

Cross-vCenter NSX インストール ガイド

Update 9

更新日：2020 年 2 月 21 日

VMware NSX Data Center for vSphere 6.3



vmware®

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

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 - 2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

1	Cross-vCenter インストール ガイド	5
2	NSX for vSphere の概要	6
	NSX for vSphere コンポーネント	7
	データ プレーン	8
	制御プレーン	9
	管理プレーン	10
	使用プラットフォーム	10
	NSX Edge	10
	NSX Services	13
3	Cross-vCenter Networking and Security の概要	15
	Cross-vCenter NSX の利点	15
	Cross-vCenter NSX の仕組み	16
	Cross-vCenter NSX での NSX Services のサポート マトリックス	17
	ユニバーサル コントローラ クラス	19
	ユニバーサル トランスポート ゾーン	19
	ユニバーサル論理スイッチ	19
	ユニバーサル分散論理ルーター	19
	ユニバーサル ファイアウォール ルール	20
	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	21
	Cross-vCenter NSX トポロジ	21
	複数サイトおよび単一サイトの Cross-vCenter NSX	21
	Local Egress (ローカル出力方向)	23
	NSX Manager ロールの変更	24
4	インストールの準備	26
	NSX のシステム要件	26
	NSX for vSphere で必要となるポートおよびプロトコル	28
	NSX と vSphere Distributed Switch	31
	例 : vSphere Distributed Switch の操作	33
	NSX のインストール ワークフローとトポロジの例	40
	Cross-vCenter NSX および拡張リンク モード	42
5	プライマリおよびセカンダリ NSX Manager のタスク	43
	NSX Manager 仮想アプライアンスのインストール	43
	Single Sign-On の設定	48
	NSX Manager への vCenter Server の登録	50

- NSX Manager の Syslog サーバの設定 52
- NSX for vSphere のライセンスのインストールと割り当て 52
- ファイアウォールによる保護からの仮想マシンの除外 54

6 プライマリ NSX Manager の設定 56

- プライマリ NSX Manager への NSX Controller のデプロイ 56
- プライマリ NSX Manager でのホストの準備 60
- プライマリ NSX Manager からの VXLAN の設定 63
- プライマリ NSX Manager へのセグメント ID プールとマルチキャスト アドレスの割り当て 67
- NSX Manager へのプライマリ ロールの割り当て 69
- プライマリ NSX Manager でのユニバーサル セグメント ID プールとユニバーサル マルチキャスト アドレスの割り当て 70
- プライマリ NSX Manager でのユニバーサル トランスポート ゾーンの追加 72
- プライマリ NSX Manager でのユニバーサル論理スイッチの追加 73
- 論理スイッチへの仮想マシンの接続 75
- プライマリ NSX Manager でのユニバーサル分散論理ルーターの追加 75

7 セカンダリ NSX Manager の設定 88

- セカンダリ NSX Manager の追加 88
- セカンダリ NSX Manager でのホストの準備 90
- セカンダリ NSX Manager からの VXLAN の設定 92
- セカンダリ NSX Manager へのセグメント ID プールとマルチキャスト アドレスの割り当て 94
- ユニバーサル トランスポート ゾーンへのクラスタの追加 94

8 プライマリおよびセカンダリ NSX Manager 設定後の作業 96

9 NSX コンポーネントのアンインストール 97

- NSX を使用するクラスタからのホストの削除 97
- NSX Edge Services Gateway または分散論理ルーターのアンインストール 98
- 論理スイッチのアンインストール 98
- ホスト クラスタからの NSX のアンインストール 99
- NSX 環境の安全な削除 100

Cross-vCenter インストール ガイド

1

本書では、Cross-vCenter NSX 環境に VMware NSX[®] for vSphere[®] をインストール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、Cross-vCenter NSX 環境で NSX をインストール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。本書は、VMware ESXi、vCenter Server、vSphere Web Client を含む VMware vSphere についての知識があることを前提としています。

VMware の技術ドキュメントの用語集

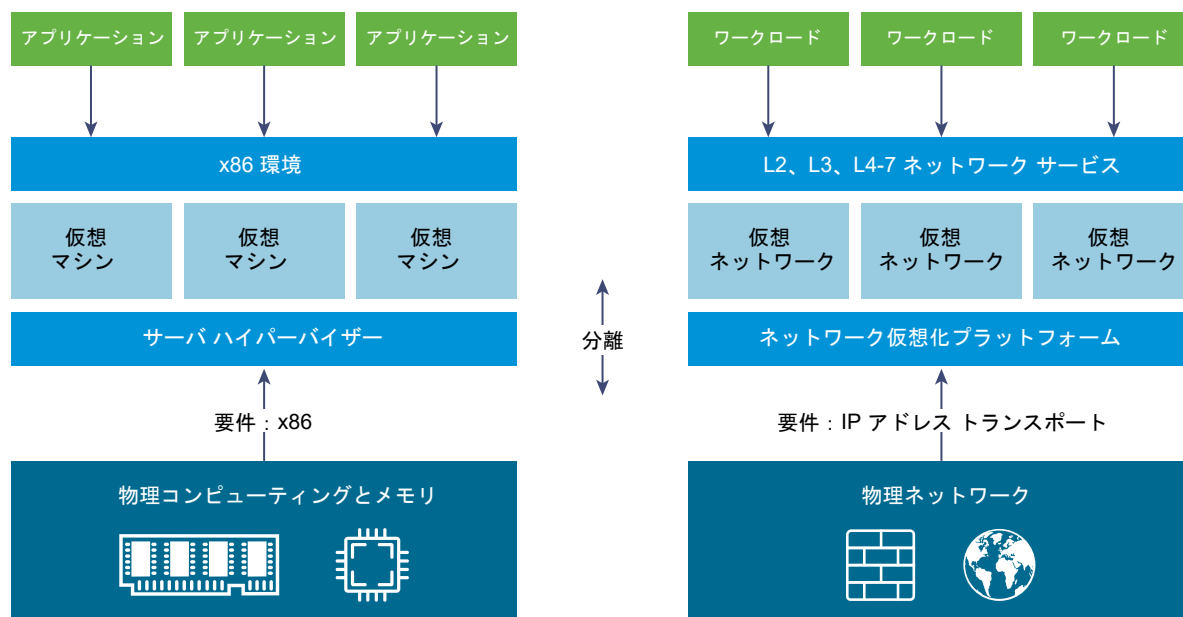
VMware は、新しい用語を集めた用語集を提供しています。当社の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

NSX for vSphere の概要

2

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。NSX for vSphere は、SDDC アーキテクチャの主要製品です。NSX for vSphere 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。サーバ仮想化では、ソフトウェア ベースの仮想マシンの作成、削除、リストア、およびスナップショットの作成をプログラムによって行います。NSX for vSphere のネットワーク仮想化は、ほぼ同じ方法で、ソフトウェア ベースの仮想ネットワークを作成、削除、リストア、およびスナップショットの作成を行います。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 マネージャが桁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 for vSphere 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無停止ソリューションです。つまり、NSX for vSphere 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るのと同様に、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。

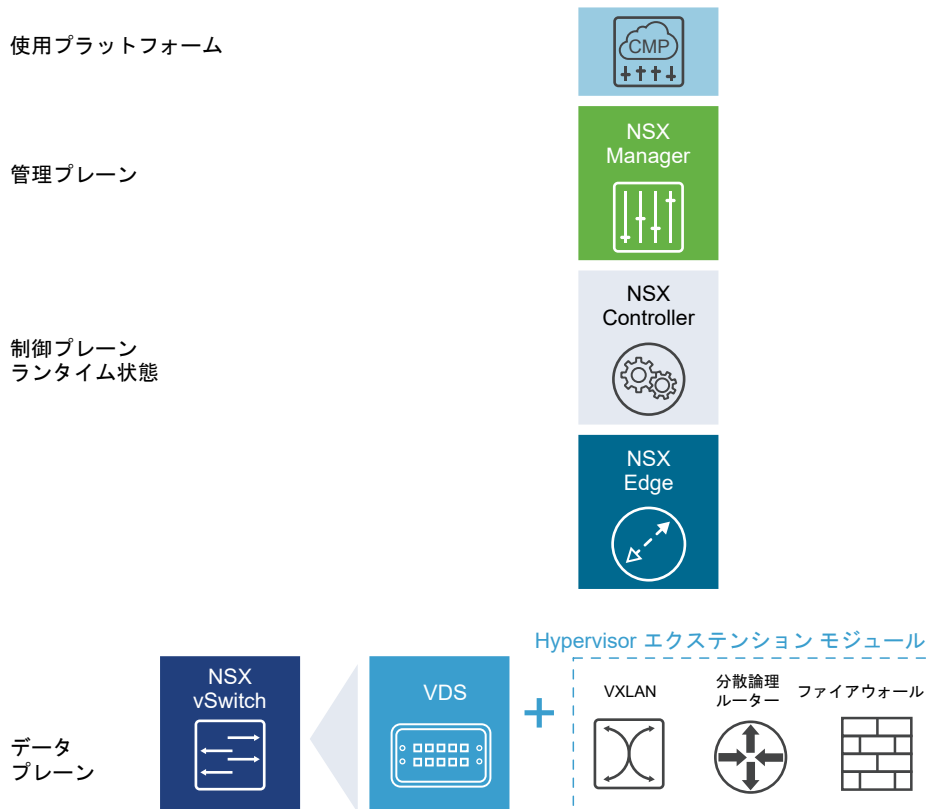
NSX for vSphere は、vSphere Web Client、コマンドライン インターフェイス (CLI)、および REST API を使用して設定できます。

この章には、次のトピックが含まれています。

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

NSX for vSphere コンポーネント

このセクションでは、NSX for vSphere 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 for vSphere のコンポーネントではありませんが、NSX for vSphere 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、スケーラビリティ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 プレーン問題」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 プレーン問題では、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。

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

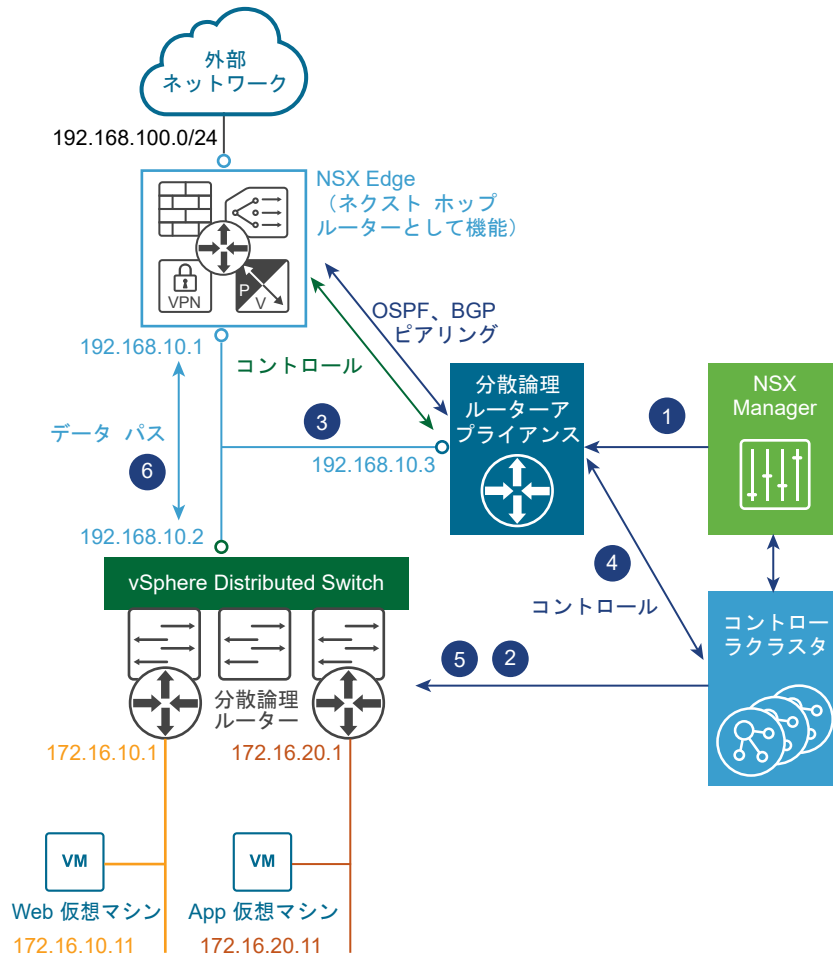
分散論理ルーターは、テナント IP アドレス空間とデータ パス分離による水平方向の分散ルーティングを提供します。複数のサブネットにわたっている同一ホスト上に存在する仮想マシンまたはワークロードは、従来のルーティング インターフェイスをトラバースすることなく相互に通信できます。

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、ESXi 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 2-1. 論理ルーティング コンポーネント



- 1 NSX Manager のユーザー インターフェイス（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、このルートのアドバタイズが 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。多くの環境では、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、次の機能をサービスとして提供します。

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、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、障害の隔離、および IP アドレス重複の回避を実現するには、アプリケーションとテナントは分離している必要があります。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、論理スイッチに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型であるため、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、East-West 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 North-South 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、動的な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分散ファイアウォール 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 Server 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。この情報によって、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が可能になります。

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、地理的な境界を越えて同じ IP アドレスを保持しながら、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。負荷の配分がユーザーにとって透過的になるように、受信サービス リクエストを複数のサーバ間で均等に配分します。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。

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

3

NSX 6.2 以降では、1 つのプライマリ NSX Manager から Cross-vCenter NSX 環境を管理できます。

この章には、次のトピックが含まれています。

- [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](#)
- [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 Server 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 以降では、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 Server 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上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 以降でサポートされています。

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。

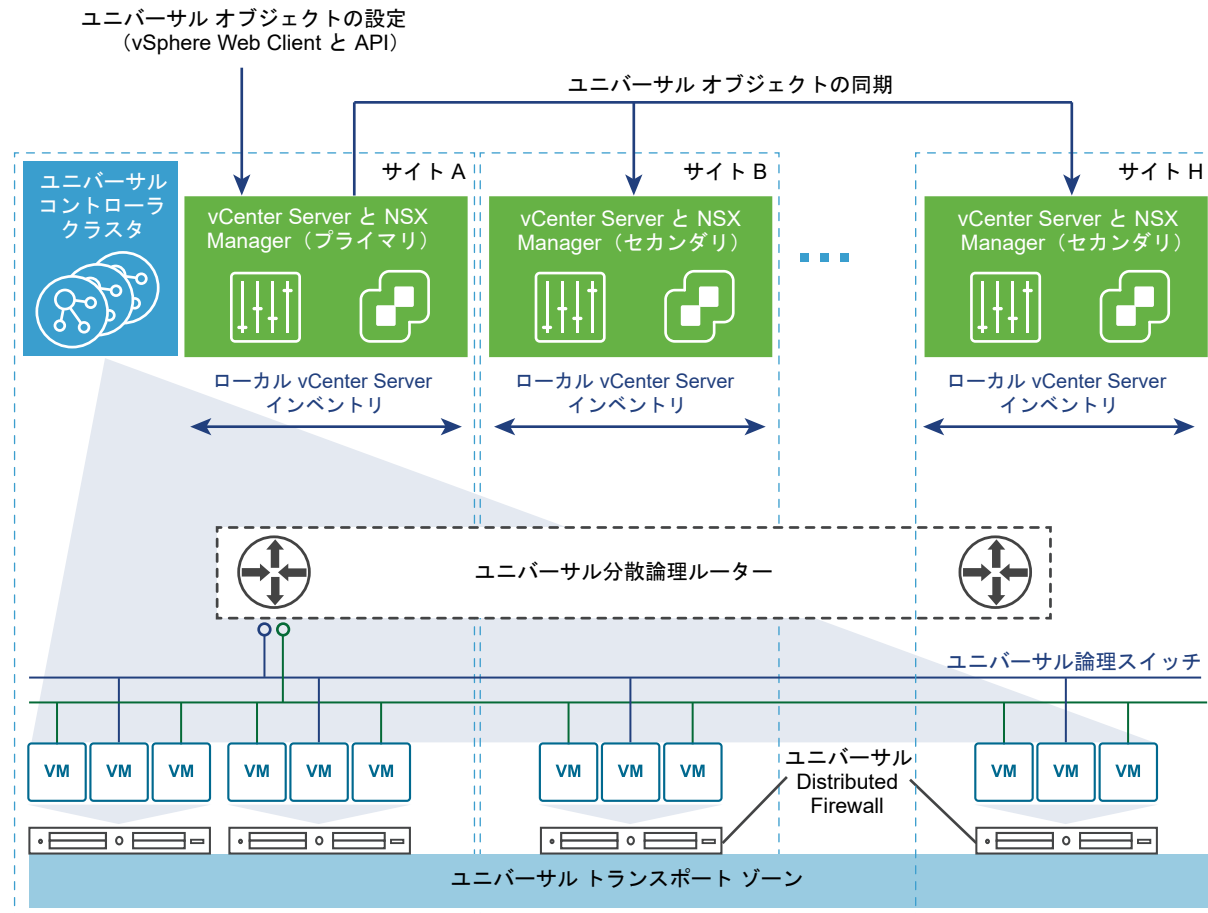
プライマリ NSX Manager は、Cross-vCenter NSX 環境の制御プレーンを提供するユニバーサル コントローラ クラスタをデプロイするために使用されます。セカンダリ NSX Manager には、各自のコントローラ クラスタはありません。

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。ユニバーサル同期で使用できないサービスを NSX Manager のローカルで使用するよう設定できます。

表 3-1. Cross-vCenter NSX での NSX Services のサポート マトリックス

NSX Service	詳細	Cross-vCenter NSX 同期のサポート
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	分散論理ルーター	はい
	分散論理ルーター アプライアンス	仕様により未サポート。ユニバーサル分散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、Local Egress（ローカル出力方向）が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	分散ファイアウォール	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
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
	セキュリティ グループ	はい。メンバーシップの設定は、ユニバーサル以外のセキュリティ グループのメンバーシップと異なります。詳細については、『NSX 管理ガイド』の「セキュリティ グループの作成」を参照してください。
	サービス	はい
	サービス グループ	はい
セキュリティ タグ		はい
ハードウェア ゲートウェイ (ハードウェア VTEP)		いいえ。詳細については、『NSX 管理ガイド』の「ハードウェア ゲートウェイのサンプル構成」を参照してください。

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、コントロール 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ル 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 環境の分散ファイアウォールにより、使用環境内のすべての vCenter Server に適用されるルールを統合管理できます。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することができます。

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。この場合、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する必要があります。あるいは、ステージング サーバが 1 台の 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 サーバから本番サーバに移動する必要があります。分散ファイアウォールでは、プライマリ NSX Manager に対して定義したファイアウォール ポリシーを最大で 7 台のセカンダリ 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分散ファイアウォール 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 つ以上のユニバーサル L2 ルール セクションと 1 つ以上のユニバーサル L3 ルール セクションを作成できます。ユニバーサル セクションは、常にプライマリおよびセカンダリ NSX Manager の最上部に表示されます。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。

次の分散ファイアウォール機能は、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 セクションに分散ファイアウォール 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 セクションの分散ファイアウォール 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します。

ユニバーサル セキュリティ グループ (USG) には、次のものを含めることができます。

- 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 セキュリティ グループ
- ユニバーサル セキュリティ タグ
- 動的基準

ユニバーサルなネットワーク オブジェクトとセキュリティ オブジェクトは、プライマリ NSX Manager でのみ作成、削除、更新ができます。セカンダリ NSX Manager では読み取りのみが可能です。ユニバーサル同期サービスでは、vCenter Server 全体で即座にオブジェクトを同期するだけでなく、強制同期を使用して必要なときに同期することもできます。

ユニバーサル セキュリティ グループは、複数の Cross-vCenter NSX 環境と Cross-vCenter NSX アクティブ/スタンバイ環境の 2 種類の導入環境で使用できます。Cross-vCenter NSX アクティブ/スタンバイ環境では、一度に 1 つのサイトのみが稼働し、残りのサイトはスタンバイ状態になります。動的メンバーシップが定義されたユニバーサル セキュリティ グループは、アクティブ/スタンバイ環境でのみ設定できます。この動的メンバーシップは、ユニバーサル セキュリティ タグに基づいた仮想マシン名の静的メンバーシップをベースとしています。一度作成されたユニバーサル セキュリティ グループを編集して、アクティブ/スタンバイ シナリオ機能向けに有効または無効にできません。メンバーシップには、含まれているオブジェクトのみが定義されます。除外し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、NSX Manager にローカルとなります。

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 Server 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SPORT ゾーン。
- ユニバーサル トランSPORT 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 3-1. 単一サイト内の Cross-vCenter NSX

