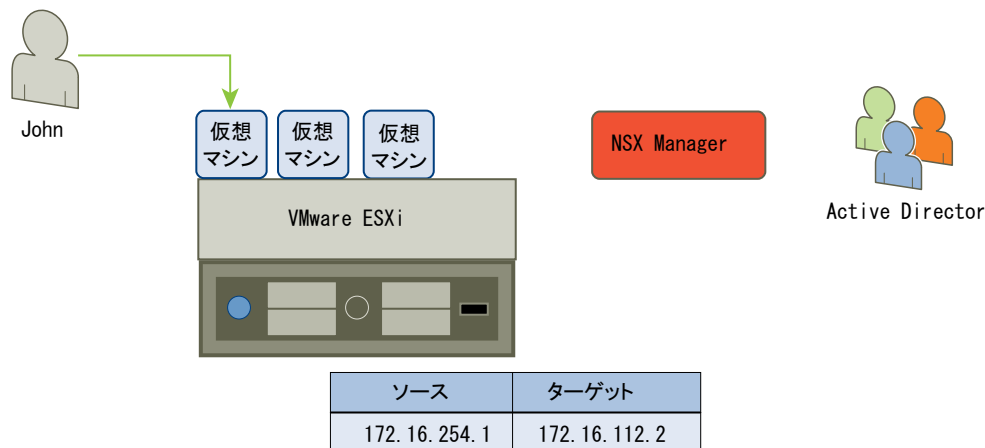
- 6 フロー収集をするには、[IPFix] をクリックして、次の手順を実行します。
- IPFix 構成の横にある [編集 (Edit)] をクリックして、[IPFix 構成の有効化 (Enable IPFix Configuration)] をクリックします。
 - [観測 DomainID (Observation DomainID)] に、フロー コレクタに対するファイアウォール エクスポートを特定する 32 ビット ID を入力します。
 - [アクティブなフロー エクスポートのタイムアウト (Active Flow Export Timeout)] に、アクティブなフローがフロー コレクタにエクスポートされるまでの時間 (分) を入力します。デフォルト値は 5 です。たとえば、フローが 30 分間アクティブであり、エクスポートのタイムアウトが 5 分の場合、フローはその有効期間中に 7 回エクスポートされます。つまり、作成と削除時に各 1 回エクスポートされ、アクティブ期間中に 5 回エクスポートされます。
 - [コレクタ IP アドレス (Collector IPs)] で、[追加] (+) アイコンをクリックして、フロー コレクタの IP アドレスと UDP ポートを入力します。
 - [OK] をクリックします。

アクティビティ モニタリング

アクティビティ モニタリングを使用すると、vCenter Server で管理している Windows デスクトップ仮想マシンで使用中のアプリケーションを可視化できます。この可視化により、組織におけるセキュリティ ポリシーを適切に実施できます。

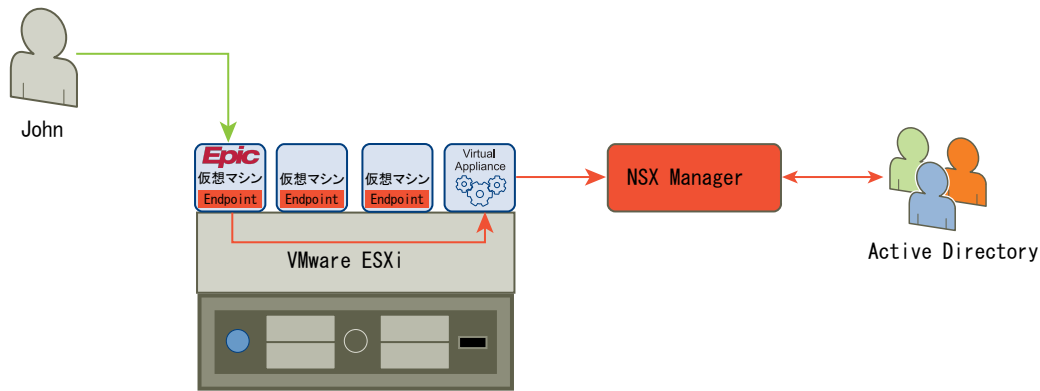
セキュリティ ポリシーによって、誰がどのアプリケーションにアクセスできるかが規定されていることがあります。クラウド管理者は、アクティビティ モニタリングのレポートを生成して、設定した IP アドレス ベースのファイアウォール ルールが意図したとおり機能しているかどうかを確認できます。アクティビティ モニタリングでは、ユーザーおよびアプリケーション レベルの詳細を示すことで、高レベルのセキュリティ ポリシーを低レベルの IP アドレスおよびネットワークに実装します。

図 23-2. 現在の仮想環境



アクティビティ モニタリング のデータ収集を有効にすると、レポートを実行して入力側トラフィック（ユーザーがアクセスする仮想マシンなど）や出力側トラフィック（リソース使用率、インベントリ コンテナ間の対話、およびサーバにアクセスした Active Directory グループ）を表示できます。

図 23-3. アクティビティ モニタリング を使用した仮想環境



ユーザー	AD グループ	アプリケーション名	ソース仮想マシン名	ターゲット仮想マシン名	ソース IP	ターゲット IP
John	Doctors	Epic.exe	DoctorsWS13	EpicSVR3	172.16.254.1	172.16.112.2

重要: Linux 仮想マシンでは アクティビティ モニタリングはサポートされません。

アクティビティ モニタリングのセットアップ

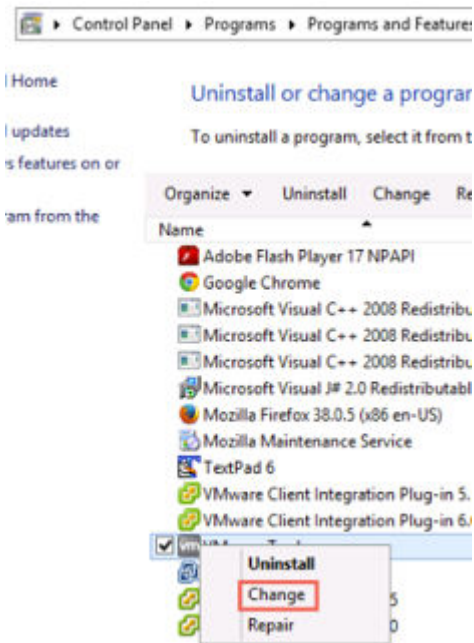
アクティビティ モニタリングを機能させるには、ゲスト イントロスペクション ドライバのインストール、ゲスト イントロスペクション 仮想マシンのインストール、NSX アクティビティ モニタリングを有効にするなど、いくつかの手順を実行する必要があります。または、Service Composer を使用してどの仮想マシンを監視するかを制御することもできます。

前提条件

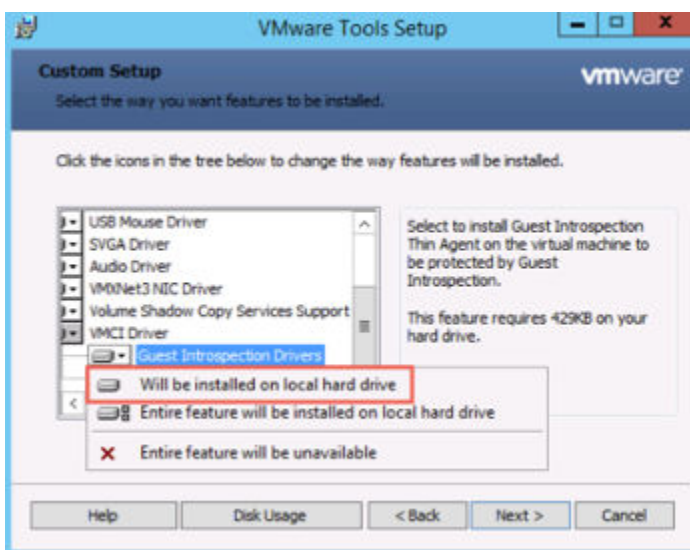
- NSX がインストール済みで、動作している必要があります。
- NSX Manager は、Windows 仮想マシン ユーザーに一致するグループを取得する Active Directory サーバにリンクされている必要があります。
- vCenter インベントリに 1 つ以上の Windows デスクトップ仮想マシンが含まれている必要があります。
- 最新の VMware Tools が Windows デスクトップ仮想マシンで実行されている必要があります。

手順

- 1 vCenter インベントリ内の Windows 仮想マシンに ゲスト イントロスペクション ドライバがまだインストールされていない場合、インストールします。
 - a [コントロール パネル\プログラム\プログラムと機能 (Control Panel\Programs\Programs and Features)] の順に移動し、[VMware Tools] を右クリックして [変更 (Change)] を選択します。



- b [変更 (Modify)] を選択します。
 - c [VMCI ドライバ (VMCI Driver)] で、[ゲスト イントロスペクション ドライバ > ローカル ハード ドライブにインストールされます (Guest Introspection Drivers > Will be installed on local hard drive)] をクリックします。