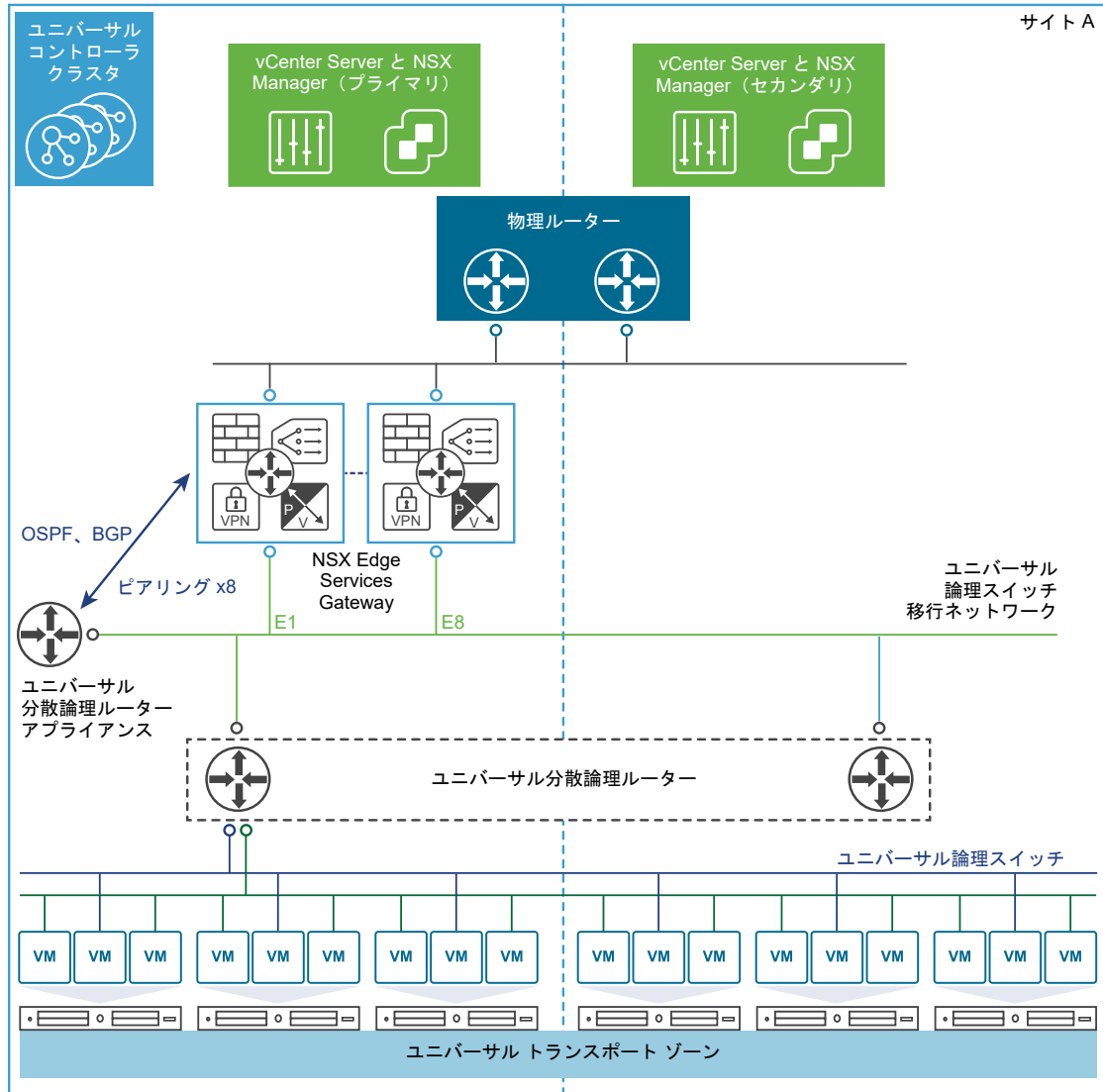
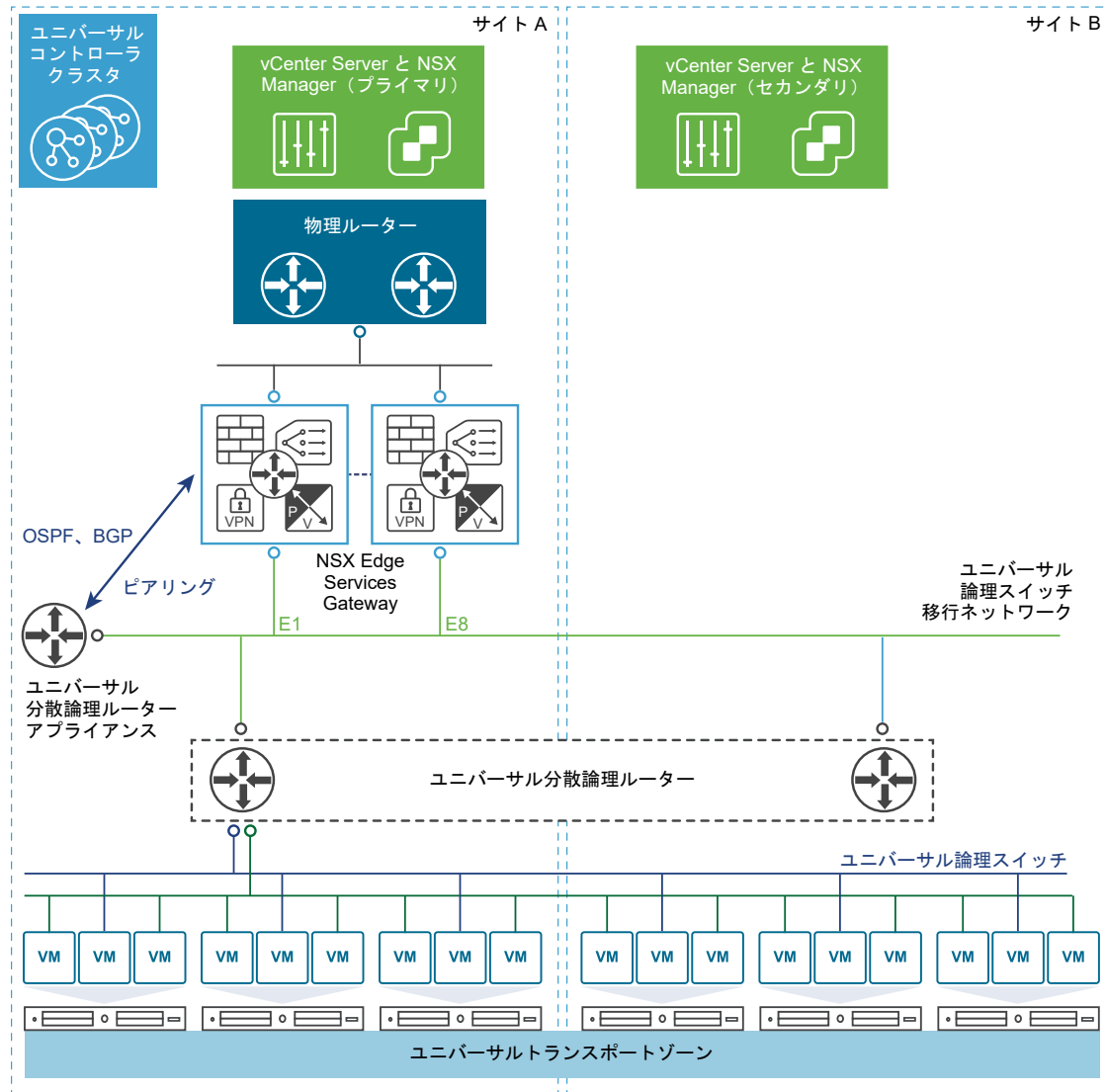


図 3-2. 2 つのサイトにまたがる Cross-vCenter NSX

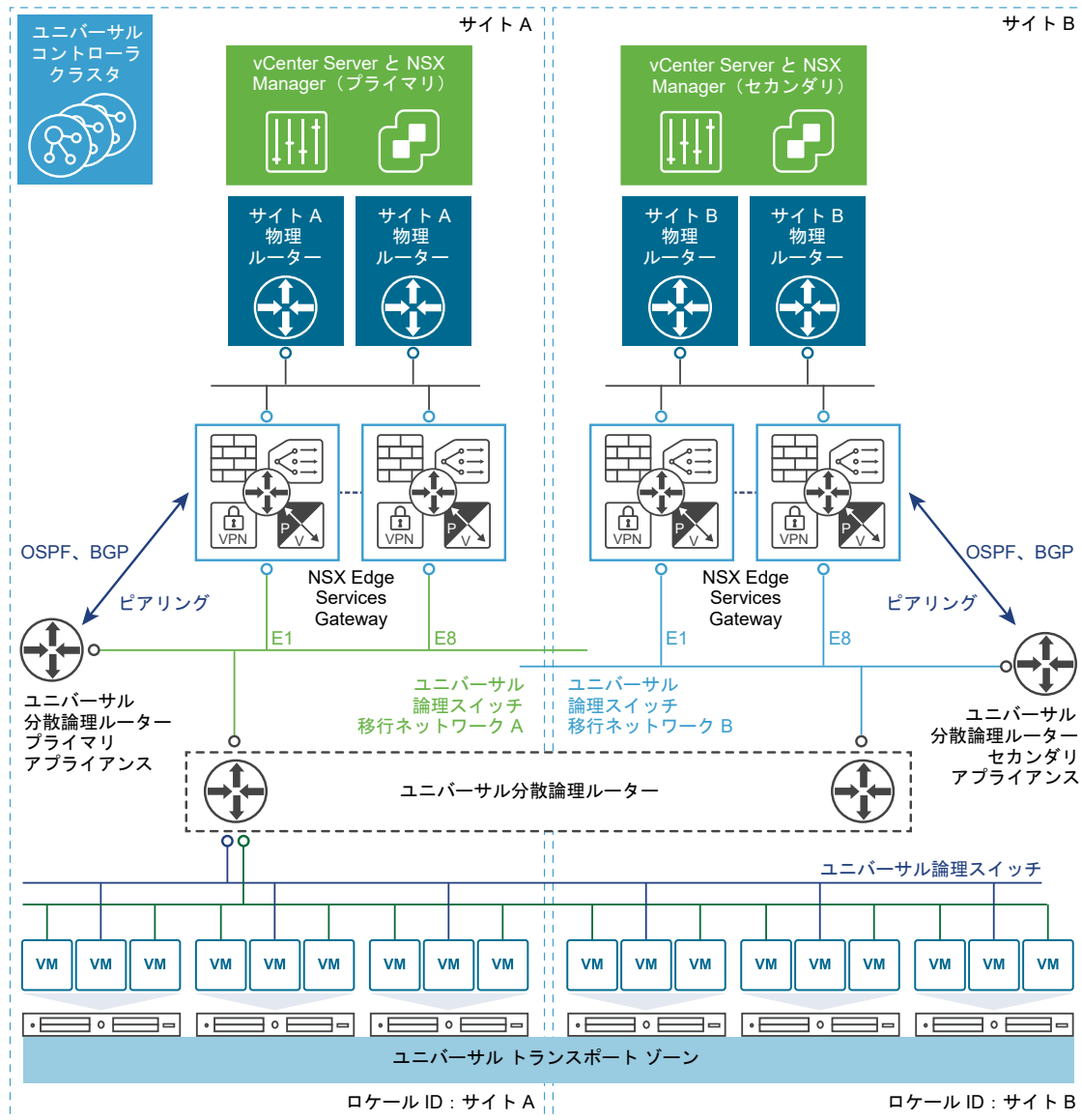


Local Egress（ローカル出力方向）

マルチサイト Cross-vCenter NSX 環境のすべてのサイトは、出力方向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、出力方向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（ローカル出力方向）機能を有効にする必要があります。

Local Egress 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（ローカル出力方向）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（ローカル出力方向）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 を持つルートを送信します。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。

インストールの準備

4

このセクションでは、NSX for vSphere のシステム要件と、開く必要のあるポートについて説明します。

この章には、次のトピックが含まれています。

- [NSX のシステム要件](#)
- [NSX for vSphere で必要となるポートおよびプロトコル](#)
- [NSX と vSphere Distributed Switch](#)
- [例：vSphere Distributed Switch の操作](#)
- [NSX のインストール ワークフローとトポロジの例](#)
- [Cross-vCenter NSX および拡張リンク モード](#)

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。vCenter Server 1 台あたり NSX Manager を 1 台、ESXi™ ホスト 1 台あたりゲスト イントロスペクションインスタンス 1 つ、1 つのデータセンターあたり複数の NSX Edge インスタンスをインストールできます。

ハードウェア

次の表は、NSX アプライアンスのハードウェア要件です。

表 4-1. アプライアンスのハードウェア要件

アプライアンス	メモリ	vCPU	ディスク容量
NSX Manager	16 GB (大規模な NSX 環境の場合は 24 GB)	4 (大規模な NSX 環境の場合は 8)	60 GB
NSX Controller	4 GB	4	28 GB

表 4-1. アプライアンスのハードウェア要件 (続き)

アプライアンス	メモリ	vCPU	ディスク容量
NSX Edge	[Compact]: 512 MB [Large]: 1 GB [Quad Large]: 2 GB [X-Large]: 8 GB	[Compact]: 1 [Large]: 2 [Quad Large]: 4 [X-Large]: 6	[Compact, Large]: 584 MB のディスク 1 台 + 512 MB のディスク 1 台 [Quad Large]: 584 MB のディスク 1 台 + 512 MB のディスク 2 台 [XLarge]: 584 MB のディスク 1 台 + 2 GB のディスク 1 台 + 512 MB のディスク 1 台
ゲスト イントロス ペクション	2 GB	2	5 GB (プロビジョニング後の容量は 6.26 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、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 に増強してください。

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。

ゲスト イントロスペクションの場合、ゲスト イントロスペクション アプライアンスのプロビジョニング後の容量は 6.26 GB と表示されます。これは、クラスタ内の複数のホストが 1 つのストレージを共有している場合、vSphere ESX Agent Manager が高速クローン用にサービス仮想マシンのスナップショットを作成するためです。このオプションを ESX Agent Manager で無効にする方法については、*ESX Agent Manager* のドキュメントを参照してください。

ネットワークの遅延

コンポーネント間のネットワーク遅延が、以下の最大遅延時間内であることを確認する必要があります。

表 4-2. コンポーネント間のネットワーク遅延の最大値

コンポーネント	遅延の最大値
NSX Manager と NSX Controller	150 ms RTT
NSX Manager と ESXi ホスト	150 ms RTT
NSX Manager と vCenter Server システム	150 ms RTT
Cross-vCenter NSX 環境での NSX Manager と NSX Manager	150 ms RTT
NSX Controller と ESXi ホスト	150 ms RTT

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、アップグレードする NSX バージョンのリリース ノートを参照してください。リリース ノートは、NSX for vSphere のドキュメント サイト <https://docs.vmware.com/jp/VMware-NSX-for-vSphere/index.html> でご覧いただけます。

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

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 ネットワークとセキュリティ (<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

NSX 環境を管理するには、次が必要です。

- 正引き/逆引きの名前解決。これは、vSphere インベントリに ESXi ホストを名前を追加した場合に必要です。この機能がないと、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には、Web ブラウザで Cookie を有効にする必要があります。
- NSX Manager と ESXi ホスト、vCenter Server、デプロイする NSX アプライアンスの間で、ポート 443 を開く必要があります。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 for vSphere で必要となるポートおよびプロトコル

NSX for vSphere 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。

注： Cross-vCenter NSX 環境で vCenter Server システムが拡張リンク モードになっている場合、vCenter Server システムから NSX Manager を管理するには、それぞれの NSX Manager アプライアンスが環境内の vCenter Server システムに接続している必要があります。

表 4-3. NSX for vSphere 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	いいえ	はい	PAM 認証
クライアント PC	NSX Manager	443	TCP	NSX Manager VIB アクセス	いいえ	いいえ	PAM 認証
ESXi ホスト	vCenter Server	443	TCP	ESXi ホストの準備	いいえ	いいえ	
vCenter Server	ESXi ホスト	443	TCP	ESXi ホストの準備	いいえ	いいえ	
ESXi ホスト	NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	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	いいえ	はい	
NSX Controller	NSX Controller	2878、 2888、 3888	TCP	コントローラ クラス タ - 状態同期	いいえ	はい	IPsec
NSX Controller	NSX Controller	7777	TCP	内部コントローラ RPC ポート	いいえ	はい	IPsec
NSX Controller	NSX Controller	30865	TCP	コントローラ クラス タ - 状態同期	いいえ	はい	IPsec
NSX Manager	NSX Controller	443	TCP	コントローラと Manager の通信	いいえ	はい	ユーザー/パスワード
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	いいえ	はい	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	いいえ	はい	
NSX Manager	ESXi ホスト	443	TCP	管理とプロビジョニン グ接続	いいえ	はい	
NSX Manager	ESXi ホスト	902	TCP	管理とプロビジョニン グ接続	いいえ	はい	
NSX Manager	DNS サーバ	53	TCP	DNS クライアント接 続	いいえ	いいえ	
NSX Manager	DNS サーバ	53	UDP	DNS クライアント接 続	いいえ	いいえ	
NSX Manager	Syslog サーバ	514	TCP	Syslog 接続	いいえ	いいえ	
NSX Manager	Syslog サーバ	514	UDP	Syslog 接続	いいえ	いいえ	
NSX Manager	NTP タイム サー バ	123	TCP	NTP クライアント接 続	いいえ	はい	
NSX Manager	NTP タイム サー バ	123	UDP	NTP クライアント接 続	いいえ	はい	
vCenter Server	NSX Manager	80	TCP	ホストの準備	いいえ	はい	
REST Client	NSX Manager	443	TCP	NSX Manager REST API	いいえ	はい	ユーザー/パスワード

表 4-3. NSX for vSphere 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
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	いいえ	はい	
ESXi ホスト	ESXi ホスト	6999	UDP	VLAN LIF 上の ARP	いいえ	はい	
ESXi ホスト	NSX Manager	8301, 8302	UDP	分散仮想スイッチ同期	いいえ	はい	
NSX Manager	ESXi ホスト	8301, 8302	UDP	分散仮想スイッチ同期	いいえ	はい	
ゲスト イントロセクション仮想マシン	NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	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	いいえ	はい	
プライマリ NSX Manager	vCenter Server	443	TCP	vSphere API	いいえ	はい	
セカンダリ NSX Manager	vCenter Server	443	TCP	vSphere API	いいえ	はい	
プライマリ NSX Manager	NSX ユニバーサル コントローラ クラスター	443	TCP	NSX Controller REST API	いいえ	はい	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 クラスター	443	TCP	NSX Controller REST API	いいえ	はい	ユーザー/パスワード
ESXi ホスト	NSX ユニバーサル コントローラ クラスター	1234	TCP	NSX 制御プレーン プロトコル	いいえ	はい	
ESXi ホスト	プライマリ NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	RabbitMQ ユーザー/パスワード
ESXi ホスト	セカンダリ NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	RabbitMQ ユーザー/パスワード

NSX と vSphere Distributed Switch

NSX ドメインにおける NSX vSwitch は、サーバのハイパーバイザーで動作するソフトウェアであり、サーバと物理ネットワーク間にソフトウェア抽象レイヤーを形成します。

NSX vSwitch は、トップオブラック (ToR) の物理スイッチとホストを接続するためのアップリンクを提供する、vSphere Distributed Switch (VDS) をベースとしています。ベスト プラクティスとして、vSphere Distributed Switch 計画と準備を行ってから、NSX for vSphere をインストールすることをお勧めします。

NSX サービスは、vSphere の標準スイッチではサポートされません。NSX サービスおよび機能を使用するには、仮想マシンのワークロードが vSphere Distributed Switch に接続されている必要があります。

1 台のホストを複数の分散仮想スイッチ (VDS) に接続できます。1 つの VDS を、複数のクラスタの複数のホストにまたがって配置できます。NSX に参加する各ホスト クラスタでは、クラスタ内の全ホストが共通の VDS に接続している必要があります。

たとえば、Host1 と Host2 を含むクラスタがあるとします。Host1 は仮想スイッチの VDS1 と VDS2 に接続されています。Host2 は VDS1 と VDS3 に接続されています。NSX 用にクラスタを準備するときは、NSX をクラスタ上の VDS1 にのみ関連付けることができます。クラスタに別のホスト (Host3) を追加しても、Host3 が VDS1 に接続されていない場合、それは無効の構成であり、Host3 は NSX 機能を使用できる状態にはなりません。

多くの場合、デプロイを簡素化するために、VDS のいくつかが複数のクラスタにわたって配置されている場合でも、ホストの各クラスタは 1 つの VDS にのみ関連付けられます。たとえば、vCenter Server に次のホスト クラスタが含まれているとします。

- アプリ層ホスト用のコンピューティング クラスタ A
- Web 層ホスト用のコンピューティング クラスタ B
- 管理および Edge ホスト用の管理および Edge クラスタ

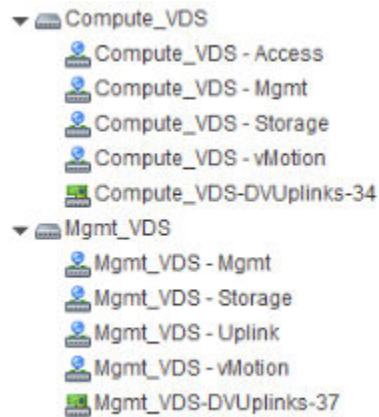
次の画面は、これらのクラスタが vCenter Server でどのように見えるかを示しています。



このようなクラスタ設計では、Compute_VDS と Mgmt_VDS と呼ばれる 2 つの VDS が存在することがあります。Compute_VDS は両方のコンピューティング クラスタにまたがって配置され、Mgmt_VDS は管理および Edge クラスタにのみ関連付けられます。

各 VDS には、送信する必要があるさまざまな種類のトラフィックに対応するために、分散ポート グループが含まれています。一般的なトラフィック タイプには、管理、ストレージ、vMotion があります。多くの場合、アップリンク ポートとアクセス ポートも必要です。通常は、各 VDS でトラフィック タイプごとに 1 つのポート グループが作成されます。

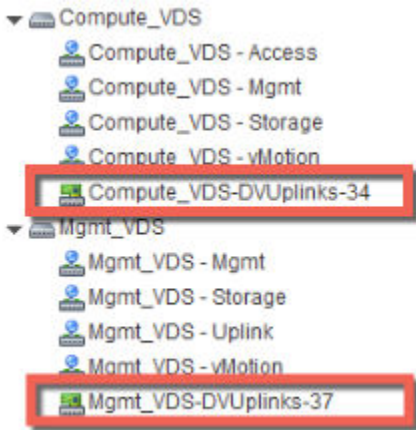
たとえば次の画面は、これらの Distributed Switch とポートが vCenter Server でどのように見えるかを示しています。



各ポート グループは、必要に応じて VLAN ID を使って設定できます。次のリストは、さまざまなトラフィック タイプを論理的に分離するために、VLAN を分散ポート グループにどのように関連付けることができるかを示した例です。

- Compute_VDS - アクセス---VLAN 130
- Compute_VDS - 管理---VLAN 210
- Compute_VDS - ストレージ---VLAN 520
- Compute_VDS - vMotion---VLAN 530
- Mgmt_VDS - アップリンク---VLAN 100
- Mgmt_VDS - 管理---VLAN 110
- Mgmt_VDS - ストレージ---VLAN 420
- Mgmt_VDS - vMotion---VLAN 430

DVUplinks ポート グループは、VDS を作成すると自動的に作成される VLAN トランクであり、トランク ポートとして、タグ付きフレームを送受信します。デフォルトでは、すべての VLAN ID (0 から 4094) を送信します。つまり、すべての VLAN ID のトラフィックが、DVUplink スロットに関連付けられた VMNIC ネットワーク アダプタを通過できますが、Distributed Switch が、トラフィックを受信するポート グループを決定するため、これらのトラフィックはハイパーバイザー ホストによってフィルタリングされます。



既存の vCenter Server 環境に Distributed Switch ではなく標準仮想スイッチが含まれている場合は、ホストを Distributed Switch に移行できます。

例：vSphere Distributed Switch の操作

この例では、新しい vSphere Distributed Switch (VDS) を作成する方法、管理、ストレージ、および vMotion トラフィック タイプのポート グループを追加する方法、標準の vSwitch 上のホストを新しい Distributed Switch に移行する方法を示しています。

ここでは手順の説明のため、1 つの例を示すのみになります。VDS の物理アップリンクおよび論理アップリンクに関する考慮事項の詳細については、『VMware NSX for vSphere Network Virtualization Design Guide』(VMware NSX for vSphere ネットワーク仮想化設計ガイド) (<https://communities.vmware.com/docs/DOC-27683>) を参照してください。

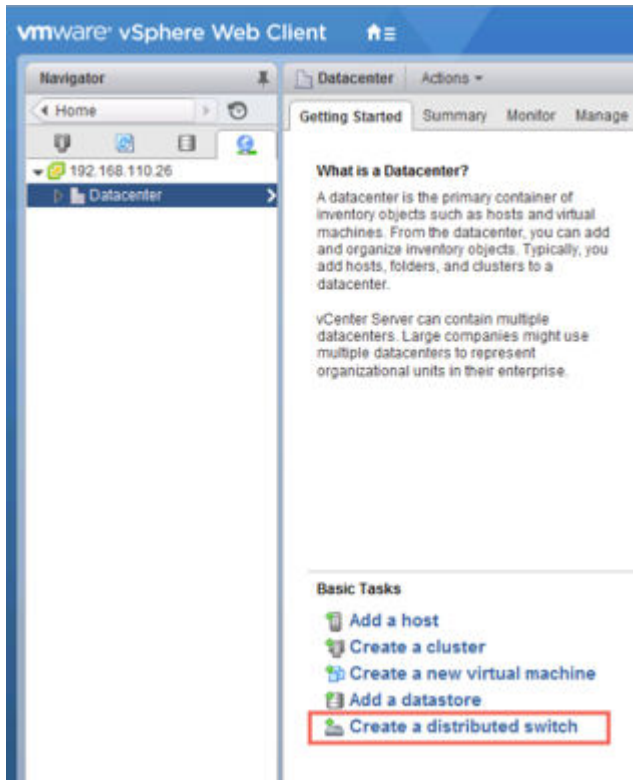
前提条件

この例は、vSphere Distributed Switch に接続する各 ESX ホストに、物理スイッチへの接続 (vmnic アップリンク) が少なくとも 1 つ存在することを前提とします。Distributed Switch および NSX VXLAN のトラフィックに対してこのアップリンクを使用できます。

手順

- 1 vSphere Web Client で、データセンターに移動します。

- 2 [Distributed Switch の作成 (Create a Distributed Switch)] をクリックします。



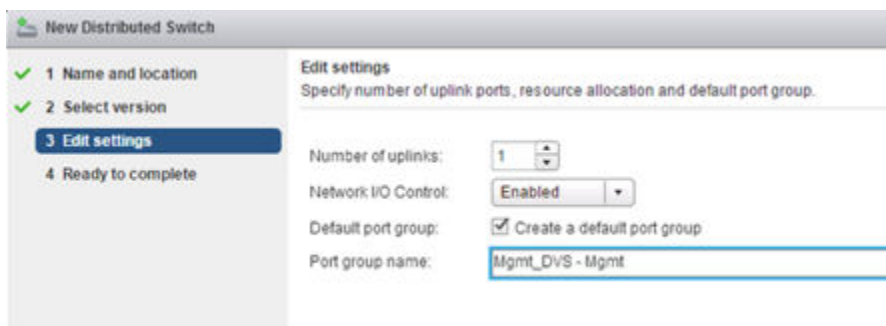
- 3 このスイッチに関連付けるホスト クラスタに基づいて、スイッチにわかりやすい名前を付けます。