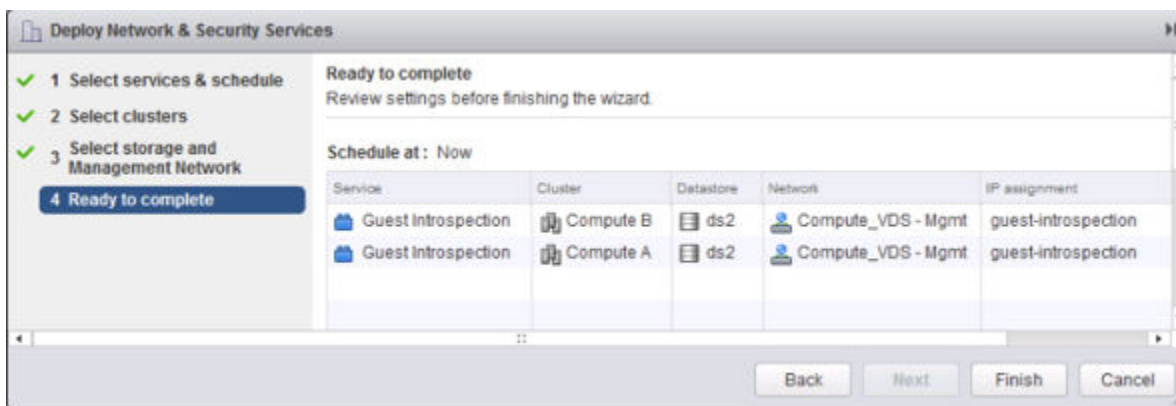
ゲスト イントロスペクション ドライバは各 Windows 仮想マシンでどのアプリケーションが実行されているかを検出し、この情報を ゲスト イントロスペクション 仮想マシンに送信します。

2 ゲスト イントロスペクション 仮想マシンをインストールします。

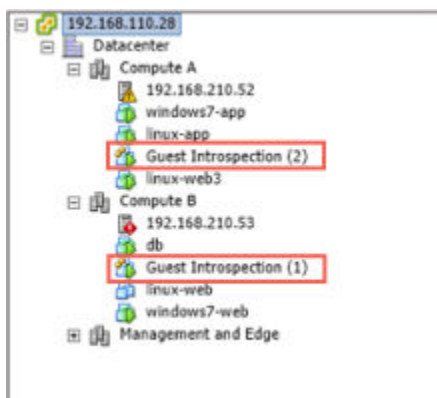
VMware Tools を初めてインストールする場合、[カスタム (Custom)] オプションを選択します。VMCI フォルダで、[ゲスト イントロスペクション ドライバ (Guest Introspection Driver)] を選択します。ドライバはデフォルトでは選択されていません。

VMware Tools をインストールした後にドライバを追加するには、次の手順を実行します。

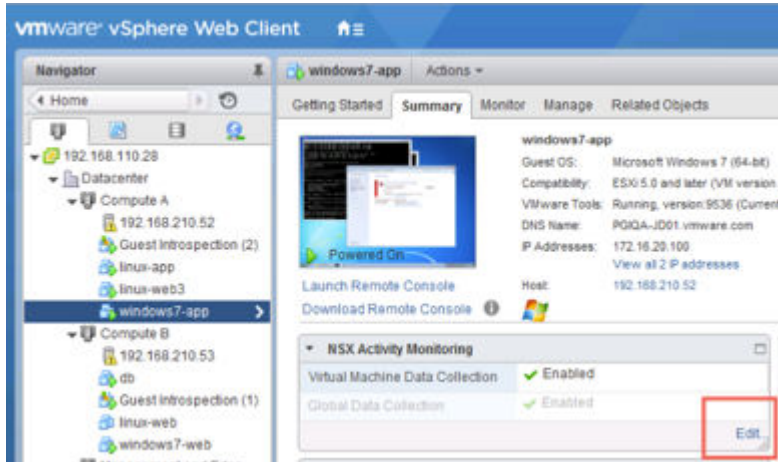
- vSphere Web Client で、[Networking and Security] > [インストール手順 (Installation)] > [サービス デプロイ (Service Deployments)] の順に移動します。
- 新しいサービス デプロイを追加します。
- [ゲスト イントロスペクション (Guest Introspection)] を選択します。
- Windows 仮想マシンが含まれるホスト クラスタを選択します。
- 適切なデータベース、ネットワーク、IP アドレス解決メカニズムを選択します。ゲスト イントロスペクション 仮想マシンで DHCP を使用していない場合、IP アドレス プールを作成して割り当てます。



各クラスタ内の各ホストに 1 つずつ、2 つの ゲスト イントロスペクション 仮想マシンがインストールされます。



- 3 Windows 仮想マシンで アクティビティ モニタリングを有効にします。
 - a [ホストおよびクラスター (Hosts and Clusters)] ビューで Windows 仮想マシンを選択し、[サマリ (Summary)] タブを選択します。
 - b NSX アクティビティ モニタリングで [編集 (Edit)] をクリックし、[はい (Yes)] をクリックします。



監視するすべての Windows 仮想マシンでこの手順を繰り返します。

- 4 (オプション) 監視する vCenter オブジェクトのリストを変更するか、動的メンバーシップルールを定義します。
 - a vSphere Web Client で、[Networking and Security] > [Service Composer] の順に移動します。
 - b [アクティビティ モニタリング データ収集 (Activity Monitoring Data Collection)] セキュリティ グループを編集します。

- c 新規の Windows 仮想マシンがクラスタに追加され、仮想マシンが自動的に監視されるように動的メンバーシップルールを定義します。
- d アクティビティ モニタリング セキュリティ グループに含める、または除外する vCenter Server オブジェクトを選択します。

アクティビティ モニタリングを有効にした仮想マシンは自動的に アクティビティ モニタリング セキュリティ グループに含まれます。

この例では、名前が「win」で始まるすべての仮想マシンが自動的に アクティビティ モニタリング セキュリティ グループに追加されます。つまり、これらの仮想マシンでは アクティビティ モニタリングが自動的に有効になります。

Edit Security Group

Ready to complete

Name: Activity Monitoring Data Collection

Description:

Scope: Global

Dynamic membership

Members matching (Any) of the criteria below

Key	Criteria	Value
VM Name	Starts with	win

Objects to Include

Name
windows7-app
windows7-web

Objects to Exclude

Name

Back Next Finish Cancel

アクティビティ モニタリング シナリオ

このセクションでは、アクティビティ モニタリングの仮想的なシナリオをいくつか説明します。

アプリケーションへのユーザー アクセス

架空の企業 ACME Enterprise では、承認されたユーザーのみに会社の資産上にある特定のアプリケーションへのアクセスを許可しています。

セキュリティ ポリシーでは、次のように定めています。

- 認証されたユーザーにのみ、重要なビジネス アプリケーションへのアクセスを許可する
- 会社のサーバ上では認証されたアプリケーションのみを許可する
- 特定のネットワークからの必要なポートのみへのアクセスを許可する

上記に基づき、会社の資産を保護するためにユーザー ID に応じた従業員のアクセス制御が必要です。まず、ACME Enterprise のセキュリティ オペレータは MS SQL Server に対し管理アクセスのみが許可されていることを確認する必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 [受信アクティビティ (Inbound Activity)] タブをクリックします。
- 4 すべての従業員からのアクセスを表示するには、[送信元 (Outbound from)] の値を [観察対象のすべての Active Directory グループ (All Observed AD Groups)] のままにします。
- 5 [ターゲット仮想マシンの場所 (Where destination virtual machine)] で [含む (includes)] を選択し、[観察対象のすべてのターゲット仮想マシン (all observed destination virtual machines)] を選択したままにします。
- 6 [およびターゲット アプリケーションの場所 (And where destination application)] で [含む (includes)] を選択し、[観察対象のすべてのターゲット アプリケーション (all observed destination applications)] をクリックして MS SQL サーバを選択します。
- 7 [検索 (Search)] をクリックします。

検索結果に、管理ユーザーのみが MS SQL Server にアクセスしていることが表示されます。グループ（財務や人事）はこれらのサーバにアクセスしていません。

- 8 [送信元 (Outbound from)] の値を人事および財務 Active Directory グループに設定することで、このクエリを逆にすることができます。
- 9 [検索 (Search)] をクリックします。

レコードは表示されず、どちらのグループのユーザーも MS SQL Server にアクセスできないことを確認できます。

データセンターのアプリケーション

セキュリティ ポリシーの一部として、ACME Enterprise では、すべてのデータセンター アプリケーションを可視化する必要があります。これにより、機密情報を収集したり、機密データを外部ソースに吸い上げたりする不正なアプリケーションを特定しやすくなります。

ACME Enterprise のクラウド管理者である John は、SharePoint Server へのアクセスが Internet Explorer を介してのみ行われ、不正なアプリケーション（FTP や RDP など）がこのサーバにアクセスできないことを確認する必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 [仮想マシン アクティビティ (VM Activity)] タブをクリックします。
- 4 [ソース仮想マシンの場所 (Where source VM)] で [含む (includes)] を選択し、データセンターのすべての仮想マシンから発信されるトラフィックをキャプチャするために [観察対象のすべての仮想マシン (All observed virtual machines)] を選択されたままにします。

- 5 [ターゲット仮想マシンの場所 (Where destination VM)] で [含む (includes)] を選択し、[観察対象のすべての仮想マシン (All observed virtual machines)] をクリックして SharePoint Server を選択します。
- 6 [検索 (Search)] をクリックします。

検索結果の [アウトバウンド App 製品名 (Outbound App Product Name)] 列に、SharePoint Server へのすべてのアクセスが Internet Explorer を介してのみ行われたことが表示されます。検索結果が比較的一様な場合は、この SharePoint Server にファイアウォール ルールが適用されていて、他のアクセス方法がすべて阻止されたことを示します。

また、検索結果には、ソース グループではなく、観察されたトラフィックのソース ユーザーが表示されます。検索結果の矢印をクリックすると、ユーザーが属する Active Directory グループなど、ソース ユーザーの詳細が表示されます。

開いているポートの検証

管理者 John は、ACME Enterprise の SharePoint Server に認証済みのアプリケーションのみがアクセスしていることを確認したうえで、企業が想定する使用に基づいて必要なポートだけを開くことができます。

前提条件


「データセンターのアプリケーション」シナリオで、管理者 John は、ACME Enterprise の SharePoint Server へのトラフィックを観察していました。現在、SharePoint Server から MSSQL サーバへのすべてのアクセスを、想定したプロトコルおよびアプリケーション経由にしたいと考えています。

手順

- 1 [ホームに移動 (Go Home)] アイコンをクリックします。
- 2 [vCenter ホーム (vCenter Home)] をクリックして、[仮想マシン (Virtual Machines)] をクリックします。
- 3 [win_sharepoint] を選択して、[監視 (Monitor)] タブをクリックします。
- 4 [アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 5 [ターゲットの場所 (Where destination)] で、[win2K-MSSQL] を選択します。
- 6 [検索 (Search)] をクリックします。

検索結果に、SharePoint Server から MSSQL サーバへのトラフィックが表示されます。[ユーザー (User)] 列と [送信 App (Outbound App)] 列に、システム プロセスのみが MSSQL サーバに接続していることが表示されます。これは John が想定していた結果です。

[受信ポート (Inbound Port)] 列と [アプリケーション (App)] 列に、すべてのアクセスが接続先サーバ上で実行される MSSQL サーバに集まっていることが表示されます。

検索結果のレコードが多すぎて Web ブラウザでは分析できない場合、ページの右下にある  アイコンをクリックすれば、一連の結果をすべてエクスポートして、ファイルを CSV 形式で保存できます。

データ収集を有効にする

アクティビティ モニタリング レポートを実行する前に、vCenter Server 上の 1 台以上の仮想マシンでデータ収集を有効にする必要があります。レポートを実行する前に、有効にした仮想マシンがアクティブであり、ネットワーク トラフィックを生成していることを確認してください。

NSX Manager は、Active Directory のドメイン コントローラにも登録する必要があります。[「NSX Manager への Windows ドメインの登録」](#)を参照してください。

アクティビティ モニタリングによって追跡されるのはアクティブな接続だけです。vNIC レベルでファイアウォール ルールによってブロックされる仮想マシン トラフィックは、レポートには反映されません。

単一の仮想マシンでのデータ収集を有効にする

データ収集は、アクティビティ モニタリング レポート実行の少なくとも 5 分前までに有効にする必要があります。

前提条件

手順

- 1 vSphere Web Client にログインします。
- 2 [vCenter] をクリックし、[仮想マシンおよびテンプレート (VMs and Templates)] をクリックします。
- 3 左側のインベントリ パネルで、仮想マシンを選択します。
- 4 [管理 (Manage)] タブをクリックして、[設定 (Settings)] タブをクリックします。
- 5 左側のパネルで、[NSX アクティビティ モニタリング (NSX Activity Monitoring)] をクリックします。
- 6 [編集 (Edit)] をクリックします。
- 7 [NSX アクティビティ モニタリング データ収集設定を編集] ダイアログ ボックスで、[はい (Yes)] をクリックします。

複数の仮想マシンでのデータ収集を有効にする

アクティビティ モニタリング データ収集セキュリティ グループは、事前定義されたセキュリティ グループです。このセキュリティ グループには一度に複数の仮想マシンを追加でき、データ収集はそれらすべての仮想マシンで有効になります。

データ収集は、アクティビティ モニタリング レポート実行の少なくとも 5 分前までに有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[Service Composer] をクリックします。
- 3 [セキュリティ グループ (Security Groups)] タブをクリックします。
- 4 アクティビティ モニタリング データ収集セキュリティ グループを選択し、[編集 (Edit)] (✎) アイコンをクリックします。

- 5 ウィザードに従って仮想マシンをセキュリティ グループに追加します。

データ収集はこのセキュリティ グループに追加した仮想マシンのすべてで有効になり、このセキュリティ グループから除外した仮想マシンのすべてで無効になります。

仮想マシン アクティビティ レポートの表示


仮想マシンが送受信するトラフィックや、環境内の一連の仮想マシンを表示できます。

[検索 (Search)] をクリックすることでデフォルトの検索条件を使用してクイック クエリを実行することも、要件に応じてクエリを作成することもできます。


前提条件

- ゲスト イントロスペクション が環境にインストールされている必要があります。
- ドメインが NSX Manager に登録されている必要があります。ドメインの登録の詳細については、[\[NSX Manager への Windows ドメインの登録\]](#) を参照してください。
- データ収集を 1 台以上の仮想マシンで有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 [仮想マシン アクティビティ (VM Activity)] タブをクリックします。
- 4 [ソースの場所 (Where source)] の横にあるリンクをクリックします。送信トラフィックを表示する仮想マシンを選択します。選択した仮想マシンをレポートに含めるか、またはレポートから除外するかを示します。
- 5 [ターゲットの場所 (Where destination)] の横にあるリンクをクリックします。受信トラフィックを表示する仮想マシンを選択します。選択した仮想マシンをレポートに含めるか、またはレポートから除外するかを示します。
- 6 [期間 (During period)] () アイコンをクリックし、検索の期間を選択します。
- 7 [検索 (Search)] をクリックします。

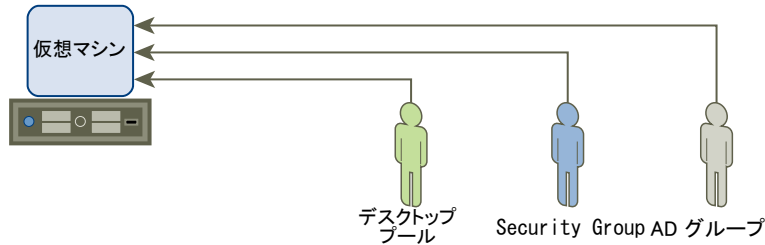
指定した条件でフィルタリングされた検索結果が表示されます。行のユーザーに関する詳細情報を表示するには、その行をクリックします。

特定のレコードまたはこのページのすべてのレコードをエクスポートして、.csv 形式でディレクトリに保存するには、ページの右下にある  アイコンをクリックします。

受信アクティビティの表示

デスクトップ プール、セキュリティ グループ、または Active Directory グループごとに、サーバのすべての受信アクティビティを表示できます。

図 23-4. 受信アクティビティの表示



[検索 (Search)] をクリックすることでデフォルトの検索条件を使用してクイック クエリを実行することも、要件に応じてクエリを作成することもできます。

前提条件


- ゲスト イントロスペクション が環境にインストールされている必要があります。
- ドメインが NSX Manager に登録されている必要があります。ドメインの登録の詳細については、[\[NSX Manager への Windows ドメインの登録\]](#) を参照してください。
- データ収集を 1 台以上の仮想マシンで有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 [受信アクティビティ (Inbound Activity)] タブをクリックします。
- 4 [発信元 (Originating from)] の横にあるリンクをクリックします。
- 5 アクティビティを表示するユーザー グループのタイプを選択します。
- 6 [フィルタのタイプ (Filter type)] で、1 つ以上のグループを選択して [OK] をクリックします。
- 7 [ターゲット仮想マシンの場所 (Where destination virtual machine)] で、[含む (includes)] または [除外 (excludes)] を選択し、選択した仮想マシンを検索に含めるか、または検索から除外するかを示します。
- 8 [およびターゲット仮想マシンの場所 (And where destination virtual machine)] の横にあるリンクをクリックします。
- 9 1 台以上の仮想マシンを選択し、[OK] をクリックします。
- 10 [およびターゲット アプリケーションの場所 (And where destination application)] で、[含む (includes)] または [除外 (excludes)] を選択し、選択したアプリケーションを検索に含めるか、または検索から除外するかを示します。
- 11 [およびターゲット アプリケーションの場所 (And where destination application)] の横のリンクをクリックします。
- 12 1 つ以上のアプリケーションを選択し、[OK] をクリックします。
- 13 [期間 (During period)] (📅) アイコンをクリックし、検索の期間を選択します。

14 [検索 (Search)] をクリックします。

指定した条件でフィルタリングされた検索結果が表示されます。結果の表の任意の場所をクリックして、指定した仮想マシンおよびアプリケーションにアクセスしたユーザーについての情報を表示します。

特定のレコードまたはこのページのすべてのレコードをエクスポートして、.csv 形式でディレクトリに保存するには、ページの右下にある  アイコンをクリックします。

送信アクティビティの表示

セキュリティ グループまたはデスクトップ プールによって実行中のアプリケーションを表示し、レポートにドリルダウンして特定のユーザー グループが送信接続を行っているクライアント アプリケーションを検出することができます。また、特定のアプリケーションにアクセス中のすべてのユーザー グループとユーザーを検索することもできます。これにより、環境でアイデンティティ ファイアウォールを調整する必要があるかどうかを判断できます。