たとえば、Distributed Switch をデータセンター管理ホストのクラスタに関連付ける場合、スイッチに VDS_Mgmt という名前を付けることができます。

- 4 Distributed Switch に少なくとも 1 つのアップリンクを指定し、IO コントロールを有効にしたまま、デフォルトのポート グループにわかりやすい名前を付けます。デフォルトのポート グループを作成することは必須ではありません。ポート グループは後で手動で作成できます。

デフォルトでは、4 つのアップリンクが作成されます。Distributed Switch 設計を反映するようにアップリンク数を調整します。通常、必要なアップリンクの数は、VDS に割り当てる物理 NIC の数と同じです。

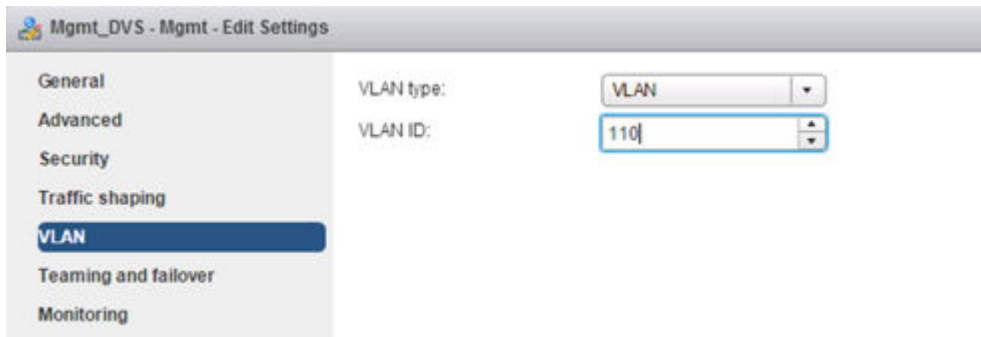
以下の画面は、管理ホスト クラスタでの管理トラフィックの設定例を示しています。



デフォルト ポート グループは、このスイッチに含まれるポート グループの 1 つです。スイッチの作成後に、異なるトラフィック タイプのポート グループを追加することができます。新しい Distributed Switch を作成する場合は、[デフォルトのポート グループの作成 (Create a default port group)] オプションの選択を解除することもできます。実際にはこれがベスト プラクティスになる場合があります。ポート グループを作成する場合は明示的に示すことをお勧めします。

- 5 (オプション) [新しい Distributed Switch] ウィザードが完了したら、デフォルト ポート グループを管理トラフィック用の適切な VLAN に配置するようにデフォルト ポート グループの設定を編集します。

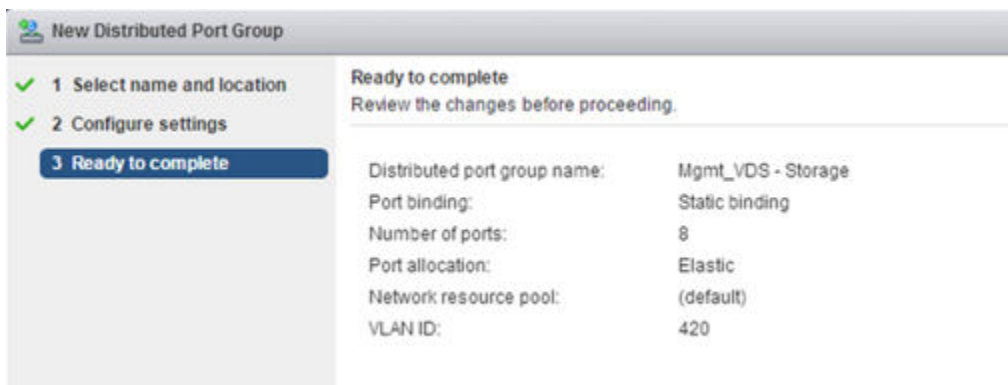
たとえば、ホストの管理インターフェイスが VLAN 110 内にある場合、デフォルト ポート グループを VLAN 110 に配置します。ホストの管理インターフェイスが VLAN 内にはない場合は、この手順をスキップします。



- 6 [新しい Distributed Switch] ウィザードが完了したら、Distributed Switch を右クリックし、[新規分散ポートグループ (New Distributed Port Group)] を選択します。

この手順をトラフィック タイプごとに繰り返し、各ポート グループにわかりやすい名前を付けて、導入環境のトラフィック分離要件に基づいて適切な VLAN ID を設定します。

ストレージ用のグループ設定の例を次に示します。



vMotion トラフィック用のグループ設定の例を次に示します。

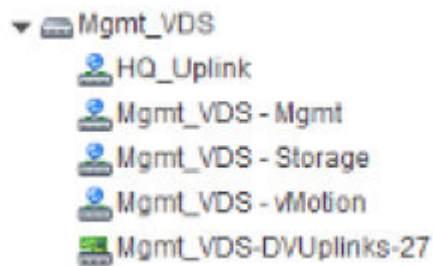
New Distributed Port Group

✓ 1 Select name and location
✓ 2 Configure settings
3 Ready to complete

Ready to complete
Review the changes before proceeding.

Distributed port group name: Mgmt_VDS - vMotion
Port binding: Static binding
Number of ports: 8
Port allocation: Elastic
Network resource pool: (default)
VLAN ID: 430

Distributed Switch とポート グループが完成すると、次のようになります。



- 7 Distributed Switch を右クリックして、[ホストの追加と管理 (Add and Manage Hosts)] を選択し、[ホストの追加 (Add Hosts)] を選択します。

関連付けられたクラスタ内にあるすべてのホストを接続します。たとえば、管理ホスト用のスイッチの場合、管理クラスタ内にあるすべてのホストを選択します。

Add and Manage Hosts

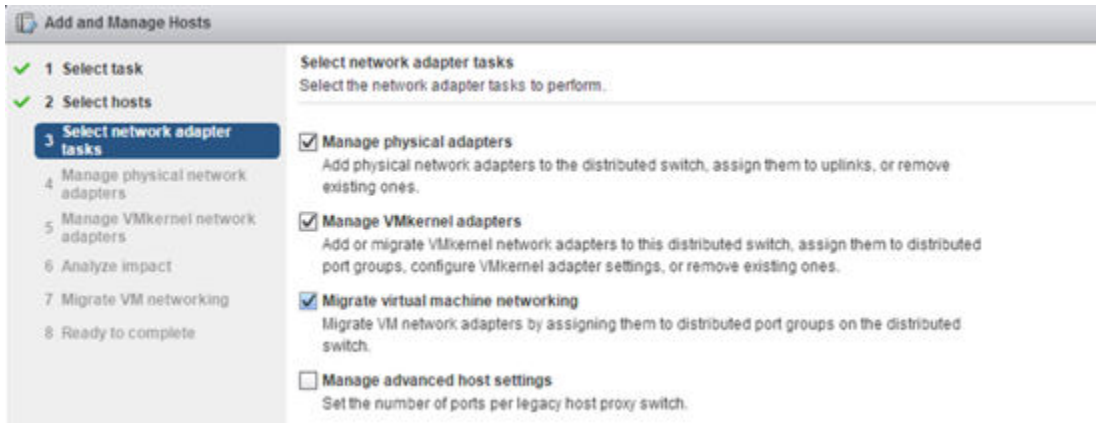
✓ 1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Select hosts
Select hosts to add to this distributed switch.

+ New hosts... | ✕ Remove

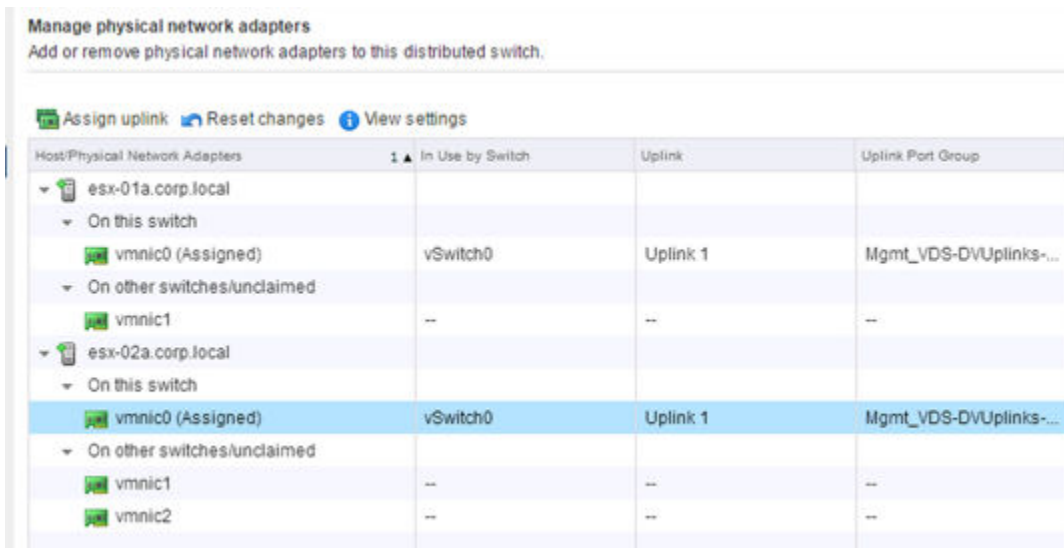
Host	Host Status
(New) esx-01a.corp.local	Connected
(New) esx-02a.corp.local	Connected

- 8 物理アダプタ、VMkernel アダプタ、および仮想マシンのネットワークを移行するための各オプションを選択します。



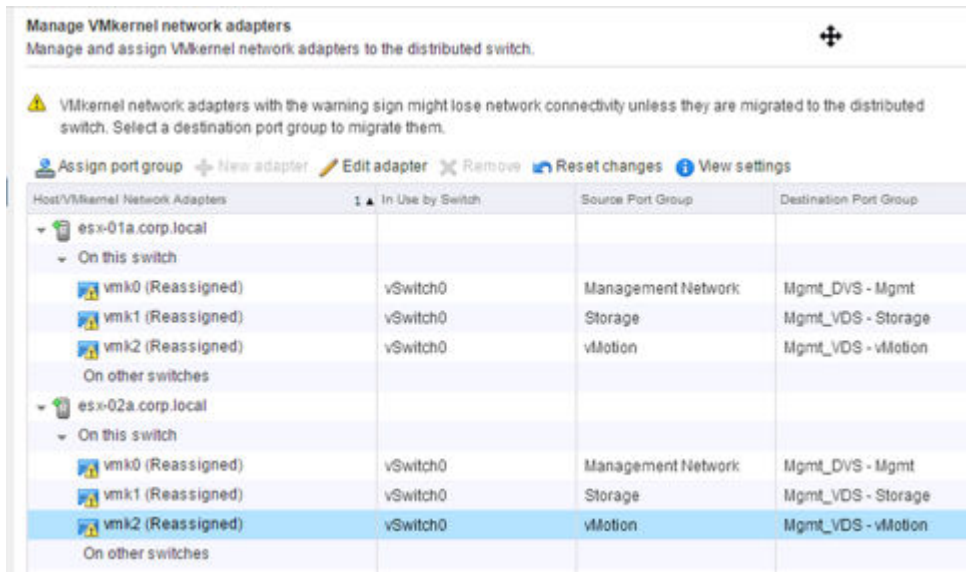
- 9 vmnic を選択し、[アップリンクの割り当て (Assign uplink)] をクリックして、vmnic を標準の vSwitch から Distributed Switch に移行します。分散 vSwitch に接続するホストごとに、この手順を繰り返します。

たとえば、この画面に表示されている 2 台のホストでは、それぞれ標準 vSwitch から分散ポートグループ Mgmt_VDS-DVUplinks に移行するように vmnic0 アップリンクが設定されています。この分散ポート グループは、あらゆる VLAN ID を伝送できるトランク ポートです。



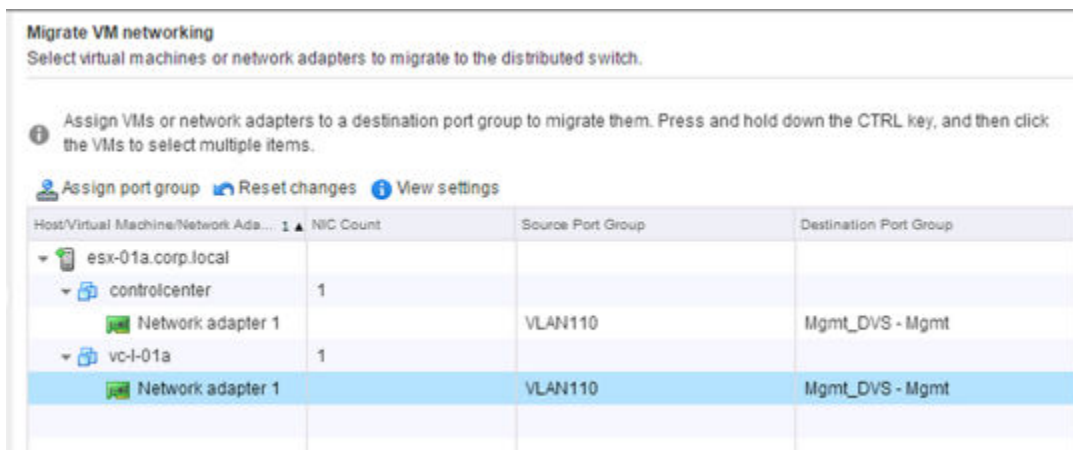
- 10 VMkernel ネットワーク アダプタを選択し、[ポート グループの割り当て (Assign port group)] をクリックします。分散 vSwitch に接続するすべてのホスト上のすべてのネットワーク アダプタに対して、この手順を繰り返します。

たとえば、この画面には、標準のポート グループから新しい分散ポート グループに移行するように設定された、2 台のホスト上の 3 つの vmk ネットワーク アダプタが表示されています。



11 ホスト上の任意の仮想マシンを分散ポートグループに移動します。

たとえば、この画面には、標準のポートグループから新しい分散ポートグループに移行するように設定された、1台のホスト上の2台の仮想マシンが表示されています。



結果

手順が完了したら、ホストの CLI で次のコマンドを実行して結果を確認できます。

```
■ ~ # esxcli network vswitch dvs vmware list
Mgmt_VDS
Name: Mgmt_VDS
VDS ID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
Class: etherswitch
Num Ports: 1862
Used Ports: 5
Configured Ports: 512
MTU: 1600
CDP Status: listen
Beacon Timeout: -1
Uplinks: vmnic0
```

```

VMware Branded: true
DVPort:
    Client: vmnic0
    DVPortgroup ID: dvportgroup-306
    In Use: true
    Port ID: 24

    Client: vmk0
    DVPortgroup ID: dvportgroup-307
    In Use: true
    Port ID: 0

    Client: vmk2
    DVPortgroup ID: dvportgroup-309
    In Use: true
    Port ID: 17

    Client: vmk1
    DVPortgroup ID: dvportgroup-308
    In Use: true
    Port ID: 9

```

```

■ ~ # esxcli network ip interface list
vmk2
    Name: vmk2
    MAC Address: 00:50:56:6f:2f:26
    Enabled: true
    Portset: DvsPortset-0
    Portgroup: N/A
    Netstack Instance: defaultTcpipStack
    VDS Name: Mgmt_VDS
    VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
    VDS Port: 16
    VDS Connection: 1235399406
    MTU: 1500
    TSO MSS: 65535
    Port ID: 50331650

vmk0
    Name: vmk0
    MAC Address: 54:9f:35:0b:dd:1a
    Enabled: true
    Portset: DvsPortset-0
    Portgroup: N/A
    Netstack Instance: defaultTcpipStack
    VDS Name: Mgmt_VDS
    VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
    VDS Port: 2
    VDS Connection: 1235725173
    MTU: 1500
    TSO MSS: 65535
    Port ID: 50331651

vmk1
    Name: vmk1

```

```

MAC Address: 00:50:56:6e:a4:53
Enabled: true
Portset: DvsPortset-0
Portgroup: N/A
Netstack Instance: defaultTcpipStack
VDS Name: Mgmt_VDS
VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
VDS Port: 8
VDS Connection: 1236595869
MTU: 1500
TSO MSS: 65535
Port ID: 50331652

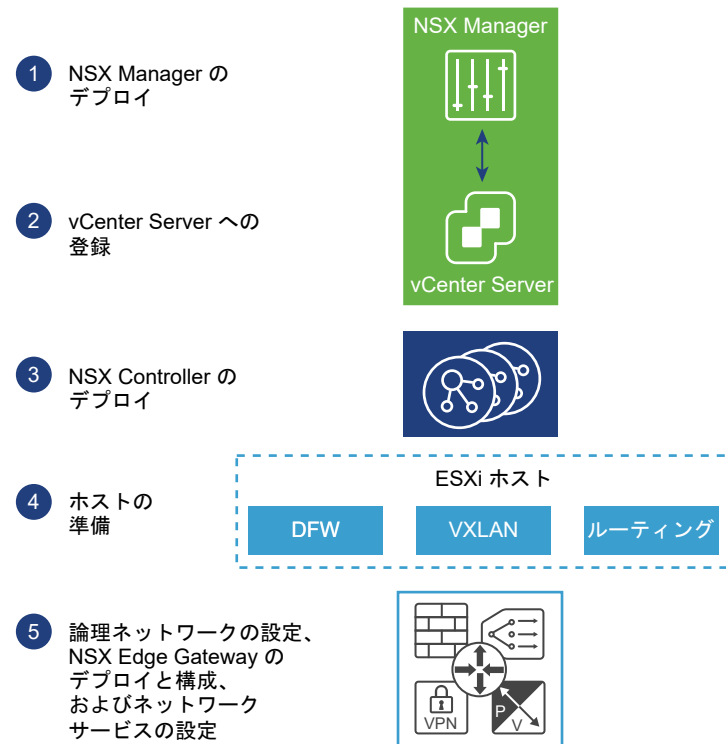
```

次のステップ

すべての vSphere Distributed Switch に対して、移行プロセスを繰り返します。

NSX のインストール ワークフローとトポロジの例

NSX のインストールでは、仮想アプライアンスのデプロイ、ESX ホストの準備、および物理デバイスと仮想デバイスすべてで通信を可能にする設定を行います。

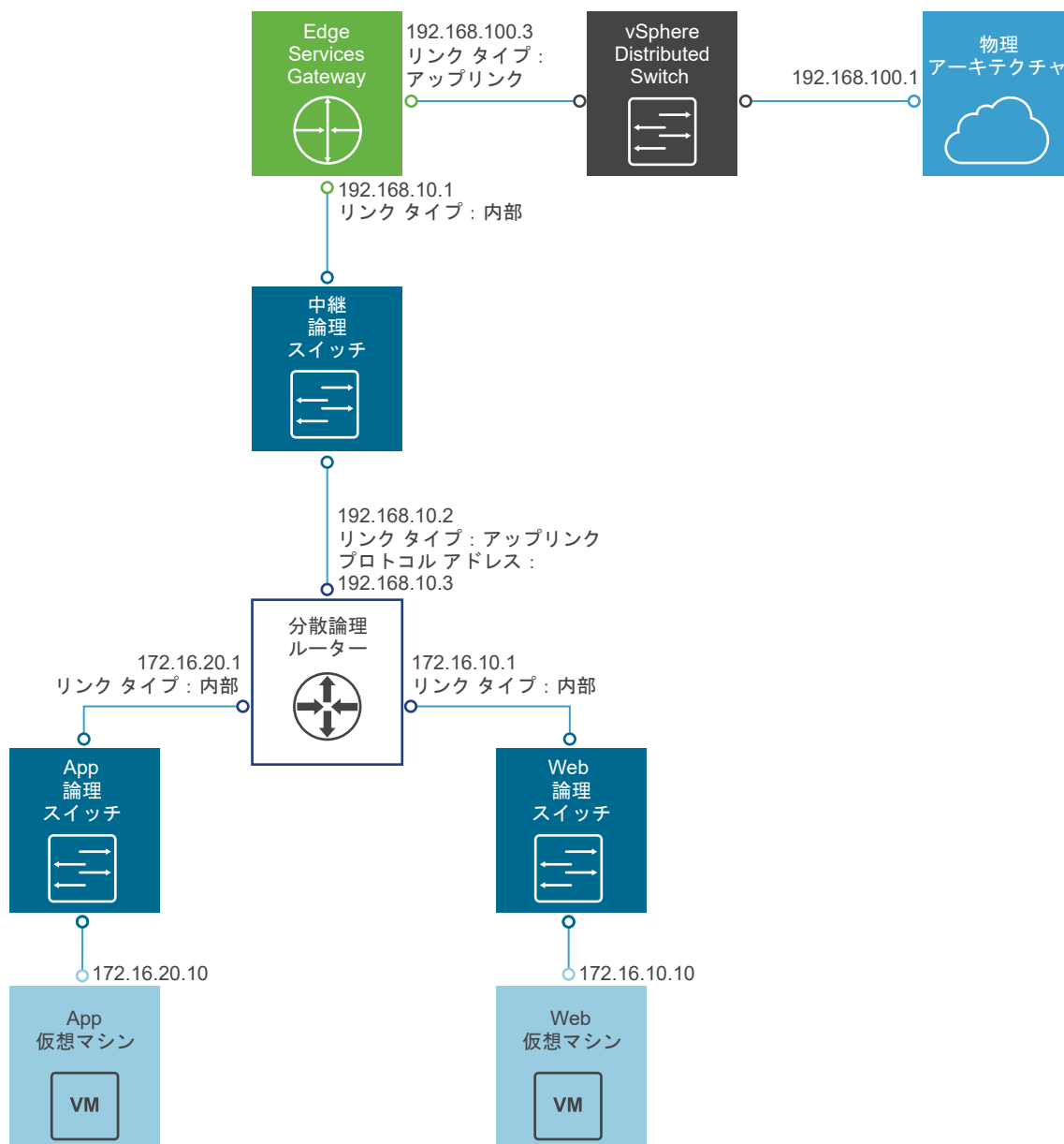


まず、NSX Manager OVF/OVA テンプレートをデプロイし、NSX Manager が管理対象の ESX ホストの管理インターフェイスに完全に接続できることを確認します。その後、登録プロセスを使用して、NSX Manager と vCenter Server インスタンスを互いにリンクする必要があります。これにより、NSX Controller のクラスターをデプロイできるようになります。NSX Manager のような NSX Controller は、ESX ホスト上で仮想アプライアンスと

して動作します。次のステップでは、いくつかの VIB をホストにインストールして、NSX 用に ESX ホストを準備します。これらの VIB により、レイヤー 2 VXLAN 機能、分散ルーティング、および分散ファイアウォールが有効になります。VXLAN の設定、仮想ネットワーク インターフェイス (VNI) 範囲の指定、およびトランスポート ゾーンの作成後、NSX オーバーレイ トポロジを構築できます。

このインストール ガイドでは、プロセスの各ステップを詳しく説明します。

このガイドは、すべての NSX のデプロイに適用でき、さらに演習、ガイダンス、リファレンス用に使用できる NSX オーバーレイのサンプル トポロジを作成する手順も示します。サンプル オーバーレイには、単一の NSX 分散論理ルーター、Edge Services Gateway (ESG)、および 2 つの NSX ルーティング デバイスを接続する NSX 論理中継スイッチが含まれます。サンプル トポロジには、2 つのサンプル仮想マシンを含む、アンダーレイの要素も含まれます。これらの仮想マシンはそれぞれ、NSX 分散論理ルーター経由の接続を可能にする個別の NSX 論理スイッチに接続されています。



Cross-vCenter NSX および拡張リンク モード

vSphere 6.0 には、1 つ以上のプラットフォーム サービス コントローラを使用して複数の vCenter Server システムをリンクする拡張リンク モードが導入されています。これにより、vSphere Web Client 内で、リンクされたすべての vCenter Server システムのインベントリの表示と検索ができます。Cross-vCenter NSX 環境で拡張リンク モードを使用すると、1 つの vSphere Web Client からすべての NSX Manager を管理できます。