図 23-5. 送信アクティビティの表示



前提条件

- ゲスト イントロスペクション が環境にインストールされている必要があります。
- ドメインが NSX Manager に登録されている必要があります。ドメインの登録の詳細については、[\[NSX Manager への Windows ドメインの登録\]](#) を参照してください。
- データ収集を 1 台以上の仮想マシンで有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 左側のペインで [送信アクティビティ (Outbound Activity)] タブが選択されていることを確認します。
- 4 [発信元 (Originating from)] の横にあるリンクをクリックします。
ゲスト イントロスペクション を介して検出されたすべてのグループが表示されます。
- 5 リソース使用率を表示するユーザー グループのタイプを選択します。
- 6 [フィルタ (Filter)] で、1 つ以上のグループを選択して [OK] をクリックします。
- 7 [アプリケーションの場所 (Where application)] で、[含む (includes)] または [除外 (excludes)] を選択し、選択したアプリケーションを検索に含めるか、または検索から除外するかを示します。
- 8 [アプリケーションの場所 (Where application)] の横にあるリンクをクリックします。
- 9 1 つ以上のアプリケーションを選択し、[OK] をクリックします。

- 10 [およびターゲットの場所 (And where destination)] で、[含む (includes)] または [除外 (excludes)] を選択し、選択した仮想マシンを検索に含めるか、または検索から除外するかを示します。
- 11 [およびターゲットの場所 (And where destination)] の横にあるリンクをクリックします。
- 12 1 台以上の仮想マシンを選択し、[OK] をクリックします。
- 13 [期間 (During period)] (📅) アイコンをクリックし、検索の期間を選択します。
- 14 [検索 (Search)] をクリックします。

右方向にスクロールして、表示されているすべての情報を確認します。

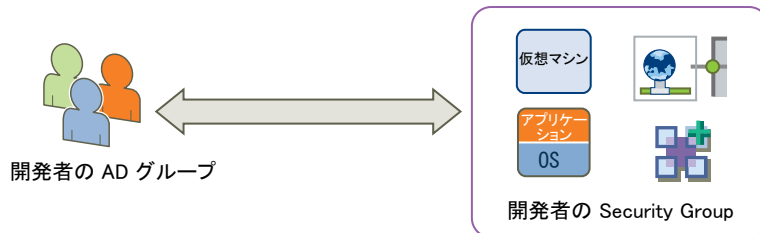
指定した条件でフィルタリングされた検索結果が表示されます。ある 1 つの行をクリックして、特定のアプリケーションを使用して特定の仮想マシンにアクセスした Active Directory グループ内のユーザーに関する情報を表示します。

特定のレコードまたはこのページのすべてのレコードをエクスポートして、.csv 形式でディレクトリに保存するには、ページの右下にある 📄 アイコンをクリックします。

インベントリ コンテナ間の相互作用の表示

Active Directory グループ、セキュリティ グループおよび/またはデスクトップ プールなどの定義済みコンテナ間で渡されるトラフィックを表示できます。これにより、共有サービスに対するアクセスを識別してでき、間違ってされたインベントリ コンテナ定義、デスクトップ プール、および Active Directory グループ間の関係を解決できます。

図 23-6. コンテナ間の相互作用




[検索 (Search)] をクリックすることでデフォルトの検索条件を使用してクイック クエリを実行することも、要件に応じてクエリを作成することもできます。

前提条件


- ゲスト イントロスペクション が環境にインストールされている必要があります。
- ドメインが NSX Manager に登録されている必要があります。ドメインの登録の詳細については、[\[NSX Manager への Windows ドメインの登録\]](#) を参照してください。
- データ収集を 1 台以上の仮想マシンで有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。

- 3 左側のペインの [コンテナ内部相互作用 (Inter Container Interaction)] タブを選択します。
- 4 [発信元 (Originating from)] の横にあるリンクをクリックします。
ゲスト イントロスペクション を介して検出されたすべてのグループが表示されます。
- 5 リソース使用率を表示するユーザー グループのタイプを選択します。
- 6 [フィルタ (Filter)] で、1 つ以上のグループを選択して [OK] をクリックします。
- 7 [ターゲットの場所 (Where the destination is)] で、[一致 (is)] または [が次でない (is not)] を選択して、選択したグループを検索に含めるか、または検索から除外するかを示します。
- 8 [ターゲットの場所 (Where the destination is)] の横にあるリンクをクリックします。
- 9 グループ タイプを選択します。
- 10 [フィルタ (Filter)] で、1 つ以上のグループを選択して [OK] をクリックします。
- 11 [期間 (During period)] () アイコンをクリックし、検索の期間を選択します。
- 12 [検索 (Search)] をクリックします。

指定した条件でフィルタリングされた検索結果が表示されます。行内をクリックして、指定したコンテナにアクセスしたユーザーについての情報を表示します。

特定のレコードまたはこのページのすべてのレコードをエクスポートして、.csv 形式でディレクトリに保存するには、ページの右下にある  アイコンをクリックします。

例：インベントリ コンテナ クエリ間の相互作用

■ 許可されている通信の確認

vCenter Server インベントリでコンテナを定義し、ルールを追加してこれらのコンテナ間の通信を許可した場合、[発信元 (Originating from)] フィールドと [ターゲットの場所 (Where the destination is)] フィールドで指定した 2 つのコンテナでこのクエリを実行することにより、ルールが機能していることを確認できます。

■ 拒否されている通信の確認

vCenter Server インベントリでコンテナを定義し、ルールを追加してこれらのコンテナ間の通信を拒否した場合、[発信元 (Originating from)] フィールドと [ターゲットの場所 (Where the destination is)] フィールドで指定した 2 つのコンテナでこのクエリを実行することにより、ルールが機能していることを確認できます。

■ 拒否されている内部コンテナ通信の確認

コンテナのメンバーに同じコンテナの他のメンバーとの通信を許可しないポリシーを実装している場合、このクエリを実行してポリシーが機能していることを確認できます。[発信元 (Originating from)] フィールドと [ターゲットの場所 (Where the destination is)] フィールドの両方でコンテナを選択します。

■ 不要なアクセスの排除

vCenter インベントリでコンテナを定義し、ルールを追加してこれらのコンテナ間の通信を許可したとします。どちらのコンテナにも、もう一方のコンテナとまったく通信しないメンバーが存在する可能性があります。その場合、こうしたメンバーを適切なコンテナから削除して、セキュリティ制御を最適化できます。このようなリストを取得するには、[発信元 (Originating from)] フィールドと [ターゲットの場所 (Where the destination is)] フィールドの両方で適切なコンテナを選択します。[ターゲットの場所 (is not)] フィールドの横にある [が次でない (Where the destination is)] を選択します。

送信 Active Directory グループ アクティビティの表示


定義済み Active Directory グループのメンバー間のトラフィックを表示し、そのデータを使用してファイアウォールルールを微調整できます。

[検索 (Search)] をクリックすることでデフォルトの検索条件を使用してクイック クエリを実行することも、要件に応じてクエリを作成することもできます。


前提条件

- ゲスト イントロスペクション が環境にインストールされている必要があります。
- ドメインが NSX Manager に登録されている必要があります。ドメインの登録の詳細については、[\[NSX Manager への Windows ドメインの登録\]](#) を参照してください。
- データ収集を 1 台以上の仮想マシンで有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 左側のペインの [Active Directory グループおよびコンテナ (AD Groups & Containers)] タブを選択します。
- 4 [発信元 (Originating from)] の横にあるリンクをクリックします。
ゲスト イントロスペクション を介して検出されたすべてのグループが表示されます。
- 5 検索に含めるユーザー グループのタイプを選択します。
- 6 [フィルタ (Filter)] で、1 つ以上のグループを選択して [OK] をクリックします。
- 7 [Active Directory グループの場所 (Where AD Group)] で、[含む (includes)] または [除外 (excludes)] を選択し、選択した Active Directory グループを検索に含めるか、または検索から除外するかを示します。
- 8 [Active Directory グループの場所 (Where AD Group)] の横のリンクをクリックします。
- 9 1 つ以上の Active Directory グループを選択し、[OK] をクリックします。
- 10 [期間 (During period)]  アイコンをクリックし、検索の期間を選択します。
- 11 [検索 (Search)] をクリックします。

指定した条件でフィルタリングされた検索結果が表示されます。行内をクリックして、指定したセキュリティ グループまたはデスクトップ プール内からネットワーク リソースにアクセスしている、指定した Active Directory グループのメンバーの情報を表示します。

特定のレコードまたはこのページのすべてのレコードをエクスポートして、.csv 形式でディレクトリに保存するには、ページの右下にある  アイコンをクリックします。

データ収集のオーバーライド

ネットワーク過負荷などの緊急事態の場合は、グローバル レベルでデータ収集をオフにできます。これにより、他のすべてのデータ収集設定がオーバーライドされます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックして、[アクティビティ モニタリング (Activity Monitoring)] をクリックします。
- 3 [設定 (Settings)] タブをクリックします。
- 4 データ収集をオーバーライドする vCenter Server を選択します。
- 5 [編集 (Edit)] をクリックします。
- 6 [レポート作成データの収集 (Collect reporting data)] を選択解除します。
- 7 [OK] をクリックします。

トレースフロー

トレースフローは、パケットを挿入し、そのパケットが物理ネットワークおよび論理ネットワークを通過するときの通り道を観察する機能を提供するトラブルシューティングのためのツールです。これを観察することで、ダウンしているノードや、パケットがターゲットに届くのを妨げているファイアウォール ルールを特定するなど、ネットワークに関する情報を判断できます。

トレースフローについて

トレースフローは、オーバーレイ ネットワークおよびアンダーレイ ネットワークの物理エンティティや論理エンティティ (ESXi ホスト、論理スイッチ、分散論理ルーターなど) をトラバースするときに、パケットを vSphere Distributed Switch (VDS) ポートに挿入し、パケットのパスに沿ったさまざまな観測ポイントを提供します。これにより、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。トレースフローは、オーバーレイ ネットワークを経由するマーク付けされたパケットを観察します。各パケットがオーバーレイ ネットワークを経由して宛先ゲスト仮想マシンに到達し、配信可能状態になるまでの様子が観察されます。ただし、挿入されたトレースフロー 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。これは、ゲスト仮想マシンがパワーオフの状態でもトレースフローが正常に動作することを意味します。

トレースフローでは、次のトラフィック タイプがサポートされています。

- レイヤー 2 ユニキャスト
- レイヤー 3 ユニキャスト
- レイヤー 2 ブロードキャスト
- レイヤー 2 マルチキャスト

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。トレースフローのソースは、常に仮想マシンの仮想 NIC (vNIC) です。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 Services Gateway (ESG) 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。

送信元 vNIC と宛先 vNIC が同じレイヤー 2 ドメイン内に存在する場合、トレースフロー操作はレイヤー 2 と見なされます。NSX の場合、これは、VXLAN ネットワーク識別子 (VNI またはセグメント ID) が同じであることを意味します。これは、2 台の仮想マシンが同じ論理スイッチに接続されている場合などに発生します。

NSX ブリッジが設定されている場合、未知のレイヤー 2 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。

レイヤー 3 トレースフロー ユニキャスト トラフィックの場合、2 つのエンド ポイントは、別々の論理スイッチ上にあり、異なる VNI が設定されていて、分散論理ルーター (DLR) に接続されています。

マルチキャスト トラフィックの場合、送信元は仮想マシン vNIC で、宛先はマルチキャスト グループ アドレスになります。

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。



警告: デプロイの論理ポート数によっては、マルチキャストおよびブロードキャスト トレースフロー操作で大量のトラフィックが生成される可能性があります。

トレースフローを使用する方法は、API と GUI の 2 種類があります。API は、GUI で使用される API と同じですが、API ではパケットを詳細に設定することができます。GUI の設定はより限定的です。

GUI では、次の値を設定できます。

- プロトコル --- TCP、UDP、ICMP。
- 存続時間 (TTL)。デフォルトは 64 ホップです。
- TCP や UDP の送信元および宛先ポート数。デフォルト値は 0 です。
- TCP フラグ。

- ICMP ID およびシーケンス番号。どちらもデフォルトは 0 です。
- トレースフロー操作の有効期限切れタイムアウト（ミリ秒単位）。デフォルトは 10,000 ミリ秒です。
- イーサネット フレーム サイズ。デフォルトは 128 バイト/フレームです。最大フレーム サイズは 1000 バイト/フレームです。
- ペイロード エンコード。デフォルトは Base64 です。
- ペイロード値。

トラブルシューティングのためのトレースフローの使用

トレースフローが役立つシナリオには、以下のように複数のシナリオがあります。

トレースフローは以下のシナリオで役立ちます。

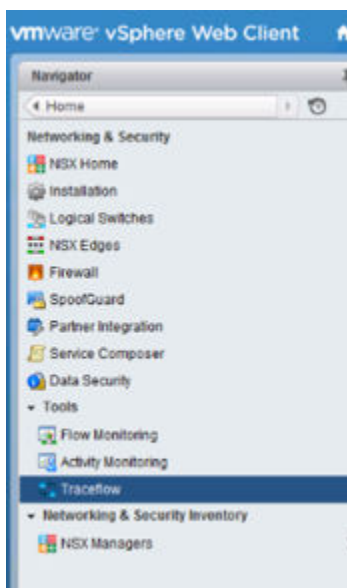
- 正確なトラフィックの経由パスを確認することによるネットワーク障害のトラブルシューティング
- リンクの使用率を確認することによるパフォーマンス監視
- ネットワークが本番環境にあるときの動作を確認することによるネットワーク計画

前提条件

- トレースフローの操作には、vCenter Server、NSX Manager、NSX Controller クラスタ、およびホスト上の netcpa ユーザー ワールド エージェント間の通信が必要です。
- トレースフローを期待どおりに動作させるには、コントローラ クラスタが接続され、健全な状態であることを確認します。

手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [トレースフロー (Traceflow)] の順に移動します。



- 2 トラフィック タイプをユニキャスト、ブロードキャスト、マルチキャストから選択します。

3 ソース仮想マシン vNIC を選択します。

その仮想マシンが、トレースフローの実行元と同じ vCenter Server 上で管理されている場合、リストから仮想マシンと vNIC を選択できます。

4 ユニキャストトレースフローの場合、ターゲット vNIC 情報を入力します。

ターゲットとして、ホスト、仮想マシン、分散論理ルーター、Edge Services Gateway などの NSX オーバーレイまたは NSX アンダーレイ内の任意のデバイスの vNIC を指定できます。ターゲットが VMware Tools の実行元の仮想マシンであり、トレースフローの実行元と同じ vCenter Server によって管理されている場合、リストから仮想マシンと vNIC を選択できます。

そうでない場合、ターゲット IP アドレス（さらに、ユニキャスト レイヤー 2 トレースフローの場合は MAC アドレス）を入力する必要があります。この情報は、デバイス コンソール、または SSH セッション内のデバイス自体から収集できます。たとえば、このマシンが Linux 仮想マシンの場合、IP アドレスと MAC アドレスは、Linux ターミナルで **ifconfig** コマンドを実行することで取得できます。分散論理ルーターまたは Edge Services Gateway の場合、この情報は **show interface** CLI コマンドで収集できます。

5 レイヤー 2 ブロードキャスト トレースフローの場合、サブネットのプリフィックスの長さを入力します。

パケットは、MAC アドレスのみに基づいてスイッチされます。ターゲット MAC アドレスは FF:FF:FF:FF:FF:FF です。

IP パケットがファイアウォール検査に有効であるためには、ソース IP アドレスおよびターゲット IP アドレスの両方が必要です。

6 レイヤー 2 マルチキャスト トレースフローの場合、マルチキャスト グループ アドレスを入力します。

パケットは、MAC アドレスのみに基づいてスイッチされます。

IP パケットが有効であるためには、ソース IP アドレスおよびターゲット IP アドレスの両方が必要です。マルチキャストの場合、MAC アドレスは IP アドレスから推定されます。

7 その他の必須およびオプション設定を行います。

8 [トレース (Trace)] をクリックします。

例：シナリオ

次の例に、単一の ESXi ホスト上で実行されている 2 つの仮想マシンを含むレイヤー 2 トレースフローを示します。2 台の仮想マシンは、単一の論理スイッチに接続されています。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Advanced Options

Protocol: TCP

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Received	esx-01a.corp.local	Firewall	Firewall
4	Forwarded	esx-01a.corp.local	Firewall	Firewall
5	Delivered	esx-01a.corp.local	vNIC	vNIC

次の例に、2 台の異なる ESXi ホスト上で実行されている 2 つの仮想マシンを含むレイヤー 2 トレースフローを示します。2 台の仮想マシンは、単一の論理スイッチに接続されています。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **Unicast**

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▼ Advanced Options

Protocol: **TCP**

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5	Received	esx-02a.corp.local	Firewall	Firewall
6	Forwarded	esx-02a.corp.local	Firewall	Firewall
7	Delivered	esx-02a.corp.local	vNIC	vNIC

次の例に、レイヤー 3 トレースフローを示します。2 つの仮想マシンは、分散論理ルーターによって分離された 2 つの異なる論理スイッチに接続されています。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d4:2b

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
4		Received	esx-01a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-01a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-01a.corp.local	Logical Switch	DB-Tier-01
7		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
9		Received	esx-02a.corp.local	Firewall	Firewall
10		Forwarded	esx-02a.corp.local	Firewall	Firewall
11		Delivered	esx-02a.corp.local	vNIC	vNIC

次の例に、3つの仮想マシンが単一の論理スイッチに接続されているデプロイ内の、ブロードキャストトレースフローを示します。仮想マシンのうちの2つは1台のホスト(esx-01a)上にあり、もう1つは別のホスト(esx-02a)上にあります。ブロードキャストは、ホスト 192.168.210.53 上の仮想マシンのいずれかから送信されます。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **L2 Broadcast** ⚠ High volume of traffic may get generated for this traffic type.