複数の vCenter Server が存在する大規模環境では、Cross-vCenter NSX を vCenter Server の拡張リンク モードと併用した方がよい場合があります。これらの 2 つは補完的な機能ですが、互いに独立しています。

Cross-vCenter NSX と拡張リンク モードの組み合わせ

Cross-vCenter NSX では、1 つのプライマリ NSX Manager と複数のセカンダリ NSX Manager を配置します。これらの各 NSX Manager は、異なる vCenter Server にリンクされます。プライマリ NSX Manager には、セカンダリ NSX Manager に表示できるユニバーサル NSX コンポーネント（スイッチ、ルーターなど）を作成できます。

個々の vCenter Server が拡張リンク モードと組み合わせてデプロイされている場合、1 つの vCenter Server で、すべての vCenter Server を表示して、1 つの画面で管理できます。

つまり、Cross-vCenter NSX を vCenter Server の拡張リンク モードと組み合わせた場合、リンクされた任意の vCenter Server から、すべての NSX Manager とすべてのユニバーサル NSX コンポーネントを表示し、管理することができます。

拡張リンク モードなしでの Cross-vCenter NSX の使用

拡張リンク モードは、Cross-vCenter NSX の前提条件や要件ではありません。拡張リンク モードを使用しなくても、Cross-vCenter のユニバーサル トランスポート ゾーン、ユニバーサル スイッチ、ユニバーサル 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。ただし、拡張リンク モードを有効にしていない場合、個々の vCenter Server にログインして各 NSX Manager インスタンスにアクセスする必要があります。

vSphere および拡張リンク モードの詳細情報

拡張リンク モードを使用する場合は、『vSphere のインストールとセットアップ ガイド』または『vSphere のアップグレード ガイド』を参照し、vSphere および拡張リンク モードの最新の要件を確認してください。

プライマリおよびセカンダリ NSX Manager のタスク

5

Cross-vCenter 環境には、1 つのプライマリ NSX Manager と最大 7 つのセカンダリ NSX Manager を配置できます。NSX Manager がプライマリまたはセカンダリのどちらの NSX Manager になるかに関係なく、各 NSX Manager でいくつかのセットアップ タスクを実行します。

この章には、次のトピックが含まれています。

- [NSX Manager 仮想アプライアンスのインストール](#)
- [Single Sign-On の設定](#)
- [NSX Manager への vCenter Server の登録](#)
- [NSX Manager の Syslog サーバの設定](#)
- [NSX for vSphere のライセンスのインストールと割り当て](#)
- [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 Manager 仮想アプライアンスのインストール

NSX Manager は、vCenter Server 環境内の任意の ESX ホスト上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 は、コントローラ、論理スイッチ、Edge Services Gateway などの、NSX コンポーネントの作成、設定、監視を行うためのグラフィカル ユーザー インターフェイス (GUI) と REST API を提供します。NSX Manager は、集約されたシステム ビューを提供するものであり、NSX のネットワーク集中管理コンポーネントです。NSX Manager 仮想マシンは OVA ファイルとしてパッケージされており、vSphere Web Client を使って NSX Manager をデータストアと仮想マシン インベントリにインポートすることができます。

高可用性を実現するには、高可用性と DRS が構成されているクラスタに、NSX Manager をデプロイすることをお勧めします。オプションで、NSX Manager と相互運用する vCenter Server とは異なる vCenter Server に NSX Manager をインストールすることもできます。1 つの NSX Manager は 1 つの vCenter Server 環境で動作します。

Cross-vCenter NSX インストールでは、各 NSX Manager に一意の UUID があることを確認します。OVA ファイルからデプロイされた NSX Manager インスタンスには、一意の UUID があります。(仮想マシンをテンプレートに変換する場合など) テンプレートからデプロイした NSX Manager の UUID は、テンプレートを作成するために使用した元の NSX Manager の UUID と同じです。この 2 つの NSX Manager を同じ Cross-vCenter NSX インストール内で使用することはできません。つまり、NSX Manager ごとに、新しいアプライアンスを、この手順で示されているとおりに最初からインストールする必要があります。

NSX Manager 仮想マシンのインストールには VMware Tools が含まれます。NSX Manager 上で VMware Tools をアップグレードしたり、インストールしたりしないでください。

インストール中に、NSX のカスタマ エクスペリエンス改善プログラム (CEIP) への参加を選択できます。プログラムへの参加または参加を中止する方法については、『NSX 管理ガイド』の NSX のカスタマ エクスペリエンス改善プログラムのセクションを参照してください。

前提条件

- NSX Manager をインストールする前に、必要なポートが開いていることを確認します。 [NSX for vSphere で必要となるポートおよびプロトコル](#)を参照してください。
- ターゲットの ESX ホストでデータストアが構成されており、アクセスできることを確認します。共有ストレージをお勧めします。高可用性には、元のホストに障害が発生した場合でも別のホストで NSX Manager アプライアンスを再起動できるよう、共有ストレージが必要になります。
- NSX Manager で使用する IP アドレスとゲートウェイ、DNS サーバの IP アドレス、ドメイン検索リスト、および NTP サーバの IP アドレスを把握していることを確認します。
- NSX Manager のネットワークを IPv4 アドレスのみ、IPv6 アドレスのみ、またはデュアル スタックのいずれの設定にするかを決定します。NSX Manager のホスト名は他のエンティティによって使用されます。そのため、そのネットワークで使用されている DNS サーバ内の適切な IP アドレスに NSX Manager のホスト名をマップする必要があります。
- NSX Manager の通信が行われる、管理トラフィックの分散ポート グループを準備します。例： [vSphere Distributed Switch の操作](#)を参照してください。NSX Manager の管理インターフェイス、vCenter Server、および ESXi ホストの管理インターフェイスに NSX ゲスト イントロスペクション インスタンスからアクセスできるようにする必要があります。
- クライアント統合プラグインがインストールされている必要があります。[OVF テンプレートのデプロイ] ウィザードは Firefox Web ブラウザで最も適切に動作します。Chrome Web ブラウザでは、クライアント統合プラグインがすでに正常にインストールされているにもかかわらず、クライアント統合プラグインのインストールに関するエラー メッセージが表示されることがあります。クライアント統合プラグインをインストールするには、次の手順を実行します。
 - a Web ブラウザを開いて、vSphere Web Client の URL を入力します。
 - b vSphere Web Client のログイン ページの下部にある [クライアント統合プラグインのダウンロード] をクリックします。

クライアント統合プラグインがすでにシステムにインストールされている場合は、同プラグインをダウンロードするためのリンクは表示されません。クライアント統合プラグインをアンインストールすると、同プラグインのダウンロード リンクが、vSphere Web Client のログイン ページに表示されます。

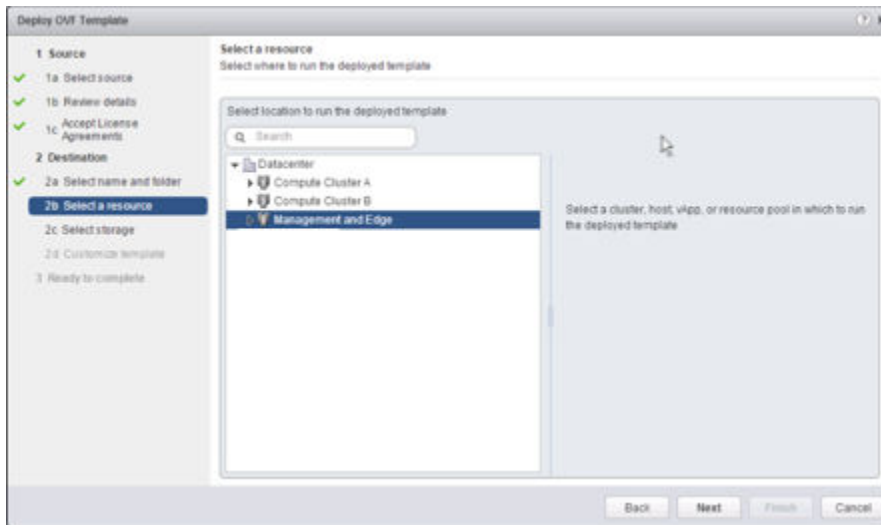
手順

- 1 NSX Manager の OVA (Open Virtualization Appliance) ファイルを見つけます。
ダウンロード URL をコピーするか、OVA ファイルをコンピュータにダウンロードします。
- 2 Firefox で、vSphere Web Client を開きます。

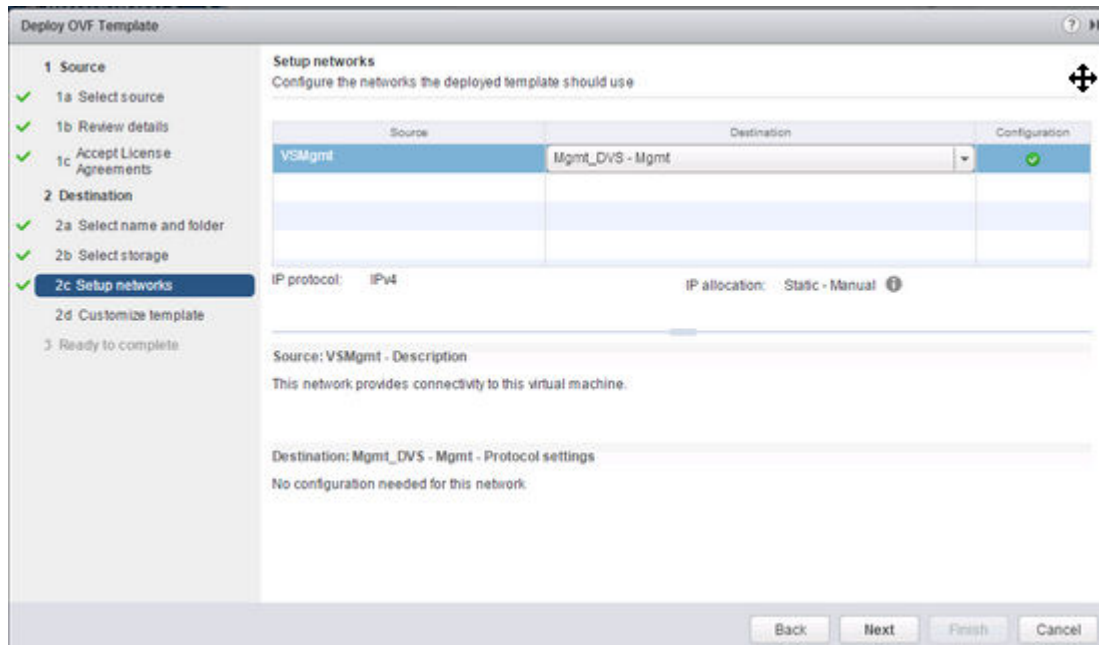
- 3 [仮想マシンおよびテンプレート (VMs and Templates)] を選択し、使用するデータセンターを右クリックして、[OVF テンプレートのデプロイ (Deploy OVF Template)] を選択します。
- 4 ダウンロード URL を張り付けるか、[参照 (Browse)] をクリックしてコンピュータ上のファイルを選択します。

注: Operation timed out エラーでインストールに失敗した場合、ストレージ デバイスとネットワーク デバイスに接続の問題が発生していないかどうかを確認します。この問題は、ストレージ デバイスへの接続が失われた場合や、物理 NIC またはスイッチとの接続エラーなど、物理インフラストラクチャに問題がある場合に発生します。

- 5 [追加の設定オプションの承諾 (Accept extra configuration options)] チェックボックスを選択します。
これにより、IPv4 と IPv6 アドレス、デフォルト ゲートウェイ、DNS、NTP、および SSH プロパティを、インストール後に手動で設定するのではなく、インストール中に設定できます。
- 6 VMware 使用許諾契約書に同意します。
- 7 NSX Manager の名前を編集し (必要な場合)、NSX Manager をデプロイする場所を選択します。
入力した名前は vCenter Server インベントリに表示されます。
選択したフォルダは、NSX Manager への権限を適用するために使用されます。
- 8 NSX Manager アプライアンスのデプロイ先であるホストまたはクラスタを選択します。
次はその例です。



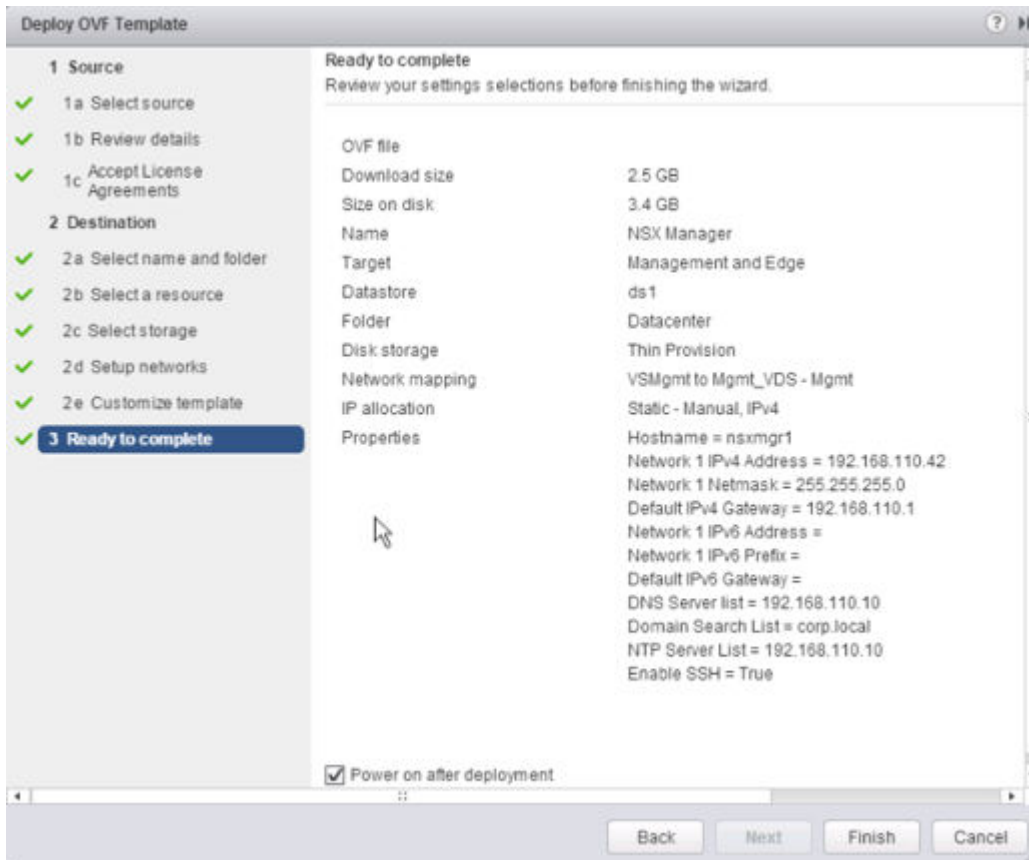
- 9 仮想ディスクのフォーマットを [シック プロビジョニング (Thick Provision)] に変更し、仮想マシンの構成ファイルと仮想ディスク用のターゲット データストアを選択します。
- 10 NSX Manager のポート グループを選択します。
たとえば、このスクリーン ショットでは「Mgmt_DVS - Mgmt」ポートグループを選択しています。



11 (オプション) [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 Customer Experience Improvement Program)] チェックボックスを選択します。