Source: * web-01a - Network adapter 1 [Change...](#) Subnet Prefix Length: * **24**

IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 172.16.10.255, MAC: FF:FF:FF:FF:FF:FF

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
3		Received	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Forwarded	esx-01a.corp.local	Firewall	Firewall
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5		Delivered	esx-01a.corp.local	vNIC	vNIC
5		Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5		Received	esx-02a.corp.local	Firewall	Firewall
6		Forwarded	esx-02a.corp.local	Firewall	Firewall
7		Delivered	esx-02a.corp.local	vNIC	vNIC

次の例に、マルチキャスト構成のデプロイ環境にマルチキャストトラフィックが送信されるときに何が起きるかを示します。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **L2 Multicast** ⚠ High volume of traffic may get generated for this traffic type.

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination IP: * e.g. 239.0.0.1
IP: 239.0.0.1, MAC: 01:00:5e:00:00:01

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Received	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Forwarded	esx-01a.corp.local	Firewall	Firewall
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5		Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5		Delivered	esx-01a.corp.local	vNIC	vNIC
5		Received	esx-02a.corp.local	Firewall	Firewall
6		Forwarded	esx-02a.corp.local	Firewall	Firewall
7		Delivered	esx-02a.corp.local	vNIC	vNIC

次の例は、ターゲット アドレスに送信された ICMP トラフィックをブロックする分散ファイアウォール ルールによって、トレースフローがドロップされるとき動作です。ターゲット仮想マシンが別のホスト上にあるにもかかわらず、トラフィックは元のホストに留まります。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **Unicast**

Source: * web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Destination: * web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▶ Advanced Options

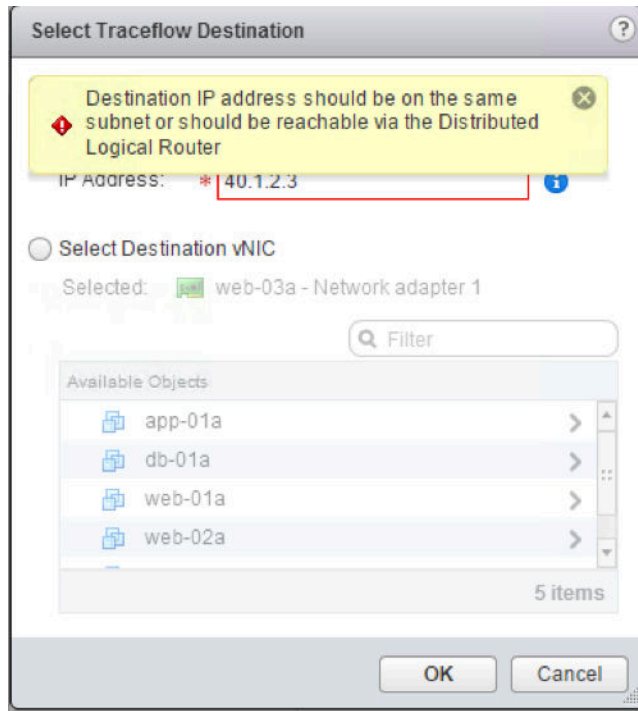
Trace

Trace Result: Traceflow dropped observation(s) reported

1 Dropped

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Dropped	esx-01a.corp.local	Firewall	Firewall (Rule - 1013)

次の例は、トレースフローのターゲットが Edge Services Gateway の外部にある場合の動作です。たとえば、インターネット上の IP アドレスや、Edge Services Gateway を介してルーティングする必要がある内部のターゲットの場合です。トレースフローは同じサブネット上にあるターゲット、あるいは分散論理ルーター (DLR) を介してアクセス可能なターゲットのいずれかでサポートされるため、トレースフローは設計上許可されません。



次の例は、トレースフロー ターゲットが別のサブネット上にあるパワーオフされた仮想マシンである場合の動作です。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: app-01a - Network adapter 1 Change...
IP: 172.16.20.11, MAC: 00:50:56:ae:23:b9

Destination: db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d...

► Advanced Options

Trace

Trace Result: No delivered or dropped observations reported

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-02a.corp.local	vNIC	vNIC
1		Received	esx-02a.corp.local	Firewall	Firewall
2		Forwarded	esx-02a.corp.local	Firewall	Firewall
3		Forwarded	esx-02a.corp.local	Logical Switch	App-Tier-01
4		Received	esx-02a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-02a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-02a.corp.local	Logical Switch	DB-Tier-01

NSX Edge VPN 構成例

このシナリオには、NSX Edge と相手側の Cisco または WatchGuard VPN の間の基本的なポイント トゥ ポイント IPSEC VPN 接続の構成例が含まれています。

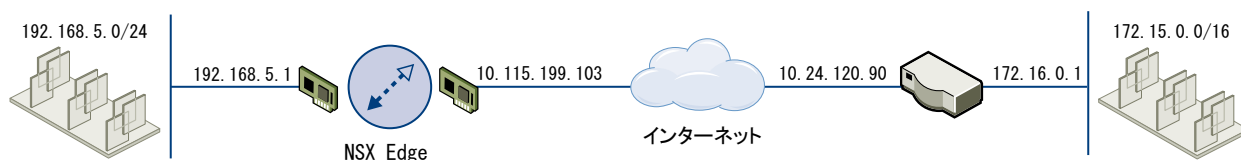
このシナリオでは、NSX Edge が内部ネットワーク 192.0.2.0/24 をインターネットに接続します。NSX Edge インターフェイスは以下のように構成されています。

- アップリンク インターフェイス : 198.51.100.1
- 内部インターフェイス : 192.0.2.1

リモート ゲートウェイは、172.16.0.0/16 内部ネットワークをインターネットに接続します。リモート ゲートウェイ インターフェイスは以下のように設定されています。

- アップリンク インターフェイス : 10.24.120.90/24
- 内部インターフェイス : 172.16.0.1/16

図 24-1. リモート VPN ゲートウェイに接続する NSX Edge



注: NSX Edge から NSX Edge IPSEC へのトンネルでは、2 番目の NSX Edge をリモート ゲートウェイとしてセットアップすることにより、同じシナリオを使用できます。

この章には、次のトピックが含まれています。

- [用語集](#)
- [IKE フェーズ 1 とフェーズ 2](#)
- [IPSec VPN サービスの設定例](#)
- [Cisco 2821 を統合したサービス ルーターの使用](#)
- [Cisco ASA 5510 の使用](#)
- [WatchGuard Firebox X500 の設定](#)
- [NSX Edge についてのトラブルシューティング例](#)

用語集

IPSec はオープン標準のフレームワークです。IPSEC VPN のトラブルシューティングに使える NSX Edge やその他の VPN アプライアンスのログには、多くの専門用語があります。

以下に、いくつかの標準を示します。

- ISAKMP (Internet Security Association and Key Management Protocol) は、Security Associations (SA) とインターネット環境の暗号化のために RFC 2408 によって策定されたプロトコルです。ISAKMP は認証のためのフレームワークと鍵交換のみを提供し、独立した鍵交換のためにデザインされています。
- Oakley は鍵同意プロトコルの 1 つで、Diffie-Hellman 鍵交換アルゴリズムを使用することにより、安全でない接続においても認証された機関同士で鍵材料の交換ができるようになっています。
- IKE (Internet Key Exchange) は ISAKMP フレームワークと Oakley の組み合わせです。NSX Edge は IKEv1 を提供します。
- Diffie-Hellman (DH) 鍵交換は、安全でない通信チャネル経由でも、お互い認識のない 2 つの機関が共同で共有秘密鍵を発行できる暗号プロトコルです。VSE は DH グループ 2 (1024 ビット) とグループ 5 (1536 ビット) をサポートしています。

IKE フェーズ 1 とフェーズ 2

IKE は安全で認証された通信に用いられる標準的手法です。

フェーズ 1 のパラメータ

フェーズ 1 では手動でのピアの認証、暗号パラメータのネゴシエーション、セッションキーの生成をセットアップします。NSX Edge で使用されるフェーズ 1 パラメータ

- メイン モード
- TripleDES/AES [設定可]
- SHA-1
- MODP グループ 2 (1024 ビット)
- プリシェアードシークレット [設定可]
- 28800 秒間 (8 時間) 有効、キロバイト再キー化不可の SA
- ISAKMP アグレッシブ モードを無効にする

フェーズ 2 のパラメータ

IKE フェーズ 2 では IPsec トンネルのためにキー材料を生成することにより IPsec トンネルをネゴシエーションします (IKE フェーズ 1 キーをベースとして使用、または新しいキー交換を実行)。NSX Edge でサポートする IKE フェーズ 2 パラメータ

- TripleDES/AES [フェーズ 1 設定とマッチ]

- SHA-1
- ESP トンネル モード
- MODP グループ 2 (1024 ビット)
- 再キー化のための完全転送セクレシー
- 3600 秒間 (1 時間) 有効、キロバイト再キー化不可の SA
- IPv4 サブネットを用いたすべての IP プロトコル、すべてのポート、2 ネットワーク間のセレクト

トランザクション モードのサンプル

NSX Edge はフェーズ 1 でメイン モードを、フェーズ 2 でクイック モードをサポートしています。

NSX Edge は PSK、3DES/AES128、sha1、DH Group 2/5 を必要とするポリシーを提示します。ピアはポリシーを受け入れる必要があり、そうでない場合、ネゴシエーション フェーズは失敗します。

フェーズ 1：メイン モード トランザクション

この例では NSX Edge から Cisco デバイスに開始されたフェーズ 1 のネゴシエーションの交換を示しています。

メイン モードでの NSX Edge と Cisco VPN デバイスとの間の一連のトランザクションを以下に示します。

- 1 NSX Edge から Cisco へ
 - プロポーザル : encrypt 3des-cbc、sha、psk、group5(group2)
 - DPD 有効
- 2 Cisco から NSX Edge へ
 - Cisco の選択によるプロポーザルを含む
 - Cisco デバイスが、ステップ 1 で NSX Edge が送信したパラメータをまったく受け付けなかった場合、Cisco デバイスは NO_PROPOSAL_CHOSEN というフラグでメッセージを送信し、ネゴシエーションを終了します。
- 3 NSX Edge から Cisco へ
 - DH キーとナンス
- 4 Cisco から NSX Edge へ
 - DH キーとナンス
- 5 NSX Edge から Cisco へ (暗号化)
 - ID (PSK) を含む
- 6 Cisco から NSX Edge へ (暗号化)
 - ID (PSK) を含む
 - Cisco デバイスが PSK がマッチしないと判断すると、Cisco デバイスは INVALID_ID_INFORMATION というフラグでメッセージを送信し、フェーズ 1 は失敗します。

フェーズ 2：クイック モード トランザクション

クイック モードでの NSX Edge と Cisco VPN デバイスとの間の一連のトランザクションを以下に示します。

1 NSX Edge から Cisco へ

NSX Edge はピアにフェーズ 2 ポリシーを提示します。次はその例です。

```
Aug 26 12:16:09 weiqing-desktop
ipsec[5789]:
"s1-c1" #2: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:d20849ac
proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
```

2 Cisco から NSX Edge へ

Cisco デバイスがこのプロポーザルに対しマッチするポリシーが見つけれない場合は、NO_PROPOSAL_CHOSEN を送り返します。それ以外では、Cisco デバイスは選択されたパラメータのセットを送信します。

3 NSX Edge から Cisco へ

デバッグを行うには、NSX Edge の IPSec ログ設定をオンにし、Cisco の暗号デバッグを有効にします (debug crypto isakmp <level>)。

IPSec VPN サービスの設定例

VPN パラメータを設定してから、IPSEC サービスを有効にする必要があります。

手順

1 NSX Edge VPN パラメータの設定例

IPSec VPN サービスを提供するには、NSX Edge で少なくとも 1 つの外部 IP アドレスを設定する必要があります。

2 IPSec VPN サービスを有効にする例

ローカル サブネットからピア サブネットにトラフィックが流れるようにするには、IPSec VPN サービスを有効にする必要があります。


NSX Edge VPN パラメータの設定例

IPSec VPN サービスを提供するには、NSX Edge で少なくとも 1 つの外部 IP アドレスを設定する必要があります。

手順

1 vSphere Web Client にログインします。

2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。

- 3 NSX Edge をダブルクリックします。
- 4 [監視] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 [追加] () アイコンをクリックします。
- 7 IPSec VPN の名前を入力します。
- 8 NSX Edge インスタンスの IP アドレスを [ローカル ID] に入力します。これは、リモート サイトのピア ID となります。
- 9 ローカル エンドポイントの IP アドレスを入力します。
プリシェアード キーを使用して IP トンネルに IP を追加する場合は、ローカル ID とローカル エンドポイント IP が同じになる可能性があります。
- 10 CIDR フォーマットで、サイト間で共有するサブネットを入力します。複数のサブネットを入力するには、コンマ区切りを使用します。
- 11 ピア サイトを一意に識別するためにピア ID を入力します。証明書認証を使用するピアの場合、この ID はピアの証明書の共通名である必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。VMware では、VPN のパブリック IP アドレス、または VPN サービスの FQDN をピア ID として使用することをお勧めしています。
- 12 ピア サイトの IP アドレスを [ピア エンドポイント] に入力します。ここを空白のままにしておくと、NSX Edge はピア デバイスの接続リクエストまで待機します。
- 13 ピア サブネットの内部 IP アドレスを CIDR フォーマットで入力します。複数のサブネットを入力するには、コンマ区切りを使用します。
- 14 暗号化アルゴリズムを選択します。
- 15 [認証方法] で、次のいずれかを選択します。

オプション	説明
PSK (Pre Shared Key)	このオプションを選択すると、NSX Edge とピア サイトが共有する秘密鍵が認証に使用されます。秘密鍵は、最大長が 128 バイトの文字列です。
証明書	このオプションを選択すると、グローバル レベルで定義された証明書が認証に使用されます。

- 16 匿名サイトが VPN サービスに接続する場合は、共有鍵を入力します。
- 17 [シェアード キーの表示] をクリックし、ピア サイト上に鍵を表示します。
- 18 [Diffie-Hellman (DH) グループ] で、ピア サイトと NSX Edge が安全でない通信チャンネル上で共有シークレットを確立できるようにする暗号化スキームを選択します。
- 19 必要に応じて MTU しきい値を変更します。
- 20 完全転送セクレシー (PFS) しきい値を有効または無効にします。IPsec ネゴシエーションでは、完全転送セクレシー (PFS) によって、新しい暗号化鍵が前の鍵のいずれとも関連付けられないようになります。

21 [OK] をクリックします。

NSX Edge で、ローカル サブネットからピア サブネットへのトンネルが作成されます。

次のステップ

IPSec VPN サービスを有効にします。

IPSec VPN サービスを有効にする例

ローカル サブネットからピア サブネットにトラフィックが流れるようにするには、IPSec VPN サービスを有効にする必要があります。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [監視] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPSec VPN] をクリックします。
- 6 [有効化] をクリックします。

次のステップ

ローカル サブネットとピア サブネットの間のトラフィック フローをログに記録するには、[ログの有効化] をクリックします。

Cisco 2821 を統合したサービス ルーターの使用

ここでは、Cisco IOS を使用して実行された構成について説明します。

手順

- 1 インターフェイスとデフォルト ルートの設定

```
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

2 IKE ポリシーの設定

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
    pre-share
Router(config-isakmp)# exit
```

3 プリシェアードシークレットで各ピアをマッチする

```
Router# config term
Router(config)# crypto isakmp key vshield
    address 10.115.199.103
Router(config-isakmp)# exit
```

4 IPSEC 変換の定義

```
Router# config term
Router(config)# crypto ipsec transform-set
    myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit
```

5 IPSEC アクセス リストの作成

```
Router# config term
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# access-list 101 permit ip
    172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

6 ポリシーのクリプト マップとの紐付けとラベル付け

以下の例では、クリプト マップが MYVPN としてラベル付けされています。

```
Router# config term
Router(config)# crypto map MYVPN 1
    ipsec-isakmp
% NOTE: This new crypto map will remain
disabled until a peer and a valid
access list have been configured.
Router(config-crypto-map)# set transform-set
    myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer
    10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

例：設定

```

router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
    esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN

```

```

!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0
      0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
scheduler allocate 20000 1000
!
end

```

Cisco ASA 5510 の使用

以下の出力を使用して Cisco ASA 5510 を設定します。

```

ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0
!
interface Ethernet0/1
nameif trusted
security-level 90
ip address 172.16.0.1 255.255.0.0

```



```

!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
    192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0
    172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
    udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
    mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
    sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800

```

```

crypto ipsec security-association lifetime kilobytes 4608000
crypto map MYVPN 1 match address ACL1
crypto map MYVPN 1 set pfs
crypto map MYVPN 1 set peer 10.115.199.103
crypto map MYVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
crypto isakmp enable untrusted
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end

```

WatchGuard Firebox X500 の設定

WatchGuard Firebox X500 をリモート ゲートウェイとして設定できます。

注: 正確な手順については、お使いの WatchGuard Firebox ドキュメントを参照してください。

手順

- 1 Firebox System Manager で、[Tools] - [Policy Manager] を選択します。
- 2 Policy Manager で、[Network] - [Configuration] の順に選択します。
- 3 インターフェイスを設定し、[OK] をクリックします。
- 4 (オプション) [Network] - [Routes] を選択して、デフォルト ルートを設定します。
- 5 [Network] - [Branch Office VPN] - [Manual IPSec] を選択して、リモート ゲートウェイを設定します。
- 6 IPSec Configuration ダイアログ ボックスで、[Gateways] をクリックして IPSEC Remote Gateway を設定します。
- 7 IPSec Configuration ダイアログ ボックスで、[Tunnels] をクリックしてトンネルを設定します。

- 8 IPsec Configuration ダイアログ ボックスで、[Add] をクリックしてルーティング ポリシーを追加します。
- 9 [閉じる (Close)] をクリックします。
- 10 トンネルが動作していることを確認します。

NSX Edge についてのトラブルシューティング例

この情報は、ご使用のセットアップでネゴシエーション問題のトラブルシューティングを行うときに参考にしてください。

成功するネゴシエーション（フェーズ 1 とフェーズ 2 共）

次の例は、NSX Edge と Cisco デバイス間の成功したネゴシエート結果を示しています。

NSX Edge

NSX Edge コマンドライン インターフェイスから（ipsec auto -status、show service ipsec コマンドの一部） の場合は次のようになります。

```
000 #2: "s1-cl":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-cl" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-cl":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

Cisco