12 NSX Manager の設定オプションを追加で設定します。

たとえば、この画面には、IPv4 のみのデプロイですべてのオプションを設定した後の最終確認画面が表示されています。



結果

NSX Manager のコンソールを開いて、ブート プロセスを追跡します。

NSX Manager が完全に起動した後、CLI にログインし、show interface コマンドを実行して、IP アドレスが想定どおりに適用されていることを確認します。

```
nsxmgr1> show interface
Interface mgmt is up, line protocol is up
index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:c7:fa
inet 192.168.110.42/24 broadcast 192.168.110.255
inet6 fe80::250:56ff:fe8e:c7fa/64
Full-duplex, 0Mb/s
input packets 1370858, bytes 389455808, dropped 50, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 1309779, bytes 2205704550, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

NSX Manager がそのデフォルト ゲートウェイ、NTP サーバ、vCenter Server、および管理するすべてのハイパーバイザー ホスト上の管理インターフェイスの IP アドレスに ping できることを確認します。

Web ブラウザを開き、NSX Manager の IP アドレスまたはホスト名に移動して、NSX Manager アプライアンスの GUI に接続します。

インストール時に設定したパスワードを使用して [admin] としてログインした後、[ホーム] ページで [サマリの表示 (View Summary)] をクリックし、次のサービスが実行されていることを確認します。

- vPostgres
- RabbitMQ
- NSX 管理サービス

最適なパフォーマンスを得るには、NSX Manager 仮想アプライアンス用にメモリを予約することをお勧めします。メモリ予約は、ホストが仮想マシン用に予約する物理メモリ容量の保証された下限であり、メモリがオーバーコミットされる場合でも、この容量が保証されます。NSX Manager が効率的に動作するのに十分なメモリが確保されるように、予約のレベルを設定します。

次のステップ

NSX Manager に vCenter Server を登録します。

Single Sign-On の設定

SSO を使用することで、各コンポーネントが個別にユーザーを認証する代わりに、さまざまなコンポーネントがセキュア トークン交換メカニズムを介して相互に通信して、vSphere と NSX の安全性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。シングル サインオン (SSO) サービスを NSX に統合すると、vCenter Server ユーザーに対するユーザー認証の安全性が強化され、NSX が Active Directory、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。

Time Settings	
<div>Unconfigure NTP Servers</div> <div>Edit</div>	
Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.	
NTP Server	192.168.110.10
Timezone	UTC
Date/Time	12/28/2016 21:31:49

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 NSX Manager 仮想アプライアンスにログインします。

- 3 ホーム ページで [アプライアンス設定の管理 (Manage Appliance Settings)] - [NSX 管理サービス (NSX Management Service)] の順にクリックします。

- 4 [Lookup Service URL] セクションの [編集 (Edit)] をクリックします。

- 5 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。

- 6 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。

- 7 SSO 管理者のユーザー名とパスワードを入力し、[OK] をクリックします。


SSO サーバの証明書のサムプリントが表示されます。

- 8 証明書のサムプリントが SSO サーバの証明書と一致することを確認します。

認証局 (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。

- 9 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 URL:	https://psc-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	● Connected 

次のステップ

『NSX 管理ガイド』で「vCenter Server ユーザーへのロールの割り当て」を参照してください。

NSX Manager への vCenter Server の登録

NSX Manager と vCenter Server は 1 対 1 の関係です。NSX Manager のインスタンスごとに 1 つの vCenter Server があります (Cross-vCenter NSX 環境も含む)。

vCenter Server システムを登録できるのは、1 つの NSX Manager だけです。vCenter Server で、設定済みの NSX Manager の登録を変更することはできません。

既存の NSX Manager の vCenter Server の登録を変更する場合は、最初にすべての NSX 構成を削除し、vCenter Server システムから NSX Manager プラグインを削除する必要があります。手順については、[NSX 環境の安全な削除](#)を参照してください。または、新しい NSX Manager アプライアンスをデプロイして、新しい vCenter Server システムを登録することも可能です。

前提条件

- NSX 管理サービスが実行されている必要があります。https://<nsx-manager-ip> の NSX Manager Web インターフェイスで、[ホーム (Home)] - [サマリの表示 (View Summary)] の順にクリックし、サービスのステータスを確認します。
- vCenter Single Sign-On 管理者グループのメンバーである vCenter Server ユーザー アカウントを使用して、NSX Manager と vCenter Server システムを同期する必要があります。アカウントのパスワードに非 ASCII 文字が含まれている場合、NSX Manager と vCenter Server システムとの同期を行う前にパスワードを変更する必要があります。root アカウントは使用しないでください。

ユーザーの追加方法については、『Platform Services Controller の管理』の「vCenter Single Sign-On ユーザーおよびグループの管理」を参照してください。

- 正引きと逆引きの名前解決が機能し、次のシステムで DNS 名を解決できることを確認します。
 - NSX Manager アプライアンス
 - vCenter Server システム
 - Platform Services Controller システム
 - ESXi ホスト

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 ホーム ページで、[vCenter 登録の管理 (Manage vCenter Registration)] をクリックします。
- 3 vCenter Server システムの IP アドレスまたはホスト名を参照するように vCenter Server の項目を編集し、vCenter Server システムのユーザー名とパスワードを入力します。

- 4 証明書のサムプリントが vCenter Server システムの証明書と一致することを確認します。

vCenter Server システムに 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。

- 5 NSX Manager がファイアウォール タイプのマスキング デバイスの背後に置かれていない限り [プラグイン スクリプトのダウンロード場所を変更する (Modify plugin script download location)] を選択しないでください。

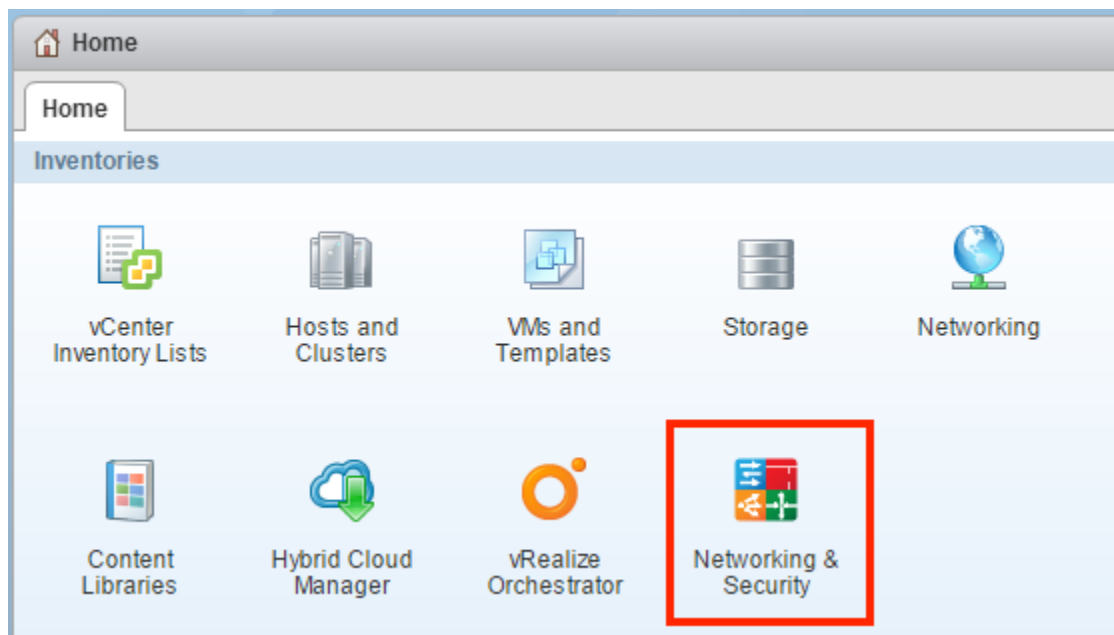
このオプションは、NSX Manager の代替 IP アドレスを入力できるようにするものです。このタイプのファイアウォールの背後には NSX Manager を配置しないでください。

- 6 vCenter Server システムの状態が [接続中 (Connected)] になっていることを確認します。

- 7 vSphere Web Client がすでに開いている場合は、ログアウトします。NSX Manager を vCenter Server に登録したときに使用したアカウントを使用して、再度ログインします。

ログアウトせずに再度ログインすると、vSphere Web Client の [ホーム (Home)] タブに [ネットワークとセキュリティ (Networking & Security)] のアイコンが表示されません。

[ネットワークとセキュリティ (Networking & Security)] アイコンをクリックして、新しく展開した NSX Manager が表示されていることを確認します。



次のステップ

NSX Manager のインストール直後に NSX Manager データのバックアップをスケジュールリングします。『NSX 管理ガイド』の「NSX のバックアップとリストア」を参照してください。

NSX for vSphere パートナー ソリューションがある場合は、パートナーのドキュメントを参照して、パートナー コンソールを NSX Manager に登録する方法を確認してください。

これで、NSX for vSphere コンポーネントをインストールして構成できます。

NSX Manager の Syslog サーバの設定

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 Controller は 1 台の Syslog サーバをサポートします。

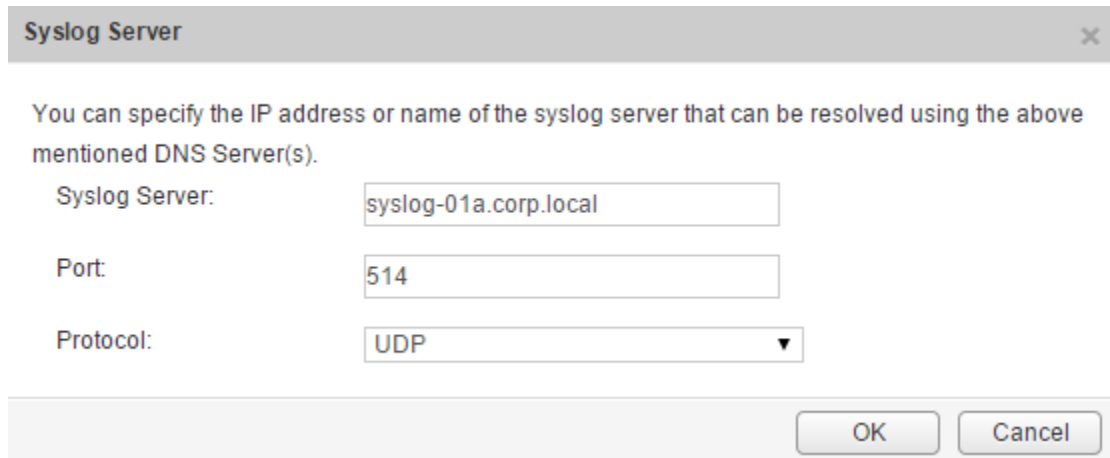
手順

- 1 NSX Manager 仮想アプライアンスにログインします。

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 ホーム ページで [アプライアンス設定の管理 (Manage Appliance Settings)] - [全般 (General)] の順にクリックします。
- 3 [Syslog サーバ (Edit)] の横にある [編集 (Syslog Server)] をクリックします。
- 4 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。

次はその例です。



- 5 [OK] をクリックします。

結果

NSX Manager のリモート ログが有効になり、スタンドアロンの Syslog サーバにログが保存されます。

NSX for vSphere のライセンスのインストールと割り当て

NSX for vSphere のライセンスは、NSX Manager のインストールが完了した後に、vSphere Web Client を用いたインストールと割り当てができます。

NSX 6.2.3 以降、インストール時のデフォルトのライセンスは、NSX for vShield Endpoint となります。このライセンスは、アンチウイルス オフロード機能のみを使用する目的で vShield Endpoint をデプロイおよび管理するために、NSX を使用できます。また、ハードコーディングによって強制的にホストの準備と NSX Edge の作成をブロックすることにより、VXLAN、ファイアウォール、および Edge サービスの使用を制限しています。

論理スイッチ、分散論理ルーター、分散ファイアウォール、NSX Edge を含む他の NSX 機能を使用する必要がある場合は、NSX ライセンスを購入してこれらの機能を使用するか、または、これらの機能を短期間使用して評価するための評価版ライセンスが必要になります。

NSX のライセンス エディションと関連機能の詳細については、<https://kb.vmware.com/kb/2145269> を参照してください。

手順

- ◆ vSphere 5.5 で、次の手順を実行して NSX のライセンスを追加します。

- a vSphere Web Client にログインします。
- b [管理 (Administration)] をクリックして、[ライセンス (Licenses)] をクリックします。
- c [ソリューション (Solutions)] タブをクリックします。
- d [ソリューション] リストで NSX for vSphere を選択します。[ライセンス キーの割り当て (Assign a license key)] をクリックします。
- e ドロップダウン メニューから [新しいライセンス キーの割り当て (Assign a new license key)] を選択します。
- f ライセンス キーを入力し、この新しいキーのラベル (オプション) を入力します。
- g [デコード (Decode)] をクリックします。
ライセンス キーをデコードして、そのキーが正しい形式であるか、および資産のライセンス供与に対して十分なキャパシティがあるかを確認します。
- h [OK] をクリックします。

- ◆ vSphere 6.0 で、次の手順を実行して NSX のライセンスを追加します。

- a vSphere Web Client にログインします。
- b [管理 (Administration)] をクリックして、[ライセンス (Licenses)] をクリックします。
- c [資産 (Assets)] タブをクリックして、[ソリューション (Solutions)] タブをクリックします。
- d [ソリューション] リストで NSX for vSphere を選択します。[すべてのアクション (All Actions)] ドロップダウン メニューから、[ライセンスの割り当て... (Assign license...)] を選択します。
- e [追加 (+) (Add)] アイコンをクリックします。ライセンス キーを入力して、[次へ (Next)] をクリックします。ライセンスの名前を追加して、[次へ (Next)] をクリックします。[終了 (Finish)] をクリックして、ライセンスを追加します。
- f 新しいライセンスを選択します。

- g (オプション) [機能の表示 (View Features)] アイコンをクリックして、このライセンスで有効になっている機能を表示します。[キャパシティ (Capacity)] 列で、ライセンスのキャパシティを確認します。
- h [OK] をクリックして、新しいライセンスを NSX に割り当てます。

次のステップ

NSX ライセンスの詳細については、<http://www.vmware.com/files/pdf/vmware-product-guide.pdf> を参照してください。

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 分散ファイアウォール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 Controller、および NSX Edge 仮想マシンは、NSX 分散ファイアウォール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勧めます。

- 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。

注： 「任意」のデフォルト ルールを許可からブロックに変更する前に、除外リストに vCenter Server を追加することが重要です。この操作を行わないと、「すべて拒否」ルールを作成した後（または、デフォルト ルールをブロック アクションに変更した後）で vCenter Server へのアクセスがブロックされます。この場合、API コマンド `https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config` を実行して、分散ファイアウォールをデフォルトのファイアウォール ルール セットにロールバックします。この要求では、ステータス 204 が返されます。これにより、分散ファイアウォールのデフォルト ポリシー（許可のデフォルト ルールも含む）がリストアされ、vCenter Server と vSphere Web Client へのアクセスが再度有効になります。

- 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 分散ファイアウォールで保護した場合、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を選択し、[追加 (Add)] をクリックします。

7 [OK] をクリックします。

結果

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。

プライマリ NSX Manager の設定

6

Cross-vCenter NSX 環境には、1 つのプライマリ NSX Manager のみが配置されます。どの NSX Manager をプライマリ NSX Manager として使用するかを選択し、構成タスクを実行して、NSX のインストール、NSX Manager へのプライマリ ロールの割り当て、およびユニバーサル オブジェクトの作成を行います。

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 クラスタはありません。

この章には、次のトピックが含まれています。

- [プライマリ NSX Manager への NSX Controller のデプロイ](#)
- [プライマリ NSX Manager でのホストの準備](#)
- [プライマリ NSX Manager からの VXLAN の設定](#)
- [プライマリ NSX Manager へのセグメント ID プールとマルチキャスト アドレスの割り当て](#)
- [NSX Manager へのプライマリ ロールの割り当て](#)
- [プライマリ NSX Manager でのユニバーサル セグメント ID プールとユニバーサル マルチキャスト アドレスの割り当て](#)
- [プライマリ NSX Manager でのユニバーサル トランスポート ゾーンの追加](#)
- [プライマリ NSX Manager でのユニバーサル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](#)
- [プライマリ NSX Manager でのユニバーサル分散論理ルーターの追加](#)

プライマリ NSX Manager への NSX Controller のデプロイ

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集中管理ポイントとして機能するもので、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。1) 分散論理ルーター、あるいは 2) ユニキャストまたはハイブリッド モードの VXLAN のデプロイを計画する場合、コントローラが必要になります。Cross-vCenter NSX では、NSX Manager にプライマリ ロールを割り当てると、そのコントローラ クラスタが Cross-vCenter NSX 環境全体のユニバーサル コントローラ クラスタになります。

NSX デプロイのサイズに関係なく、VMware では、各 NSX Controller クラスタに 3 つのコントローラ ノードが含まれている必要があります。各クラスタのコントローラ ノード数を 3 つ以外にすることはできません。

クラスタの各コントローラのディスク ストレージ システムでは、ピーク時の書き込み遅延が 300 ミリ秒未満、平均書き込み遅延が 100 ミリ秒未満である必要があります。ストレージ システムがこれらの要件を満たしていない場合は、クラスタが不安定になり、システム停止の原因となる場合があります。

前提条件

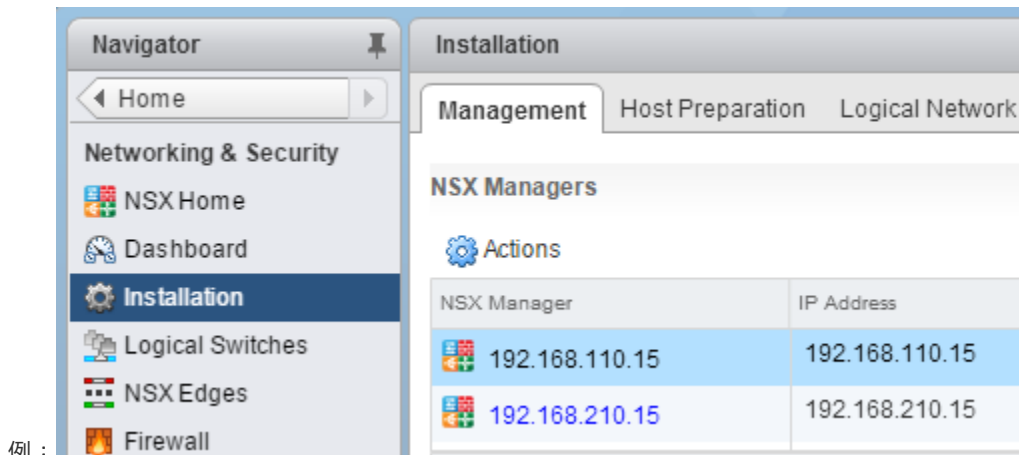
- NSX Controller を展開する前に、NSX Manager アプライアンスを展開し、vCenter Server を NSX Manager に登録する必要があります。
- ゲートウェイおよび IP アドレス範囲を含め、コントローラ クラスタの IP アドレス プール設定を決定します。DNS 設定はオプションです。NSX Controller の IP ネットワークには、NSX Manager への接続と、ESXi ホスト上の管理インターフェイスへの接続が必要です。

手順

- 1 vSphere Web Client を使用して、プライマリとして使用する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] > [Networking and Security] > [インストール手順 (Installation)] の順に移動して、[管理 (Management)] タブを選択します。



vCenter Server システムが拡張リンク モードの場合、関連付けられたすべての NSX Manager がここに一覧表示されます。

- 3 [NSX Manager] セクションで、プライマリとして使用する NSX Manager を選択します。
- 4 [NSX Controller ノード] セクションで、[ノードの追加 (Add Node)] (+) アイコンをクリックします。
- 5 環境に適した NSX Controller 設定を入力します。

NSX Controller は、vSphere Standard スイッチまたは vSphere Distributed Switch のポート グループに展開する必要があります。これらのスイッチは、VXLAN ベースではなく、IPv4 を介して NSX Manager、その他のコントローラ、およびホストに接続します。

次はその例です。

Add Controller
?

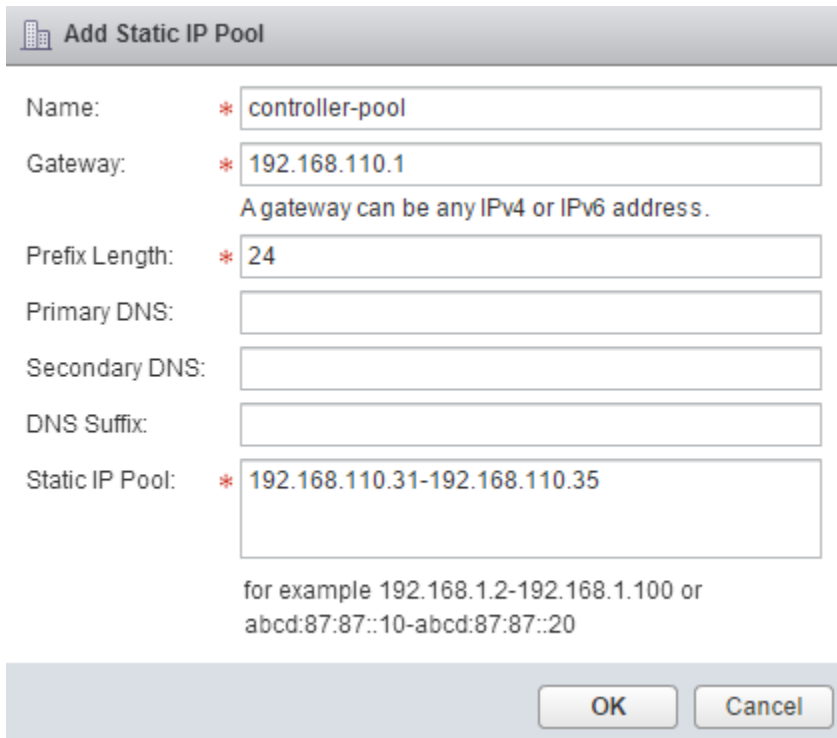
Name: * controller-1
NSX Manager: * 192.168.110.15
Datacenter: * Datacenter Site A
Cluster/Resource Pool: * Management & Edge Cl...
Datastore: * ds-site-a-nfs01
Host: esxmgt-01a.corp.local
Folder: NSX Controllers
Connected To: * vds-mgt_Managem Change Remove
IP Pool: * controller-pool Select
Password: *
Confirm password: *

OK Cancel

- 6 コントローラ クラスターの IP アドレス ルールをまだ設定していない場合は、ここで [新規 IP アドレス プール (New IP Pool)] をクリックして設定します。

必要な場合は、個々のコントローラを別々の IP サブネットに含めることができます。

次はその例です。



Add Static IP Pool

Name: * controller-pool

Gateway: * 192.168.110.1
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: * 192.168.110.31-192.168.110.35

for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20

OK Cancel

7 コントローラのパスワードを入力し、再入力します。

注： パスワードの一部にユーザー名を含めることはできません。いずれの文字も 3 回以上連続して使用できません。

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 つ以上の数字
- 1 文字以上の特殊文字

8 最初のコントローラを完全にデプロイした後、追加の 2 つのコントローラをデプロイします。

3 つのコントローラが必須です。コントローラが同一ホスト上に存在することがないように、DRS の非アフィニティ ルールを設定することをお勧めします。

結果

デプロイが正常に終了すると、コントローラのステータスが [接続済み (Connected)] になり、緑色のチェック マークが表示されます。

デプロイが正常に終了しなかった場合は、『NSX トラブルシューティング ガイド』の「NSX Controller のデプロイ」を参照してください。

プライマリ NSX Manager でのホストの準備

ホストの準備とは、NSX Manager が 1) vCenter クラスタのメンバーである ESXi ホストに NSX カーネル モジュールをインストールし 2) NSX 制御プレーンおよび管理プレーンのファブリックを構築するプロセスです。VIB ファイルにパッケージ化された NSX カーネル モジュールは、ハイパーバイザー カーネル内で実行され、分散ルーティング、分散ファイアウォール、VXLAN ブリッジ機能などのサービスを提供します。

ネットワーク仮想化に向けて環境を準備するには、必要に応じて、vCenter Server ごとにクラスタ単位レベルでネットワーク インフラストラクチャ コンポーネントをインストールする必要があります。これにより、クラスタ内のすべてのホストに必要なソフトウェアがインストールされます。このクラスタに新しいホストが追加されると、新しく追加されたホストに必要なソフトウェアが自動的にインストールされます。

ESXi をステートレス モードで使用している、つまり ESXi の再起動時に以前の状態が維持されない場合、NSX VIB を手動でダウンロードして、ホスト イメージに組み込む必要があります。NSX VIB のダウンロード パスは、https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties ページに記載されています。ダウンロード パスは NSX のリリースごとに変わる可能性があるため、注意してください。必ず https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties ページを確認して、適切な VIB を取得してください。Auto Deploy を通じて VXLAN をデプロイする手順については、<https://kb.vmware.com/kb/2041972> を参照してください。

前提条件

- vCenter Server を NSX Manager に登録して、NSX Controller をデプロイします。
- NSX Manager の IP アドレスで照会されたときに、DNS の逆引き参照で完全修飾ドメイン名が返されることを確認します。次はその例です。

```
C:\Users\Administrator>nslookup 192.168.110.42
Server: localhost
Address: 127.0.0.1

Name: nsxmgr-l-01a.corp.local
Address: 192.168.110.42
```

- ホストが vCenter Server の DNS 名を解決できることを確認します。
- ホストが vCenter Server のポート 80 に接続できることを確認します。
- vCenter Server と ESXi ホスト間でネットワーク時刻が同期されることを確認します。
- NSX に参加する各ホスト クラスタで、クラスタ内の各ホストが共通の vSphere Distributed Switch (VDS) に接続していることを確認します。

たとえば、Host1 と Host2 を含むクラスタがあるとします。Host1 は仮想スイッチの VDS1 と VDS2 に接続されています。Host2 は VDS1 と VDS3 に接続されています。NSX 用にクラスタを準備するときは、NSX をクラスタ上の VDS1 にのみ関連付けることができます。クラスタに別のホスト (Host3) を追加しても、Host3 が VDS1 に接続されていない場合、それは無効の構成であり、Host3 は NSX 機能を使用できる状態にはなりません。

- お使いの環境に vSphere Update Manager (VUM) がある場合は、クラスタでネットワーク仮想化の準備をする前に、VUM を無効にしておく必要があります。VUM が有効かどうかを確認する方法と、必要に応じて VUM を無効にする方法については、<http://kb.vmware.com/kb/2053782> を参照してください。
- NSX ホストの準備プロセスを開始する前に、クラスタのステータスが解決済みであること、つまり [解決 (Resolve)] オプションがクラスタの [アクション (Actions)] リストに表示されていないことを必ず確認してください。

次はその例です。

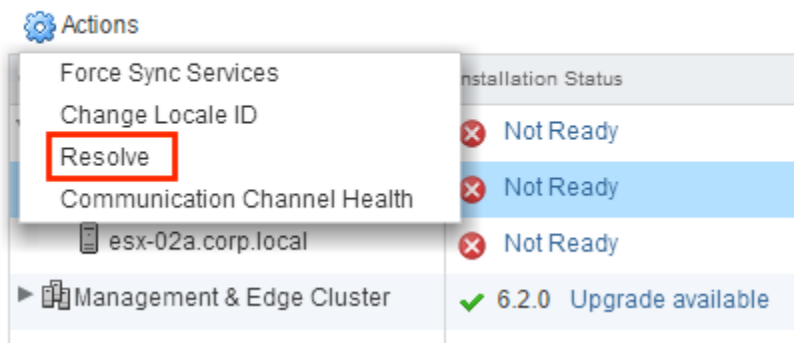
NSX Component Installation on Hosts



クラスタ内のホストを再起動する必要がある場合に、[解決 (Resolve)] オプションが表示されることがあります。

また、解決しなければならないエラーが発生したために、[解決 (Resolve)] オプションが表示されることもあります。エラーを表示するには、[準備ができていません (Not Ready)] リンクをクリックします。できれば、エラー状態を解除してください。クラスタのエラー状態を解除できない場合、1 つの解決策として、ホストを新規または別のクラスタに移動して、古いクラスタを削除します。

NSX Component Installation on Hosts




[解決 (Resolve)] オプションで問題が解決しない場合は、『NSX トラブルシューティング ガイド』を参照してください。[解決 (Resolve)] オプションで解決された問題の一覧については、『NSX のログ作成とシステム イベント』を参照してください。

手順

- 1 vSphere Web Client を使用して、プライマリとして使用する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] の順に移動し、[ホストの準備 (Host Preparation)] タブを選択します。
- 3 NSX の論理スイッチ、論理ルーティング、論理ファイアウォールを必要とするすべてのクラスタに対し、[アクション (Actions) ()] をクリックして [インストール (Install)] をクリックします。

コンピューティング クラスタ（パイロード クラスタとも呼ばれる）は、アプリケーション仮想マシン（Web、データベースなど）を含むクラスタです。コンピューティング クラスタで NSX スイッチ、ルーティング、またはファイアウォールを使用する場合は、コンピューティング クラスタに対応する [インストール (Install)] をクリックする必要があります。

（例に示す）「管理および Edge」共有クラスタでは、NSX Manager とコントローラ仮想マシンが 1 つのクラスタを Edge デバイス（分散論理ルーター (DLR)、Edge Services Gateway (ESG) など）と共有します。この場合は、共有クラスタに対応する [インストール (Install)] をクリックすることが重要です。

逆に、管理および Edge にそれぞれ専用の共有されないクラスタがある場合（本番環境で推奨）、管理クラスタではなく Edge クラスタに対応する [インストール (Install)] をクリックします。

注： インストールの進行中は、いずれのサービスまたはコンポーネントについてもデプロイ、アップグレード、またはアンインストールしないでください。

- 4 [インストール ステータス (Installation Status)] 列に緑色のチェック マークが表示されるまで、インストールを監視します。

[インストール ステータス (Installation Status)] 列に赤の警告アイコンと [準備ができていません (Not Ready)] という表示が現れたら、[解決 (Resolve)] をクリックします。[解決 (Resolve)] をクリックすると、ホストが再起動されることがあります。インストールが依然として成功しない場合は、警告アイコンをクリックします。すべてのエラーが表示されます。必要な操作を行い、再度 [解決 (Resolve)] をクリックします。

インストールが完了すると、[インストールの状態 (Installation Status)] 列に、インストールされた NSX のバージョンとビルドが表示され、[ファイアウォール (Firewall)] 列に [有効 (Enabled)] と表示されます。いずれの列にも緑色のチェック マークが表示されます。[インストールの状態 (Installation Status)] 列に [解決] の表示がある場合は、[解決] をクリックし、ブラウザ ウィンドウを更新します。

結果

VIB がインストールされ、準備されたクラスタ内のすべてのホストに VIB が登録されます。インストールされている VIB は、インストールされている NSX と ESXi のバージョンによって異なります。

ESXi バージョン	NSX バージョン	インストールされている VIB
5.5	すべての 6.3.x	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 以降	6.3.2 以前	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 以降	6.3.3 以降	<ul style="list-style-type: none"> ■ esx-nsxv

確認するには、各ホストに SSH で接続し、`esxcli software vib list` コマンドを実行して関連する VIB を確認します。このコマンドでは、VIB のほかに、インストールされている VIB のバージョンも表示されます。