```
ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

IKE Peer: 10.20.129.80
Type : L2L          Role    : responder
Rekey : no          State   : MM_ACTIVE
Encrypt : 3des      Hash    : SHA
Auth : preshared    Lifetime: 28800
Lifetime Remaining: 28379
```

フェーズ 1 ポリシーがマッチしない

以下に、フェーズ 1 ポリシーがマッチしないエラーのログを示します。

NSX Edge

NSX Edge が STATE_MAIN_I1 状態でハングしています。/var/log/messages の内容を調べ、ピアが「NO_PROPOSAL_CHOSEN」を設定して IKE メッセージを送り返したことを示す情報があることを確認してください。

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
    expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
    import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    |     next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |     length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    |     DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |     protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |     SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    |     Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    "s1-c1" #1: ignoring informational payload,
    type NO_PROPOSAL_CHOSEN msgid=00000000
```

Cisco

デバッグクリプトが有効の場合、プロポーザルが受け入れられなかったというエラーメッセージがプリントされます。

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
    IP = 10.20.129.80, IKE_DECODE RECEIVED
    Message (msgid=0) with payloads : HDR + SA (1)
    + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
    processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
    types for class Group Description: Rcv'd: Group 5
    Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
    types for class Group Description: Rcv'd: Group 5
    Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
    Message (msgid=0) with payloads : HDR + NOTIFY (11)
    + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
    All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
    payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
    FSM error history (struct &0xd8355a60) <state>, <event>:
    MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM-->MM_START,
```

```

EV_START_MM-->MM_START, EV_START_MM-->MM_START,
EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
MM:9e0e4511 terminating: flags 0x01000002, refcnt 0,
tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
delete/delete with reason message

```

フェーズ 2 がマッチしない

以下に、フェーズ 2 ポリシーがマッチしないエラーのログを示します。

NSX Edge

NSX Edge は、STATE_QUICK_I1 状態でハングしています。ログメッセージは、ピアが NO_PROPOSAL_CHOSEN メッセージを送信したことを示しています。

```

000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | next payload
type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |
| DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | Notify Message
Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
ignoring informational payload, type NO_PROPOSAL_CHOSEN
msgid=00000000

```

Cisco

フェーズ 1 は完了したがフェーズ 2 はポリシー ネゴシエーションの失敗により失敗したという、デバッグメッセージが示されます。

```

Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
+ SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
total length : 288

```

```

.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
    Session is being torn down. Reason: Phase 2 Mismatch

```

PFS 不一致

以下に、PFS 不一致エラー ログを示します。

NSX Edge

PFS はフェーズ 2 の一部としてネゴシエートされます。PFS が一致しない場合、「[フェーズ 2 がマッチしない](#)」で説明されている失敗ケースと類似の反応を示します。

```

000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
    QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
    idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
    (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |     next payload
    type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |     length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    |     DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |     protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |     SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |     Notify Message
    Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
    informational payload, type NO_PROPOSAL_CHOSEN
    msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
    91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    | processing informational NO_PROPOSAL_CHOSEN (14)

```

Cisco

```

<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, sending delete/delete with
    reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, constructing IKE delete payload

```

```

Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
    Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
    + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
    Session is being torn down. Reason: Phase 2 Mismatch

```

PSK が一致しない

以下に、PSK が一致しないエラーのログを示します。

NSX Edge

PSK はフェーズ 1 の最後のラウンドでネゴシエートされます。PSK ネゴシエーションに失敗した場合、NSX Edge の状態は STATE_MAIN_I4 です。ピアは INVALID_ID_INFORMATION を含むメッセージを送信します。

```

Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
    "s1-c1" #1: transition from state STATE_MAIN_I3 to
    state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
    STATE_MAIN_I4: ISAKMP SA established
    {auth=OAKLEY_PRESHARED_KEY
    cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
    Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
    initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
    {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
    pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
    ignoring informational payload, type INVALID_ID_INFORMATION
    msgid=00000000

```

Cisco

```

Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
    IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
    + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
    + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
    + NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
    IP = 10.115.199.191, Received encrypted Oakley Main Mode
    packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
    Message (msgid=0) with payloads : HDR + NOTIFY (11)
    + NONE (0) total length : 80

```

```
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, ERROR, had problems decrypting
packet, probably due to mismatched pre-shared key.
Aborting
```

成功するネゴシエーションのためのパケットのキャプチャ

以下に、NSX Edge と Cisco デバイスの間で正常に行われたネゴシエーションでのパケット キャプチャ セッションを示します。

No.	Time	Source	Destination	Protocol	Info
9203	768.394800	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

Frame 9203 (190 bytes on wire, 190 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 0000000000000000
 Next payload: Security Association (1)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x00
 Message ID: 0x00000000
 Length: 148
 Security Association payload
 Next payload: Vendor ID (13)
 Payload length: 84
 Domain of interpretation: IPSEC (1)
 Situation: IDENTITY (1)
 Proposal payload # 0
 Next payload: NONE (0)
 Payload length: 72
 Proposal number: 0
 Protocol ID: ISAKMP (1)
 SPI Size: 0
 Proposal transforms: 2
 Transform payload # 0
 Next payload: Transform (3)
 Payload length: 32
 Transform number: 0
 Transform ID: KEY_IKE (1)
 Life-Type (11): Seconds (1)
 Life-Duration (12): Duration-Value (28800)
 Encryption-Algorithm (1): 3DES-CBC (5)
 Hash-Algorithm (2): SHA (2)
 Authentication-Method (3): PSK (1)
 Group-Description (4): 1536 bit MODP group (5)
 Transform payload # 1
 Next payload: NONE (0)


```

    Payload length: 32
    Transform number: 1
    Transform ID: KEY_IKE (1)
    Life-Type (11): Seconds (1)
    Life-Duration (12): Duration-Value (28800)
    Encryption-Algorithm (1): 3DES-CBC (5)
    Hash-Algorithm (2): SHA (2)
    Authentication-Method (3): PSK (1)
    Group-Description (4): Alternate 1024-bit MODP group (2)
Vendor ID: 4F456C6A405D72544D42754D
    Next payload: Vendor ID (13)
    Payload length: 16
    Vendor ID: 4F456C6A405D72544D42754D
Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

```

No.	Time	Source	Destination	Protocol Info
9204	768.395550	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
    Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
    Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 92585D2D797E9C52
    Responder cookie: 34704CFC8C8DBD09
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags: 0x00
    Message ID: 0x00000000
    Length: 104
    Security Association payload
        Next payload: Vendor ID (13)
        Payload length: 52
        Domain of interpretation: IPSEC (1)
        Situation: IDENTITY (1)
    Proposal payload # 1
        Next payload: NONE (0)
        Payload length: 40
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
    Transform payload # 1
        Next payload: NONE (0)
        Payload length: 32
        Transform number: 1
        Transform ID: KEY_IKE (1)
        Encryption-Algorithm (1): 3DES-CBC (5)

```

```

    Hash-Algorithm (2): SHA (2)
    Group-Description (4): Alternate 1024-bit MODP group (2)
    Authentication-Method (3): PSK (1)
    Life-Type (11): Seconds (1)
    Life-Duration (12): Duration-Value (28800)
Vendor ID: Microsoft L2TP/IPSec VPN Client
Next payload: NONE (0)
Payload length: 24
Vendor ID: Microsoft L2TP/IPSec VPN Client

```

No.	Time	Source	Destination	Protocol Info
9205	768.399599	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

```

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data

```

No.	Time	Source	Destination	Protocol Info
9206	768.401192	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9206 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00

```

```

Message ID: 0x00000000
Length: 256
Key Exchange payload
  Next payload: Nonce (10)
  Payload length: 132
  Key Exchange Data (128 bytes / 1024 bits)
Nonce payload
  Next payload: Vendor ID (13)
  Payload length: 24
  Nonce Data
Vendor ID: CISCO-UNITY-1.0
  Next payload: Vendor ID (13)
  Payload length: 20
  Vendor ID: CISCO-UNITY-1.0
Vendor ID: draft-beaulieu-ike-xauth-02.txt
  Next payload: Vendor ID (13)
  Payload length: 12
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
  Next payload: Vendor ID (13)
  Payload length: 20
  Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
Vendor ID: CISCO-CONCENTRATOR
  Next payload: NONE (0)
  Payload length: 20
  Vendor ID: CISCO-CONCENTRATOR

```

No.	Time	Source	Destination	Protocol	Info
9207	768.404990	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

```

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
  Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
  Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
  Encrypted payload (40 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9208	768.405921	10.20.131.62	10.20.129.80	ISAKMP	Identity Protection (Main Mode)

```

Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
  Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),

```

Dst: 10.20.129.80 (10.20.129.80)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x01
 Message ID: 0x00000000
 Length: 84
 Encrypted payload (56 bytes)

No.	Time	Source	Destination	Protocol	Info
9209	768.409799	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

Frame 9209 (334 bytes on wire, 334 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

No.	Time	Source	Destination	Protocol	Info
9210	768.411797	10.20.131.62	10.20.129.80	ISAKMP	Quick Mode

Frame 9210 (334 bytes on wire, 334 bytes captured)
 Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

No.	Time	Source	Destination	Protocol	Info
9211	768.437057	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```
Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 52
  Encrypted payload (24 bytes)
```