```
[root@host:~] esxcli software vib list | grep esx
esx-XXXX      6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2016-12-29
```

準備されたクラスタにホストを追加したら、NSX VIB が自動的にホストにインストールされます。

準備されていないクラスタにホストを移動すると、NSX VIB が自動的にホストからアンインストールされます。

プライマリ NSX Manager からの VXLAN の設定

VXLAN ネットワークを使用し、ホスト間でレイヤー 2 の論理スイッチングを行うことで、基盤となる複数のレイヤー 3 ドメインにまたがることができます。VXLAN はクラスタ単位で設定します。その場合、NSX に参加する各クラスタを vSphere Distributed Switch (VDS) にマッピングします。クラスタを Distributed Switch にマップすると、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。ここで選択した設定は VMkernel インターフェイスの作成で使用されます。

また、論理ルーティングと論理スイッチングが必要である場合は、ホストに NSX VIB がインストールされているすべてのクラスタで VXLAN 転送パラメータが設定されている必要があります。分散ファイアウォールのみをデプロイするように計画する場合、VXLAN 転送パラメータを設定する必要はありません。

VXLAN ネットワークを設定する場合、vSphere Distributed Switch、VLAN ID、MTU サイズ、IP アドレス指定メカニズム（DHCP または IP アドレス プール）、および NIC チーミング ポリシーを指定する必要があります。

各スイッチの MTU は、1550 以上に設定する必要があります。デフォルトでは、1600 に設定されています。

vSphere Distributed Switch の MTU サイズが VXLAN の MTU より大きい場合、vSphere Distributed Switch の MTU の値が下方調整されることはありません。VDS の MTU の値の方が小さい場合は、VXLAN の MTU と一致するように調整されます。たとえば、vSphere Distributed Switch の MTU が 2000 に設定されている場合に VXLAN の MTU をデフォルトの 1600 にしても、vSphere Distributed Switch の MTU は変更されません。

vSphere Distributed Switch の MTU が 1500 で VXLAN の MTU が 1600 である場合は、vSphere Distributed Switch の MTU が 1600 に変更されます。

VTEP には VLAN ID が関連付けられています。ただし、VTEP に VLAN ID = 0 を指定することができます。これは、フレームのタグが解除されることを意味します。

管理クラスタとコンピューティング クラスタで異なる IP アドレス設定を使用したい場合があります。別の設定が使用されるかどうかは物理ネットワークの設計によって異なりますが、小規模なデプロイで使用される可能性はまずありません。

前提条件

- クラスタ内のすべてのホストを、共通の vSphere Distributed Switch に接続する必要があります。
- NSX Manager がインストールされている
- 制御プレーンにマルチキャスト レプリケーション モードを使用していない場合は、NSX Controller をインストールする必要があります。
- NIC チーミング ポリシーを計画します。NIC チーミング ポリシーによって、vSphere Distributed Switch のロード バランシングおよびフェイルオーバーの設定が決まります。

特定の vSphere Distributed Switch 上の各ポートグループには同一のチーミング ポリシーを適用してください。つまり、一部のポートグループにイーサチャネル、LACPv1、または LACPv2 を使用して、その他のポートグループに異なるチーミング ポリシーを使用することはできません。これらの異なるチーミング ポリシーでアップリンクが共有されると、トラフィックの中断につながります。分散論理ルーターが存在する場合は、ルーティングの問題が発生します。このような設定はサポートされていないため、回避する必要があります。

IP ハッシュに基づいたチーミング（イーサチャネル、LACPv1、または LACPv2）でのベスト プラクティスは、vSphere Distributed Switch 上のすべてのアップリンクをチーミングして使用し、その vSphere Distributed Switch 上のポートグループに複数の異なるチーミング ポリシーを設定しないことです。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。

- VXLAN Tunnel End Point (VTEP) の IP アドレス指定方式を計画します。VTEP は、VXLAN のカプセル化されたフレームの発信と終了を行う ESX ホストを一意に識別するために外部 IP ヘッダで使用する、ソース IP アドレスとターゲット IP アドレスです。VTEP IP アドレスには、DHCP または手動で設定した IP アドレス プールを使用できます。

特定の IP アドレスを VTEP に割り当てるには、1) DHCP 固定アドレスまたは予約を使用して、MAC アドレスを DHCP サーバ内の特定の IP アドレスにマッピングするか、2) IP アドレス プールを使用して、[ホストおよびクラスター (Hosts and Clusters)] - [ホスト (*host*)] - [管理 (Manage)] - [ネットワーク (Networking)] - [仮想スイッチ (Virtual Switches)] の順に移動し、vmknics に割り当てた VTEP IP アドレスを手動で編集します。

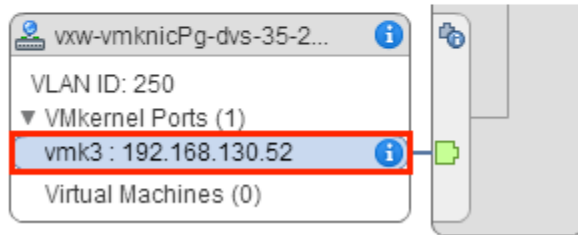
注： IP アドレスを手動で編集している場合は、IP アドレスが元の IP アドレス プール範囲に似ていないことを確認します。

次はその例です。

Distributed switch: Compute_VDS (vmk3)



Assigned port groups filter applied, showing: 5/5



- 同じ VDS のメンバーであるクラスタでは、VTEP の VLAN ID と NIC チーミングが同じでなければなりません。
- VXLAN のクラスタを準備する前に、vSphere Distributed Switch の設定をエクスポートすることをおすすめします。 <http://kb.vmware.com/kb/2034602> を参照してください。

手順

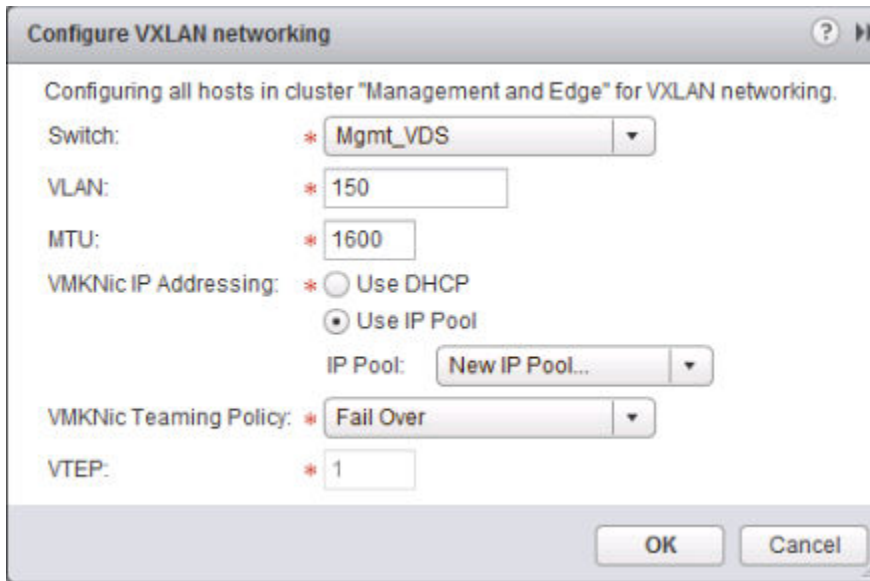
- 1 vSphere Web Client を使用して、プライマリとして使用する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] の順に移動し、[ホストの準備 (Host Preparation)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 [VXLAN] 列の [未構成 (Not Configured)] をクリックします。
- 5 論理ネットワークを設定します。

この設定では、vSphere Distributed Switch、VLAN ID、MTU サイズ、IP アドレス指定メカニズム、および NIC チーミング ポリシーを選択します。

次の画面例に示す管理クラスタの設定では、IP プール アドレス範囲 182.168.150.1 ~ 192.168.150.100、VLAN 150 でのバックギング、およびフェイルオーバー NIC チーミング ポリシーが設定されています。



Configure VXLAN networking

Configuring all hosts in cluster "Management and Edge" for VXLAN networking.

Switch: * Mgmt_VDS

VLAN: * 150

MTU: * 1600

VMKNic IP Addressing: * ☐ Use DHCP
☒ Use IP Pool

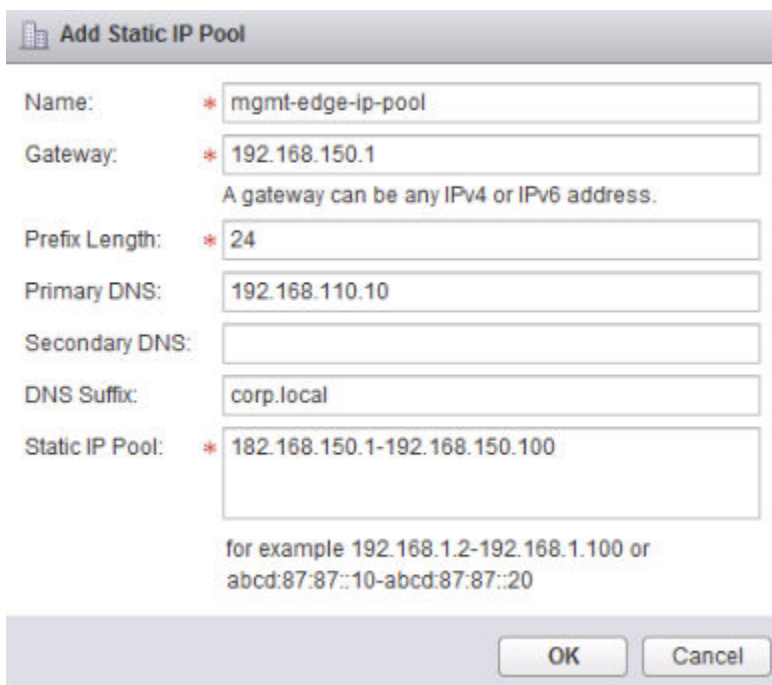
IP Pool: New IP Pool...

VMKNic Teaming Policy: * Fail Over

VTEP: * 1

OK Cancel

VTEP の数をユーザー インターフェイスで編集することはできません。VTEP 数は、準備する vSphere Distributed Switch 上の dvUplink 数と一致するように設定されます。



Add Static IP Pool

Name: * mgmt-edge-ip-pool

Gateway: * 192.168.150.1
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: * 182.168.150.1-192.168.150.100
for example 192.168.1.2-192.168.1.100 or
 abcd:87:87::10-abcd:87:87::20

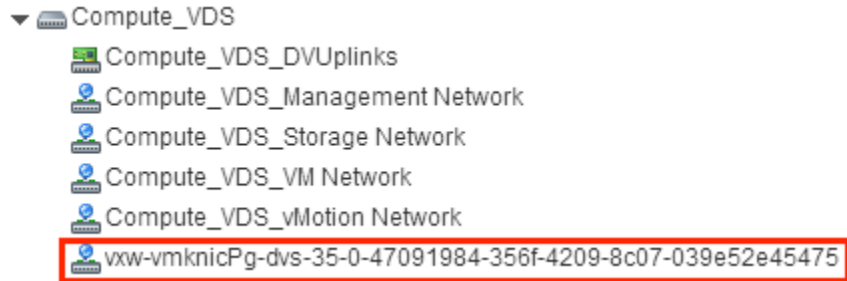
OK Cancel

コンピューティング クラスタには、別の IP アドレス設定を使用できます（たとえば 192.168.250.0/24 と VLAN 250 など）。別の設定が使用されるかどうかは物理ネットワークの設計によって異なりますが、小規模なデプロイで使用する可能性はまずありません。

結果

VXLAN を設定すると、指定した vSphere Distributed Switch 内に新しく分散ポート グループが作成されます。

次はその例です。



VXLAN のトラブルシューティングに関する詳細については、『NSX トラブルシューティング ガイド』を参照してください。

プライマリ NSX Manager へのセグメント ID プールとマルチキャスト アドレスの割り当て

VXLAN セグメントは、VXLAN トンネルとエンド ポイント (VTEP) 間で構築されます。各 VXLAN トンネルにはセグメント ID があります。プライマリ NSX Manager のセグメント ID プールを指定して、ネットワーク トラフィックを分離する必要があります。現在の環境に NSX Controller がデプロイされていない場合は、マルチキャスト アドレス範囲を追加してネットワーク全体にトラフィックが拡散するようにし、1 つのマルチキャスト アドレスが過負荷に陥るのを防ぐ必要もあります。

各セグメント ID プールのサイズを決める場合、セグメント ID 範囲で、作成できる論理スイッチの数が決まることに注意してください。16,000,000 個の VNI 候補から少量のサブセットを選択します。vCenter Server では、dvPortgroup の数が 10,000 個に制限されているため、1 つの vCenter Server で 10,000 個を超える VNI を設定しないでください。

Cross-vCenter NSX 環境の NSX Manager はすべて、重複しないセグメント ID プールを使用する必要があります。また、ユニバーサル セグメント ID プールは、Cross-vCenter NSX 環境のどのセグメント ID プールとも重複してはいけません。1 つの NSX Manager および vCenter Server 環境内では、自動的に VNI が重複しないようになっています。ただし、別々の NSX デプロイで VNI が重複していないことを確認することが重要です。一意の VNI によって追跡が容易になります。また、デプロイで Cross-vCenter NSX 環境の準備状況の確認に役立ちます。

トランスポート ゾーンのいずれかでマルチキャストまたはハイブリッドのレプリケーション モードを使用する場合は、マルチキャスト アドレスまたはマルチキャスト アドレスの範囲を追加する必要があります。

マルチキャスト アドレスの範囲を指定すると、ネットワーク全体にトラフィックが分散し、1 つのマルチキャスト アドレスへのオーバーロードを防ぐことができるほか、適切な BUM レプリケーションが含まれるようになります。

指定したマルチキャスト アドレスまたはアドレス範囲が、Cross-vCenter NSX 環境内の NSX Manager で割り当てられた他のマルチキャスト アドレスと競合しないようにする必要があります。

239.0.0.0/24 または 239.128.0.0/24 をマルチキャスト アドレス範囲として使用しないでください。これは、これらのネットワークがローカル サブネット制御に使用されるため、つまりこれらのアドレスを使用するすべてのトラフィックが物理スイッチからフラッドされるためです。使用できないマルチキャスト アドレスの詳細については、<https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01> を参照してください。

VXLAN マルチキャストおよびハイブリッド レプリケーション モードが設定されていて、適切に機能している場合、IGMP 結合メッセージを送信したホストにのみマルチキャスト トラフィックのコピーが配信されます。正しく機能していない場合は、物理ネットワークから同じブロードキャスト ドメイン内のすべてのホストにすべてのマルチキャスト トラフィックがフラッディングされます。このようなフラッディングを回避するには、次の作業を行う必要があります。

- 基盤となる物理スイッチが 1600 以上のサイズの MTU で設定されていることを確認します。
- VTEP トラフィックを伝送するネットワーク セグメントに、基盤となる物理スイッチが、IGMP スヌーピング および IGMP Querier を使用して正しく設定されていることを確認します。
- トランスポート ゾーンが、推奨されるマルチキャスト アドレス範囲で設定されていることを確認します。推奨されるマルチキャスト アドレス範囲は、239.0.1.0/24 で始まり、239.128.0.0/24 が除外されます。

vSphere Web Client インターフェイスでは、単一のセグメント ID 範囲と単一のマルチキャスト アドレスまたはマルチキャスト アドレス範囲を設定できます。複数のセグメント ID 範囲または複数のマルチキャスト アドレス範囲を設定したい場合は、NSX API を使用して設定できます。詳細については、『NSX API ガイド』を参照してください。

手順

- 1 vSphere Web Client を使用して、プライマリとして使用する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] > [Networking and Security] > [インストール手順 (Installation)] の順に移動し、[論理ネットワークの準備 (Logical Network Preparation)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 [セグメント ID (Segment ID)] > [編集 (Edit)] をクリックします。
- 5 セグメント ID の範囲 (5000–5999 など) を入力します。
- 6 (オプション) トランスポート ゾーンのいずれかでマルチキャストまたはハイブリッドのレプリケーション モードを使用する場合は、マルチキャスト アドレスまたはマルチキャスト アドレスの範囲を追加する必要があります。
 - a [マルチキャスト アドレス指定の有効化 (Enable Multicast addressing)] チェック ボックスを選択します。
 - b マルチキャスト アドレスまたはマルチキャスト アドレス範囲を入力します。例：
239.0.0.0–239.255.255.255

結果

論理スイッチを設定すると、各論理スイッチがプールからセグメント ID を受け取ります。

NSX Manager へのプライマリ ロールの割り当て

プライマリ NSX Manager はコントローラ クラスタを実行します。その他の NSX Manager はセカンダリです。プライマリ NSX Manager によってデプロイされたコントローラ クラスタは共有オブジェクトであり、ユニバーサル コントローラ クラスタと呼ばれます。セカンダリ NSX Manager はユニバーサル コントロール クラスタを自動的にインポートします。Cross-vCenter NSX 環境には、1 つのプライマリ NSX Manager と最大 7 つのセカンダリ NSX Manager を配置できます。

NSX Manager は、次の 4 つのうちの 1 つのロールを持つことができます。

- プライマリ
- セカンダリ
- スタンドアロン
- 移行

NSX Manager のロールを表示するには、NSX Manager にリンクされている vCenter Server にログインし、[ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] に移動し、[管理 (Management)] タブを選択します。[NSX Manager] セクションの [ロール] 列にロールが表示されます。[ロール] 列が表示されない場合、NSX Manager はスタンドアロン ロールを持っています。

前提条件

- NSX Manager (プライマリ NSX Manager と、セカンダリ ロールを割り当てる NSX Manager) のバージョンが一致する必要があります。
- プライマリ NSX Manager のノード ID と、セカンダリ ロールを割り当てる NSX Manager のノード ID が存在し、それらが異なる必要があります。OVA ファイルからデプロイした NSX Manager インスタンスには、一意のノード ID があります。(仮想マシンをテンプレートに変換する場合など) テンプレートからデプロイした NSX Manager のノード ID は、テンプレートを作成するために使用した元の NSX Manager のノード ID と同じです。この 2 つの NSX Manager を同じ Cross-vCenter NSX インストール内で使用できません。

注： 次の REST API 呼び出しを使用して、NSX Manager のノード ID を確認できます。

```
GET https://NSX-Manager-IP-Address/api/2.0/services/vsmconfig
```

- 各 NSX Manager を、別々の一意の vCenter Server システムに登録する必要があります。
- VXLAN で使用する UDP ポートは、すべての NSX Manager で同じである必要があります。

注： vSphere Web Client を使って VXLAN ポートを確認および変更するには、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [論理ネットワークの準備 (Logical Network Preparation)] の順に移動します。詳細については、『NSX 管理ガイド』の「VXLAN ポートの変更」を参照してください。

- NSX Manager にセカンダリ ロールを割り当てる場合、その NSX Manager にリンクされた vCenter Server システムに NSX Controller をデプロイすることはできません。

- セカンダリ ロールを割り当てる NSX Manager のセグメント ID プールが、プライマリ NSX Manager のセグメント ID プールまたは他のセカンダリ NSX Manager のセグメント ID プールと重複することはできません。
- セカンダリ ロールを割り当てる NSX Manager は、スタンドアロン ロールまたは移行ロールを持つ必要があります。

手順

- 1 vSphere Web Client を使用して、プライマリ NSX Manager にリンクされた vCenter Server にログインします。
- 2 [ホーム (Home)] > [Networking and Security] > [インストール手順 (Installation)] の順に移動して、[管理 (Management)] タブを選択します。
- 3 プライマリとして割り当てる NSX Manager を選択して、[アクション (Actions)] > [プライマリ ロールの割り当て (Assign Primary Role)] の順にクリックします。

選択した NSX Manager にプライマリ ロールが割り当てられます。Cross-vCenter NSX 環境内の他の NSX Manager はスタンドアロン ロールとして表示されます。

プライマリ NSX Manager でのユニバーサル セグメント ID プールとユニバーサル マルチキャスト アドレスの割り当て

ユニバーサル セグメント ID プールでは、論理ネットワーク セグメントの構築時に使用する範囲を指定します。Cross-vCenter NSX 環境では、すべてのセカンダリ NSX Manager でユニバーサル論理スイッチの VXLAN ネットワーク識別子 (VNI) が一致するように、一意のユニバーサル セグメント ID プールが使用されます。

ユニバーサル セグメント ID プールは、プライマリ NSX Manager で一度定義されると、セカンダリ NSX Manager と同期されます。セグメント ID 範囲は、Cross-vCenter NSX デプロイで使用するすべての NSX Manager で一意である必要があります。次の例では、今後のスケーラビリティを確保するために、上位の範囲が使用されています。

各セグメント ID プールのサイズを決める場合、セグメント ID 範囲で、作成できる論理スイッチの数が決まることに注意してください。16,000,000 個の VNI 候補から少量のサブセットを選択します。vCenter Server では、dvPortgroup の数が 10,000 個に制限されているため、1 つの vCenter Server で 10,000 個を超える VNI を設定しないでください。

VXLAN が別の NSX 環境に配置されている場合は、すでに使用されている VNI を確認して、VNI が重複しないようにしてください。1 つの NSX Manager および vCenter Server 環境内では、自動的に VNI が重複しないようになっています。ローカルの VNI 範囲を重複させることはできません。ただし、別々の NSX デプロイで VNI が重複していないことを確認することが重要です。一意の VNI は追跡に利用できます。また、デプロイが Cross-vCenter 環境用に準備できているかどうか確認する際に役立ちます。

トランスポート ゾーンのいずれかでマルチキャストまたはハイブリッドのレプリケーション モードを使用する場合は、マルチキャスト アドレスまたはマルチキャスト アドレスの範囲を追加する必要があります。

指定したマルチキャスト アドレスまたはアドレス範囲が、Cross-vCenter NSX 環境内の NSX Manager で割り当てられた他のマルチキャスト アドレスと競合しないようにする必要があります。

マルチキャスト アドレスの範囲を指定すると、ネットワーク全体にトラフィックが分散し、1 つのマルチキャスト アドレスへのオーバーロードを防ぐことができるほか、適切な BUM レプリケーションが含まれるようになります。

239.0.0.0/24 または 239.128.0.0/24 をマルチキャスト アドレス範囲として使用しないでください。これは、これらのネットワークがローカル サブネット制御に使用されるため、つまりこれらのアドレスを使用するすべてのトラフィックが物理スイッチからフラッディングされるためです。使用できないマルチキャスト アドレスの詳細については、<https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01> を参照してください。

VXLAN マルチキャストおよびハイブリッド レプリケーション モードが設定されていて、適切に機能している場合、IGMP 結合メッセージを送信したホストにのみマルチキャスト トラフィックのコピーが配信されます。正しく機能していない場合は、物理ネットワークから同じブロードキャスト ドメイン内のすべてのホストにすべてのマルチキャスト トラフィックがフラッディングされます。このようなフラッディングを回避するには、次の作業を行う必要があります。

- 基盤となる物理スイッチが 1600 以上のサイズの MTU で設定されていることを確認します。
- VTEP トラフィックを伝送するネットワーク セグメントに、基盤となる物理スイッチが、IGMP スヌーピング および IGMP Querier を使用して正しく設定されていることを確認します。
- トランスポート ゾーンが、推奨されるマルチキャスト アドレス範囲で設定されていることを確認します。推奨されるマルチキャスト アドレス範囲は、239.0.1.0/24 で始まり、239.128.0.0/24 が除外されます。

vSphere Web Client インターフェイスでは、単一のセグメント ID 範囲と単一のマルチキャスト アドレスまたはマルチキャスト アドレス範囲を設定できます。複数のセグメント ID 範囲または複数のマルチキャスト アドレス範囲を設定したい場合は、NSX API を使用して設定できます。詳細については、『NSX API ガイド』を参照してください。

手順

- 1 vSphere Web Client を使用して、プライマリとして使用する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] > [Networking and Security] > [インストール手順 (Installation)] の順に移動し、[論理ネットワークの準備 (Logical Network Preparation)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 [セグメント ID (Segment ID)] > [編集 (Edit)] をクリックします。
- 5 ユニバーサル セグメント ID の範囲 (900000-909999 など) を入力します。

注意： ユニバーサル セグメント ID の範囲が Cross-vCenter NSX 環境内の NSX Manager に割り当てられている他の範囲と重なっていないことを確認します。

- 6 (オプション) いずれかのトランスポート ゾーンでマルチキャストまたはハイブリッドのレプリケーション モードを使用する場合は、[ユニバーサル マルチキャスト アドレス指定の有効化 (Enable Universal multicast addressing)] を選択し、ユニバーサル マルチキャスト アドレスまたはユニバーサル マルチキャスト アドレスの範囲を入力します。

注意： 指定したマルチキャスト アドレスが、Cross-vCenter NSX 環境内の NSX Manager で割り当てられた他のマルチキャスト アドレスと競合しないことを確認します。

結果

ユニバーサル論理スイッチを設定した後で、各ユニバーサル論理スイッチは、プールからユニバーサル セグメント ID を受け取ります。

プライマリ NSX Manager でのユニバーサル トランスポート ゾーンの追加

ユニバーサル トランスポート ゾーンでは、ユニバーサル論理スイッチがアクセスできるホストを制御します。ユニバーサル トランスポート ゾーンは、プライマリ NSX Manager で作成されて、セカンダリ NSX Manager にレプリケートされます。ユニバーサル トランスポート ゾーンは、Cross-vCenter NSX 環境内の 1 つ以上の vSphere クラスタにまたがる可能性があります。

作成したユニバーサル トランスポート ゾーンは、Cross-vCenter NSX 環境内のすべてのセカンダリ NSX Manager で使用できます。ユニバーサル トランスポート ゾーンは 1 つしか設定できません。


前提条件

プライマリ NSX Manager を作成したら、ユニバーサル トランスポート ゾーンを設定します。

手順

- 1 vSphere Web Client を使用して、プライマリ NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール手順 (Installation)] の順に移動し、[論理ネットワークの準備 (Logical Network Preparation)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 [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。
- 5 [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。

このトランスポート ゾーンがセカンダリ NSX Manager と同期されます。

- 6 制御プレーン 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 Controller 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 サブネットに 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。

7 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。

結果

ユニバーサル トランスポート ゾーンは、Cross-vCenter NSX 環境内のすべての NSX Manager で使用できます。

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

次のステップ

次に、ユニバーサル論理スイッチを作成します。

プライマリ NSX Manager でのユニバーサル論理スイッチの追加

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。論理スイッチをユニバーサル トランスポート ゾーンに追加した場合、その論理スイッチはユニバーサルです。

論理スイッチを作成する際は、トランスポート ゾーンやレプリケーション モードの選択以外に、2 つのオプション (IP アドレス検出と MAC ラーニング) を設定します。

IP アドレス検出により、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に抑えることができます。IP アドレス検出はデフォルトで有効になっています。

注： ユニバーサル論理スイッチを作成する際に IP アドレス検出を無効にはできません。ユニバーサル論理スイッチを作成してから、API を使用して IP アドレス検出を無効にできます。この設定は各 NSX Manager で別々に管理されます。『NSX API ガイド』を参照してください。

MAC ラーニングは、VLAN/MAC ペアのラーニング テーブルを各 vNIC に作成します。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。(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 アドレスの学習を有効にできます。

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 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 ■ トランスポート ゾーンが作成されている ■ セグメント ID プールが設定されている 	<ul style="list-style-type: none"> ■ vSphere Distributed Switch が設定されている ■ NSX Manager 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 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。 ■ 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。

手順

- 1 [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 プライマリ NSX Manager を選択します。
- 3 [新規論理スイッチ (New Logical Switch)] () アイコンをクリックします。
- 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 [転送ゾーン] セクションで [変更 (Change)] をクリックし、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 ゾーンを選択して、ユニバーサル論理スイッチを作成します。

重要： 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、Cross-vCenter NSX 環境内の NSX Manager で割り当てられた他のマルチキャスト アドレスと競合しないようにする必要があります。

- 6 （オプション） トランスポート ゾーンで決定されたレプリケーション モードを上書きすることができます。

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。

作成する論理スイッチの BUM トラフィックの伝送量に関する特性が大幅に異なる場合、個々の論理スイッチの継承したトランスポート ゾーンの制御プレーン レプリケーション モードをオーバーライドする必要が生じることがあります。この場合、ユニキャスト モードとして使用するトランスポート ゾーンを作成し、個々の論理スイッチでハイブリッド モードまたはマルチキャスト モードを使用することができます。

- 7 （オプション） [MAC ラーニングの有効化 (Enable MAC learning)] をクリックします。

例： 論理スイッチとユニバーサル論理スイッチ

App 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。

Universal-App 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。

Virtual Wire ID	Segment ID	Name	Status	Transport Zone
virtualwire-1	5000	App	✓ Normal	Transport-Zone
universalwire-2	900000	Universal-App	✓ Normal	Universal-Transport-Zone

次のステップ


仮想マシンをユニバーサル論理スイッチに追加します。

また、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することで、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を接続できます。

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。

プライマリ NSX Manager でのユニバーサル分散論理ルーターの追加

ホストの分散論理ルーター 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、必要に応じて動的なルーティング機能を提供します。ユニバーサル分散論理ルーターは、ユニバーサル論理スイッチ間の水平方向ルーティングを提供します。

新しい分散論理ルーターをデプロイする際には、次のことに留意してください。

- NSX バージョン 6.2 以降では、分散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。
- 分散論理ルーター 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。

- 特定の分散論理ルーター 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分散論理ルーター インスタンスの整合性が確保されます。
- 分散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、その分散論理ルーターを 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、ホスト間で分散論理ルーター 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 の分散論理ルーター 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 の分散論理ルーター 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 の分散論理ルーター インターフェイスを作成できます。
- VXLAN が設定されている場合、分散論理ルーター インターフェイスは、VXLAN が設定されている vSphere Distributed Switch の分散ポート グループに接続されている必要があります。他の vSphere Distributed Switch のポート グループには、分散論理ルーター インターフェイスを接続しないでください。

以下のリストでは、分散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。
- 分散論理ルーターの管理インターフェイスの詳細については、ナレッジベースの記事「Management Interface Guide: DLR Control VM - NSX」(<http://kb.vmware.com/kb/2122060>) を参照してください。


重要： Cross-vCenter NSX 環境の NSX Edge で高可用性を有効にするには、アクティブとスタンバイの両方の NSX Edge アプライアンスが同じ vCenter Server 内に配置されている必要があります。高可用性の 2 台の NSX Edge のいずれかを別の vCenter Server システムに移行すると、高可用性の 2 台のアプライアンスがペアとして動作しなくなり、トラフィックの中断が発生する可能性があります。

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。
- NSX 論理スイッチを作成する予定がない場合でも、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。
- 分散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。分散論理ルーターは、NSX Controller 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。分散論理ルーターは、Edge Services Gateway (ESG) とは異なり、NSX Controller がなければ機能しません。
- 分散論理ルーターを VLAN dvPortgroup に接続する場合、分散論理ルーター 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。分散論理ルーターの VLAN ベース ARP プロキシを機能させるには、このポートで通信を行う必要があります。

- 分散論理ルーター アプライアンスの展開先を決めます。
 - 宛先のホストが、新しい分散論理ルーターのインターフェイスに接続されている論理スイッチ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。
 - ECMP セットアップで ESG を使用している場合は、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、分散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 が高可用性モードの場合は、このガイドラインは適用されません。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。
- 分散論理ルーター アプライアンスをインストールするホスト クラスタが NSX 用に準備されていることを確認します。『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。
- Local Egress（ローカル出力方向）を有効にする必要があるかどうかを判断します。Local Egress 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。ユニバーサル分散論理ルーターの作成後に Local Egress を有効にはできません。

手順

- 1 vSphere Web Client で、[ホーム(Home)] > [ネットワークとセキュリティ(Networking & Security)] > [NSX Edges] の順に移動します。
- 2 プライマリ NSX Manager を選択して、ユニバーサル分散論理ルーターを追加します。
- 3 [追加 (Add)] () アイコンをクリックします。
- 4 [ユニバーサル分散論理ルーター (Universal Logical (Distributed) Router)] を選択します。
- 5 (オプション) Local Egress（ローカル出力方向）を有効にします。
- 6 デバイスの名前を入力します。

この名前は vCenter Server 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分散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。

- 7 (オプション) Edge アプライアンスをデプロイします。

[Edge アプライアンスのデプロイ (Deploy Edge Appliance)] はデフォルトで選択されています。Edge アプライアンス（分散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分散論理ルーター アプライアンスのファイアウォールで必要になり、分散論理ルーターの 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 アプライアンスをデプロイしない場合、Edge アプライアンス オプションを選択解除できます。分散論理ルーターの作成後は、Edge アプライアンスを分散論理ルーターに追加できません。

8 (オプション) 高可用性を有効にします。

[高可用性の有効化 (Enable High Availability)] はデフォルトで選択されていません。[高可用性の有効化 (Enable High Availability)] チェック ボックスを選択し、高可用性を有効にして構成します。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。

9 分散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 つ以上の数字
- 1 文字以上の特殊文字

10 (オプション) SSH を有効にします。

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分散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 プロセスで分散論理ルーター仮想アプライアンスが実行されます。分散論理ルーターのプロトコル アドレスへの SSH アクセスを許可するには、分散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、分散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。

11 (オプション) FIPS モードを有効にして、ログ レベルを設定します。

デフォルトでは、FIPS モードは無効です。[FIPS モードの有効化 (Enable FIPS mode)] チェック ボックスを選択して、FIPS モードを有効にします。FIPS モードを有効にすると、NSX Edge が送受信するセキュアな通信はすべて、FIPS で許可される暗号化アルゴリズムまたはプロトコルを使用します。

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。

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: *

Password: *

Confirm password: *

☐ Enable SSH access

☐ Enable FIPS mode

Edge Control Level Logging EMERGENCY ▼

Set the Edge Control Level Logging

12 環境を設定します。

- ◆ [Edge アプライアンスのデプロイ (Deploy Edge Appliance)] 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。
- ◆ [Edge アプライアンスのデプロイ (Deploy Edge Appliance)] を選択した場合は、分散論理ルーター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。

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool:	*	Management & Edge ...	▼
Datastore:	*	ds-1	▼
Host:		esxmgt-01a.corp.local	▼
Folder:		Dis covered virtual mac...	▼

13 インターフェイスを設定します。分散論理ルーターでは、IPv4 アドレスのみがサポートされます。

a 高可用性インターフェイスの接続と、オプションで IP アドレスを設定します。

[Edge アプライアンスのデプロイ (Deploy Edge Appliance)] を選択した場合は、高可用性インターフェイスを分散ポート グループまたは論理スイッチに接続する必要があります。このインターフェイスを高可用性インターフェイスとしてのみ使用している場合は、論理スイッチを使用します。/30 サブネットは、リンク ローカル範囲 169.254.0.0/16 から割り当てられ、2 つの NSX Edge アプライアンスそれぞれの IP アドレスを用意するために使用されます。

オプションで、このインターフェイスを NSX Edge への接続に使用する場合は、高可用性インターフェイス用に別の IP アドレスとプリフィックスを指定できます。

注： NSX 6.2 より前のリリースでは、高可用性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。高可用性インターフェイスとは異なる IP サブネットから SSH を使用して高可用性インターフェイスに接続することはできません。高可用性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 を無効にできますが、高可用性には逆効果です。SSH アクセスには、分散論理ルーターのプロトコル アドレスも使用できます。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 以降では、分散論理ルーターの高可用性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。

b この NSX Edge のインターフェイスを設定します。

[この NSX Edge のインターフェイスを設定します (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、分散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、North - South の通信を行うためのインターフェイスです。分散論理ルーター アップリンク インターフェイスは、Edge Services Gateway またはサードパーティのルーター仮想マシンに接続する場合があります。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、分散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。分散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高可用性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

+ ✎ ✕

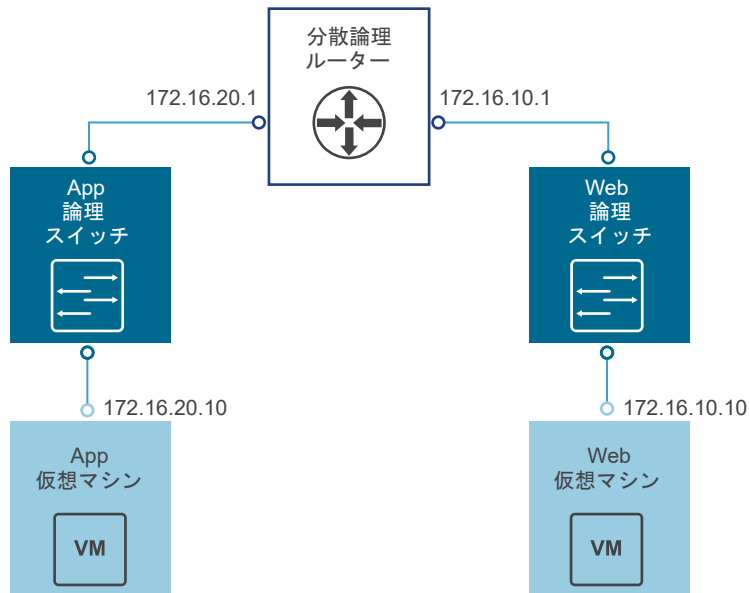
Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back Next Finish Cancel

- 14 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 ゲートウェイに分散論理ルーター 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。

結果

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 またはコンソールを使用して NSX Manager に接続し、次のコマンドを実行します。

- すべての分散論理ルーター 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 クラスタから分散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、指定した分散論理ルーター（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 ゾーンのメンバー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。

- 分散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致している必要があります。

```

nsx-mgr-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、ルーターに関する追加情報をリストします。この出力は、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 [コントローラ IP アドレス] 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に ping を送信します。

app 仮想マシンから Web 仮想マシン :

```
vmware@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 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
```

分散論理ルーター情報を確認します。各分散論理ルーター 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分散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、分散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フォワーディング テーブルとして使用するためです。

- このコントローラに接続しているすべての分散論理ルーターを一覧表示します。

```
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の間の接続は、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
5001	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202
(up)	1	0	0

注： vSphere 6.0 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 Plane (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 アドレス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。
- 分散論理ルーターが 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 ホストの分散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 アプライアンスをインストールすると、vSphere HA がクラスタ上で無効になっている場合は、NSX がホスト上での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クラスタ内の別のホストに移行すると、新しいホストでは、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、vSphere HA が無効になっているクラスタに NSX Edge アプライアンスをインストールする場合は、クラスタ内のすべてのホストをチェックして、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か確認することをお勧めします。詳細については、『vSphere 仮想マシン管理』の「仮想マシンの起動およびシャットダウン設定の編集」を参照してください。

分散論理ルーターを展開した後、分散論理ルーター 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。

セカンダリ NSX Manager の設定

7

プライマリ Cross-vCenter NSX Manager を設定したら、セカンダリ NSX Manager を設定できます。セカンダリ NSX Manager では、プライマリ NSX Manager でデプロイされたものと同じユニバーサル コントロール クラスタが使用されます。Cross-vCenter NSX 環境には、最大 7 個のセカンダリ NSX Manager を配置できます。NSX Manager にセカンダリ ロールを割り当てたら、その NSX Manager でユニバーサル論理スイッチなどのユニバーサル オブジェクトを使用できます。

Cross-vCenter NSX 環境内のセカンダリ NSX Manager ごとに構成タスクを完了します。

セカンダリ NSX Manager の追加

Cross-vCenter NSX 環境には、最大 7 個のセカンダリ NSX Manager を追加できます。プライマリ NSX Manager 上に設定されたユニバーサル オブジェクトは、セカンダリ NSX Manager に同期されます。

NSX Manager は、次の 4 つのうちの 1 つのロールを持つことができます。

- プライマリ
- セカンダリ
- スタンドアロン
- 移行

NSX Manager のロールを表示するには、NSX Manager にリンクされている vCenter Server にログインし、[ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] に移動し、[管理 (Management)] タブを選択します。[NSX Manager] セクションの [ロール] 列にロールが表示されます。[ロール] 列が表示されない場合、NSX Manager はスタンドアロン ロールを持っています。

前提条件

- 1 つのプライマリ ロールを持つ NSX Manager と、1 つのスタンドアロン ロールまたは移行ロールを持つ NSX Manager の少なくとも 2 つの NSX Manager が必要です。
- NSX Manager (プライマリ NSX Manager と、セカンダリ ロールを割り当てる NSX Manager) のバージョンが一致する必要があります。

- プライマリ NSX Manager のノード ID と、セカンダリ ロールを割り当てる NSX Manager のノード ID が存在し、それらが異なる必要があります。OVA ファイルからデプロイした NSX Manager インスタンスには、一意のノード ID があります。(仮想マシンをテンプレートに変換する場合など) テンプレートからデプロイした NSX Manager のノード ID は、テンプレートを作成するために使用した元の NSX Manager のノード ID と同じです。この 2 つの NSX Manager を同じ Cross-vCenter NSX インストール内で使用できません。

注： 次の REST API 呼び出しを使用して、NSX Manager のノード ID を確認できます。

```
GET https://NSX-Manager-IP-Address/api/2.0/services/vsmconfig
```

- 各 NSX Manager を、別々の一意の vCenter Server システムに登録する必要があります。
- VXLAN で使用する UDP ポートは、すべての NSX Manager で同じである必要があります。

注： vSphere Web Client を使って VXLAN ポートを確認および変更するには、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [論理ネットワークの準備 (Logical Network Preparation)] の順に移動します。詳細については、『NSX 管理ガイド』の「VXLAN ポートの変更」を参照してください。

- NSX Manager にセカンダリ ロールを割り当てる場合、その NSX Manager にリンクされた vCenter Server システムに NSX Controller をデプロイすることはできません。
- セカンダリ ロールを割り当てる NSX Manager のセグメント ID プールが、プライマリ NSX Manager のセグメント ID プールまたは他のセカンダリ NSX Manager のセグメント ID プールと重複することはできません。
- セカンダリ ロールを割り当てる NSX Manager は、スタンドアロン ロールまたは移行ロールを持つ必要があります。
- ユニバーサル同期を正常に機能させるには、プライマリとセカンダリの NSX Manager は同じ TLS バージョンを使用する必要があります。

プライマリ NSX Manager で設定されている 1 つ以上の TLS バージョンを使用するようにセカンダリ NSX Manager が設定されていることを確認します。『NSX 管理ガイド』の「NSX Manager での FIPS モードと TLS 設定の変更」を参照してください。

手順





- 1 プライマリ NSX Manager にリンクされた vCenter Server にログインします。
- 2 [ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] の順に移動し、[管理 (Management)] タブを選択します。
- 3 プライマリ NSX Manager を選択します。次に、[アクション (Actions)] - [セカンダリ NSX Manager の追加 (Add Secondary NSX Manager)] を選択します。
- 4 セカンダリ NSX Manager の IP アドレス、ユーザー名、およびパスワードを入力します。

注： プライマリ NSX Manager が IPv6 アドレスを使用している場合、セカンダリ NSX Manager の設定にはホスト名を使用する必要があります。

- 5 [OK] をクリックします。

- 6 証明書のサムプリントがセカンダリ NSX Manager の証明書と一致することを確認します。
- 7 登録が正常に完了すると、ロールがスタンドアロンからセカンダリに変わります。

vCenter Server システムが拡張リンク モードの場合、その vCenter Server システムに関連付けられたすべての NSX Manager のロールを [ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] タブで表示できます。

NSX Manager	Role	1 ▲ IP Address	vCenter
 192.168.110.15	Primary	192.168.110.15	 vcsa-01a.corp.local
 192.168.210.15	Secondary	192.168.210.15	 vcsa-01b.corp.local

環境で拡張リンク モードを使用していない場合は、セカンダリ NSX Manager にリンクされた vCenter Server にログインし、NSX Manager のロールを表示します。

NSX Manager のロールの変更が表示されない場合は、vSphere Web Client からログアウトし、再度ログインします。

注: 最初は、コントローラのステータスに切断と表示される可能性があります。数秒待ってから vSphere Web Client を更新すると、ステータスが標準に変わります。

セカンダリ NSX Manager でのホストの準備

ホストの準備時に、セカンダリ NSX Manager は、vCenter Server クラスタのメンバーである ESXi ホストに NSX カーネル モジュールをインストールし、NSX 制御プレーンおよび管理プレーン ファブリックを構築します。VIB ファイルにパッケージ化された NSX カーネル モジュールは、ハイパーバイザー カーネル内で実行され、分散ルーティング、分散ファイアウォール、VXLAN ブリッジ機能などのサービスを提供します。


前提条件

ホストの準備の前提条件については、[プライマリ NSX Manager でのホストの準備](#)を参照してください。

手順

- 1 vSphere Web Client を使用して、変更する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。
- 2 [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] の順に移動し、[ホストの準備 (Host Preparation)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。

- 4 NSX の論理スイッチ、論理ルーティング、論理ファイアウォールを必要とするすべてのクラスタに対し、[アクション (Actions) ()] をクリックして [インストール (Install)] をクリックします。

コンピューティング クラスタ（パイロード クラスタとも呼ばれる）は、アプリケーション仮想マシン（Web、データベースなど）を含むクラスタです。コンピューティング クラスタで NSX スイッチ、ルーティング、またはファイアウォールを使用する場合は、コンピューティング クラスタに対応する [インストール (Install)] をクリックする必要があります。

（例に示す）「管理および Edge」共有クラスタでは、NSX Manager とコントローラ仮想マシンが 1 つのクラスタを Edge デバイス（分散論理ルーター (DLR)、Edge Services Gateway (ESG) など）と共有します。この場合は、共有クラスタに対応する [インストール (Install)] をクリックすることが重要です。

逆に、管理および Edge にそれぞれ専用の共有されないクラスタがある場合（本番環境で推奨）、管理クラスタではなく Edge クラスタに対応する [インストール (Install)] をクリックします。

注： インストールの進行中は、いずれのサービスまたはコンポーネントについてもデプロイ、アップグレード、またはアンインストールしないでください。

- 5 [インストール ステータス (Installation Status)] 列に緑色のチェック マークが表示されるまで、インストールを監視します。

[インストール ステータス (Installation Status)] 列に赤の警告アイコンと [準備ができていません (Not Ready)] という表示が現れたら、[解決 (Resolve)] をクリックします。[解決 (Resolve)] をクリックすると、ホストが再起動されることがあります。インストールが依然として成功しない場合は、警告アイコンをクリックします。すべてのエラーが表示されます。必要な操作を行い、再度 [解決 (Resolve)] をクリックします。

インストールが完了すると、[インストールの状態 (Installation Status)] 列に、インストールされた NSX のバージョンとビルドが表示され、[ファイアウォール (Firewall)] 列に [有効 (Enabled)] と表示されます。いずれの列にも緑色のチェック マークが表示されます。[インストールの状態 (Installation Status)] 列に [解決] の表示がある場合は、[解決] をクリックし、ブラウザ ウィンドウを更新します。

結果

VIB がインストールされ、準備されたクラスタ内のすべてのホストに VIB が登録されます。インストールされている VIB は、インストールされている NSX と ESXi のバージョンによって異なります。

ESXi バージョン	NSX バージョン	インストールされている VIB
5.5	すべての 6.3.x	<ul style="list-style-type: none"> ■ esx-vmtoolsd ■ esx-vxlan
6.0 以降	6.3.2 以前	<ul style="list-style-type: none"> ■ esx-vmtoolsd ■ esx-vxlan
6.0 以降	6.3.3 以降	<ul style="list-style-type: none"> ■ esx-nsxv

確認するには、各ホストに SSH で接続し、`esxcli software vib list` コマンドを実行して関連する VIB を確認します。このコマンドでは、VIB のほかに、インストールされている VIB のバージョンも表示されます。

```
[root@host:~] esxcli software vib list | grep esx
esx-XXXX      6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2016-12-29
```

準備されたクラスタにホストを追加したら、NSX VIB が自動的にホストにインストールされます。

準備されていないクラスタにホストを移動すると、NSX VIB が自動的にホストからアンインストールされます。

セカンダリ NSX Manager からの VXLAN の設定

VXLAN ネットワークを使用し、ホスト間でレイヤー 2 の論理スイッチングを行うことで、基盤となる複数のレイヤー 3 ドメインにまたがることができます。VXLAN はクラスタ単位で設定します。その場合、NSX に参加する各クラスタを vSphere Distributed Switch (VDS) にマッピングします。クラスタを Distributed Switch にマップすると、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。ここで選択した設定は VMkernel インターフェイスの作成で使用されます。

前提条件

前提条件の詳細については、[プライマリ NSX Manager からの VXLAN の設定](#)を参照してください。

手順

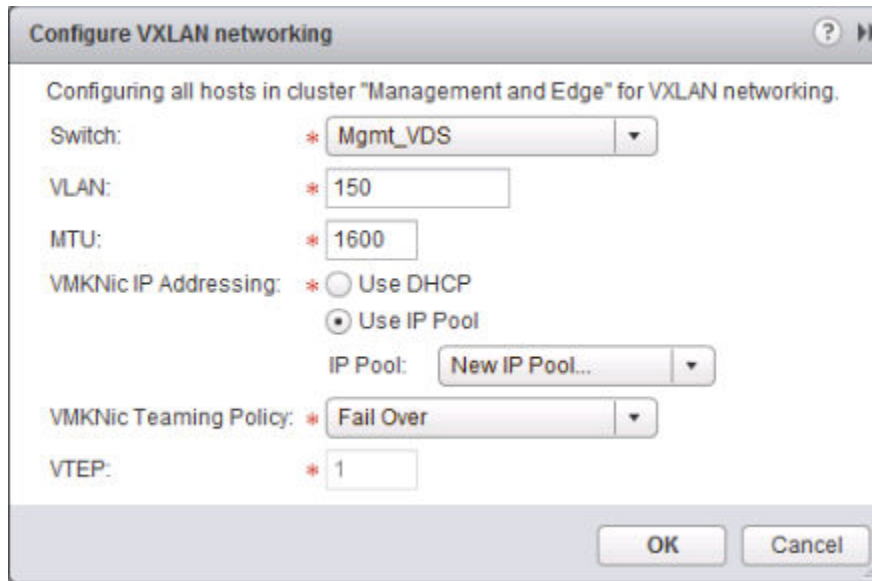
- 1 vSphere Web Client を使用して、変更する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] の順に移動し、[ホストの準備 (Host Preparation)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 [VXLAN] 列の [未構成 (Not Configured)] をクリックします。
- 5 論理ネットワークを設定します。

この設定では、vSphere Distributed Switch、VLAN ID、MTU サイズ、IP アドレス指定メカニズム、および NIC チーミング ポリシーを選択します。

次の画面例に示す管理クラスタの設定では、IP プール アドレス範囲 182.168.150.1 ~ 192.168.150.100、VLAN 150 でのバックギング、およびフェイルオーバー NIC チーミング ポリシーが設定されています。



Configure VXLAN networking

Configuring all hosts in cluster "Management and Edge" for VXLAN networking.

Switch: * Mgmt_VDS

VLAN: * 150

MTU: * 1600

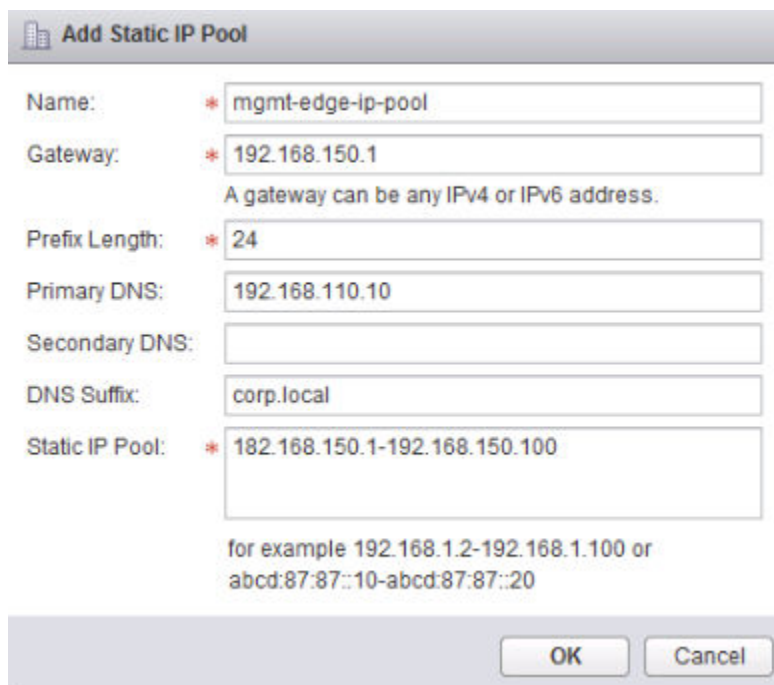
VMKNic IP Addressing: * ☐ Use DHCP
☒ Use IP Pool
 IP Pool: New IP Pool...

VMKNic Teaming Policy: * Fail Over

VTEP: * 1

OK Cancel

VTEP の数をユーザー インターフェイスで編集することはできません。VTEP 数は、準備する vSphere Distributed Switch 上の dvUplink 数と一致するように設定されます。



Add Static IP Pool

Name: * mgmt-edge-ip-pool

Gateway: * 192.168.150.1
 A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: * 182.168.150.1-192.168.150.100
 for example 192.168.1.2-192.168.1.100 or
 abcd:87:87::10-abcd:87:87::20

OK Cancel

コンピューティング クラスタには、別の IP アドレス設定を使用できます（たとえば 192.168.250.0/24 と VLAN 250 など）。別の設定が使用されるかどうかは物理ネットワークの設計によって異なりますが、小規模なデプロイで使われる可能性はまずありません。

セカンダリ NSX Manager へのセグメント ID プールとマルチキャスト アドレスの割り当て

セカンダリ NSX Manager には、プライマリ NSX Manager から同期されたユニバーサル セグメント ID プールが表示されます。また、セカンダリ NSX Manager にローカルなセグメント ID プールを作成できます。これを使用して、その NSX Manager にローカルな論理スイッチを作成します。ユニバーサル論理スイッチのみを作成する場合、セカンダリ NSX Manager にローカルなセグメント ID プールを追加する必要はありません。

前提条件

セグメント ID プールおよびマルチキャスト アドレスの計画に関する前提条件とガイダンスについては、[プライマリ NSX Manager へのセグメント ID プールとマルチキャスト アドレスの割り当て](#)を参照してください。

手順

- 1 vSphere Web Client を使用して、変更する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [論理ネットワークの準備 (Logical Network Preparation)] の順にクリックし、[セグメント ID (Segment ID)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 ローカル セグメント ID の範囲を入力します (20000 ~ 29999 など)。

注意： 指定するローカルおよびユニバーサルの各セグメント ID 範囲は、重複することはできません。

- 5 (オプション) いずれかのトランスポート ゾーンでマルチキャストまたはハイブリッドのレプリケーション モードを使用する場合は、[マルチキャスト アドレス指定の有効化 (Enable multicast addressing)] を選択し、マルチキャスト アドレスまたはマルチキャスト アドレスの範囲を入力します。

注意： 指定したマルチキャスト アドレスが、Cross-vCenter NSX 環境内の NSX Manager で割り当てられた他のマルチキャスト アドレスと競合しないことを確認します。

結果

これで、セカンダリ NSX Manager には、プライマリ NSX Manager から提供されたインポート済みのユニバーサル セグメント ID と、ローカル セグメント ID の両方が設定されます。


ユニバーサル トランスポート ゾーンへのクラスタの追加

セカンダリ NSX Manager に関連付けられたクラスタを、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。これにより、このようなクラスタ上にある仮想マシンをユニバーサル論理スイッチに接続できます。

手順

- 1 vSphere Web Client を使用して、変更する NSX Manager に登録されている vCenter Server システムにログインします。

Cross-vCenter NSX 環境内の vCenter Server システムが拡張リンク モードになっている場合は、リンクされた vCenter Server システムの [NSX Manager] ドロップダウン メニューから関連する NSX Manager を選択することで、その NSX Manager にアクセスできます。

- 2 [ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [論理ネットワークの準備 (Logical Network Preparation)] の順にクリックし、[トランスポート ゾーン (Transport Zones)] タブを選択します。
- 3 [NSX Manager] ドロップダウン メニューで、適切な NSX Manager が選択されていることを確認します。
- 4 ユニバーサル トランスポート ゾーンを選択し、[アクション () (Actions)] - [クラスタの接続 (Connect Clusters)] をクリックします。ユニバーサル 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。

プライマリおよびセカンダリ NSX Manager 設定後の作業

8

プライマリ NSX Manager と 1 台以上のセカンダリ NSX Manager が構成されました。プライマリ NSX Manager でユニバーサル オブジェクトを作成するだけでなく、特定の vCenter Server NSX 環境向けに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、Edge Services Gateway など）を作成することもできます。ローカルなオブジェクトは、プライマリまたはセカンダリの NSX Manager 上で作成できます。それらのオブジェクトは、作成された vCenter Server NSX 環境内にのみ存在するようになります。Cross-vCenter NSX 環境の他の NSX Manager では表示されません。また、クラスタにホストを追加したり、クラスタからホストを削除することができます。

実行が必要な追加の管理タスクの詳細については、『NSX 管理ガイド』を参照してください。

NSX コンポーネントのアンインストール

9

この章では、vCenter Server インベントリから NSX コンポーネントをアンインストールする際に必要なステップについて説明します。

注： NSX によってデプロイされたアプライアンス（コントローラや Edge など）を vCenter Server から直接削除しないでください。NSX アプライアンスの管理と削除は、必ず vSphere Web Client の [Networking and Security (Networking & Security)] タブから行ってください。

この章には、次のトピックが含まれています。

- [NSX を使用するクラスタからのホストの削除](#)
- [NSX Edge Services Gateway または分散論理ルーターのアンインストール](#)
- [論理スイッチのアンインストール](#)
- [ホスト クラスタからの NSX のアンインストール](#)
- [NSX 環境の安全な削除](#)

NSX を使用するクラスタからのホストの削除

このセクションでは、ネットワーク仮想化の準備ができているクラスタからホストを削除する手順を説明します。たとえば、ホストを NSX に参加させない場合は、そのホストを削除することができます。

重要： ホストに NSX 6.3.0 以降および ESXi 6.0 以降がインストールされている場合、VIB のアンインストール時にホストを再起動する必要はありません。それより前のバージョンの NSX および ESXi の場合、VIB のアンインストールを完了するには再起動が必要です。

手順

- 1 ホストをメンテナンス モードにして、DRS によるホストの退避を待つか、vMotion を使用して、稼働中の仮想マシンをホストから手動で移動します。
- 2 ホストを未準備のクラスタに移動するか、クラスタに所属しないスタンドアロン ホストにして、ホストを準備済みクラスタから削除します。

NSX により、ネットワーク仮想コンポーネントとサービス仮想マシンがホストからアンインストールされます。

- 3 ホストに NSX 6.2.x 以前、または ESXi 5.5 がインストールされている場合は、ホストを再起動します。

- 4 VIB のアンインストールが完了したことを確認します。
 - a vSphere Web Client の [最近のタスク] ペインを確認します。
 - b [ホストの準備 (Host Preparation)] タブで、ホストが削除されたクラスタの [インストール ステータス] に緑色のチェックマークが付いていることを確認します。

[インストール ステータス] が インストールしています である場合、アンインストールはまだ進行中です。
- 5 アンインストールが完了したら、ホストのメンテナンス モードを終了します。

結果

NSX VIB がホストから削除されます。確認のために、ホストに SSH で接続し、`esxcli software vib list | grep esx` コマンドを実行します。次の VIB がホストに存在しないことを確認します。

- esx-vmtoolsd
- esx-vxlan

VIB がホストに残っている場合は、ログを表示して、VIB の自動削除が機能しなかった理由を確認できます。

次のコマンドを実行して、VIB を手動で削除できます。

- `esxcli software vib remove --vibName=esx-vxlan`
- `esxcli software vib remove --vibName=esx-vmtoolsd`

NSX Edge Services Gateway または分散論理ルーターのアンインストール

vSphere Web Client を使用して、NSX Edge をアンインストールできます。

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。

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 を選択し、[削除 (Delete)] (✖) アイコンをクリックします。

論理スイッチのアンインストール


論理スイッチをアンインストールする前に、その論理スイッチからすべての仮想マシンを削除する必要があります。Cross-vCenter NSX 環境では、すべての NSX Manager 上のユニバーサル論理スイッチから、すべての仮想マシンを削除する必要があります。

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。

手順

- 1 vSphere Web Client で、[ホーム(Home)] > [ネットワークとセキュリティ(Networking & Security)] > [論理スイッチ(Logical Switches)] の順に移動します。
- 2 論理スイッチから仮想マシンをすべて削除します。

- a 1 台の論理スイッチを選択し、[仮想マシンの削除] アイコン ([]) をクリックします。
- b すべての仮想マシンを [使用可能なオブジェクト] から [選択したオブジェクト] に移動し、[OK] をクリックします。

ユニバーサル論理スイッチをアンインストールする場合、プライマリ NSX Manager とセカンダリ NSX Manager 上のユニバーサル論理スイッチに仮想マシンが接続されている可能性があります。Cross-vCenter NSX 環境内のすべての NSX Manager で前述の手順を繰り返し、ユニバーサル論理スイッチからすべての仮想マシンを削除します。

- 3 論理スイッチを選択した状態で、[削除 (Delete)] () アイコンをクリックします。

ユニバーサル分散分散論理ルーターをアンインストールする場合、プライマリ NSX Manager からユニバーサル分散論理ルーターを削除する必要があります。

ホスト クラスタからの NSX のアンインストール

NSX は、クラスタ内のすべてのホストからアンインストールできます。

クラスタ全体からではなく、NSX を個々のホストから削除する場合は、[NSX を使用するクラスタからのホストの削除](#)を参照してください。

前提条件


- クラスタの仮想マシンを論理スイッチから切断します。

手順

- 1 トランスポート ゾーンからクラスタを削除します。

[論理ネットワークの準備 (Logical Network Preparation)] > [トランスポート ゾーン (Transport Zones)] の順に移動して、トランスポート ゾーンからクラスタを切断します。

クラスタがグレイアウトされていてトランスポート ゾーンから削除できない場合、原因として 1) クラスタ内のホストが切断されているかパワーオン状態でない、または 2) トランスポート ゾーンに接続された仮想マシンまたはアプライアンスが 1 台以上クラスタに含まれていることが考えられます。たとえば、ホストが管理クラスタに含まれ、そのホストに NSX Controller がインストールされている場合は、最初にコントローラを削除または移動します。

- 2 NSX VIB をアンインストールします。vSphere Web Client で [Networking and Security] > [インストール (Installation)] > [ホストの準備 (Host Preparation)] の順に移動します。クラスタを選択し、[アクション (Actions)] () をクリックして、[アンインストール (Uninstall)] を選択します。

[インストール ステータス] に [準備ができていません (Not Ready)] と表示されています。[準備ができていません (Not Ready)] をクリックすると、ダイアログ ボックスに「エージェント VIB のインストールを完了するには、ホストをメンテナンス モードにする必要があります」という内容のメッセージが表示されます。

- 3 クラスタを選択し、[解決 (Resolve)] アクションをクリックして、アンインストールを完了します。

- ホストに NSX 6.2.x 以前、または ESXi バージョン 5.5 がインストールされている場合、アンインストールを完了するには再起動が必要になります。クラスタで DRS が有効になっている場合は、DRS は、仮想マシンの動作を停止しない制御された方法で、ホストの再起動を試みます。何らかの理由で DRS の操作が失敗した場合、[解決 (Resolve)] アクションは停止します。この場合、仮想マシンを手動で移動して、[解決 (Resolve)] アクションをもう一度実行するか、ホストを手動で再起動する必要があります。
- ホストに NSX 6.3.0 以降、および ESXi 6.0 以降がインストールされている場合、アンインストールを完了するには、ホストをメンテナンス モードに切り替える必要があります。クラスタで DRS が有効になっている場合、DRS は、仮想マシンの動作を停止しない制御された方法で、ホストをメンテナンス モードに切り替えようとします。何らかの理由で DRS の操作が失敗した場合、[解決 (Resolve)] アクションは停止します。この場合、仮想マシンを手動で移動して、[解決 (Resolve)] アクションをもう一度実行するか、ホストを手動でメンテナンス モードにする必要があります。

重要： ホストを手動でメンテナンス モードにした場合、ホストの VIB アンインストールが完了していることを確認してから、ホストのメンテナンス モードを終了してください。

- a vSphere Web Client の [最近のタスク] ペインを確認します。
- b [ホストの準備 (Host Preparation)] タブで、ホストが削除されたクラスタの [インストール ステータス] に緑色のチェックマークが付いていることを確認します。

[インストール ステータス] が インストールしています である場合、アンインストールはまだ進行中です。

NSX 環境の安全な削除

NSX を完全にアンインストールすると、ホスト VIB、NSX Manager、コントローラ、すべての VXLAN の設定、論理スイッチ、分散論理ルーター、NSX ファイアウォール、および vCenter Server NSX プラグインが削除されます。クラスタ内のすべてのホストで、次の手順を必ず実行してください。vCenter Server から NSX プラグインを削除する前に、クラスタからネットワーク仮想化コンポーネントをアンインストールすることをお勧めします。

注： NSX Edge アプライアンスなど、NSX によって作成されたアプライアンスを vCenter Server から直接削除しないでください。これらのアプライアンスの管理と削除は、必ず vSphere Web Client の [Networking and Security] タブから行ってください。

前提条件

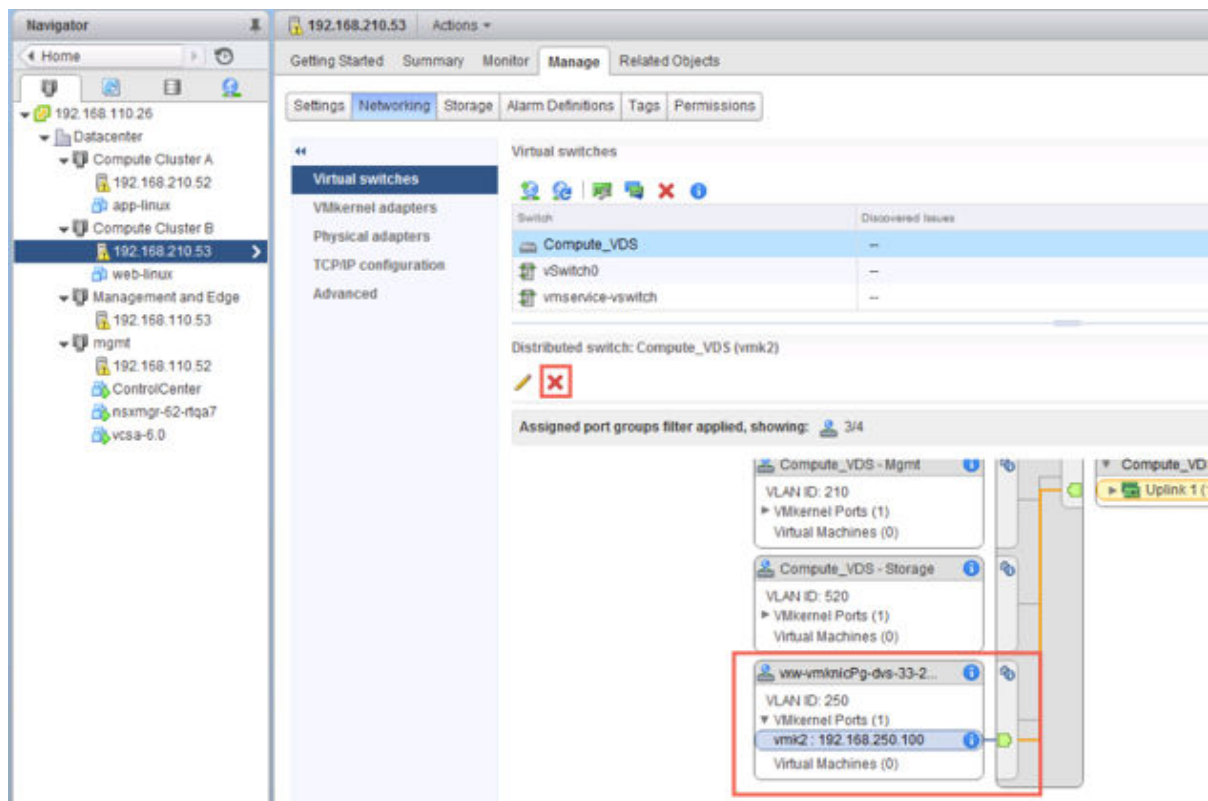
- Enterprise Administrator または NSX Administrator のロールが割り当てられている必要があります。

- ホストの準備を取り消す前に、登録されているパートナー ソリューション、およびエンドポイント サービスを削除して、クラスタ内のサービス仮想マシンが正常に削除されるようにします。
- すべての NSX Edge を削除します。[NSX Edge Services Gateway](#) または分散論理ルーターのアンインストールを参照してください。
- トランスポート ゾーンの仮想マシンを論理スイッチから接続解除して、論理スイッチを削除します。[論理スイッチのアンインストール](#)を参照してください。
- NSX をホスト クラスタからアンインストールします。[ホスト クラスタからの NSX のアンインストール](#)を参照してください。

手順

- 1 トランスポート ゾーンを削除します。
- 2 NSX Manager アプライアンス、およびすべての NSX Controller アプライアンス仮想マシンをディスクから削除します。
- 3 残りの VTEP VMkernel インターフェイスを削除します。

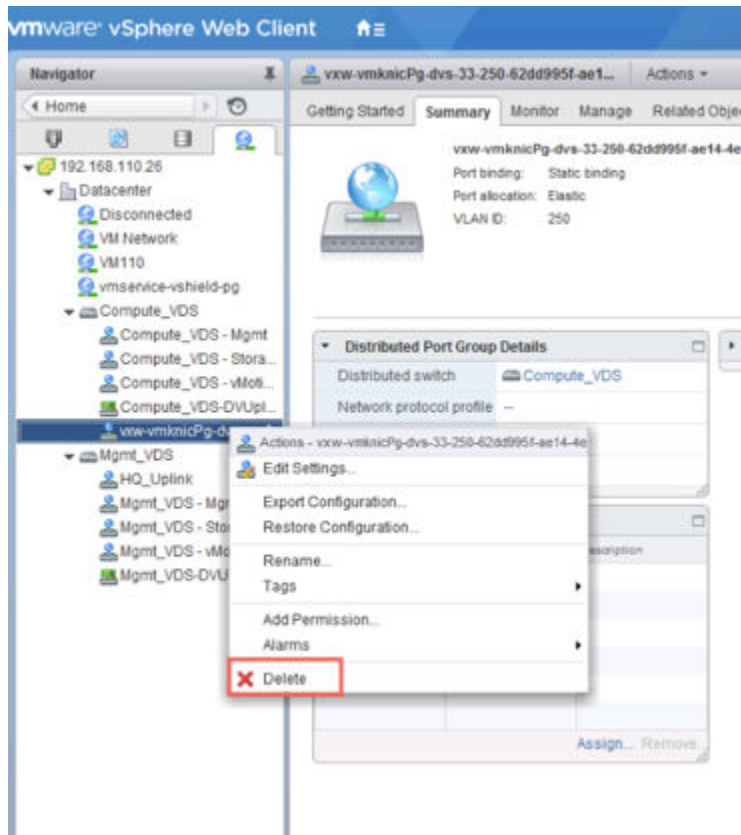
次はその例です。



VTEP VMkernel インターフェイスは、通常、これより前のアンインストール操作で削除されています。

- 4 VTEP で使用されている残りの dvPortgroup を削除します。

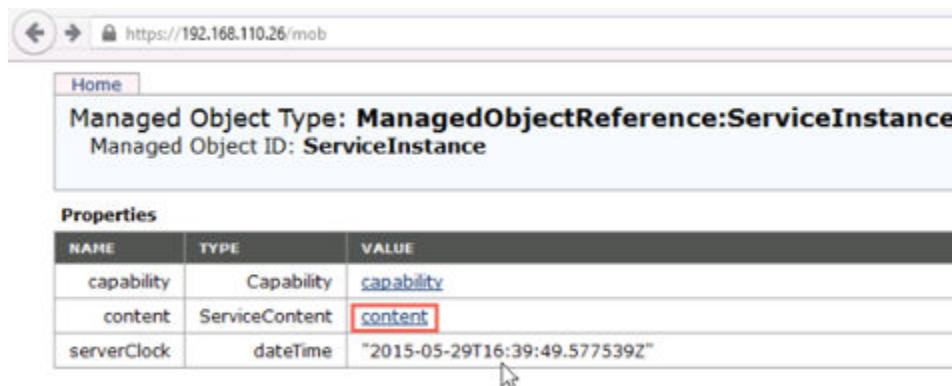
次はその例です。



VTEP で使用されている dvPortgroup は、通常、これより前のアンインストール操作ですでに削除されています。

- 5 VTEP vmkernel インターフェイスまたは dvPortgroup を削除した場合、ホストを再起動してください。
- 6 NSX Manager プラグインを削除する vCenter Server で、https://your_vc_server/mob の管理対象オブジェクト ブラウザにログインします。
- 7 [[Content] (Content)] をクリックします。

次はその例です。



8 [ExtensionManager] をクリックします。

← → https://192.168.110.26/mob/?moid=ServiceInstance&doPath=content

Home

Data Object Type: ServiceContent
Parent Managed Object ID: **ServiceInstance**
Property Path: **content**

Properties

NAME	TYPE	VALUE
about	AboutInfo	about
accountManager	ManagedObjectReference:HostLocalAccountManager	Unset
alarmManager	ManagedObjectReference:AlarmManager	AlarmManager
authorizationManager	ManagedObjectReference:AuthorizationManager	AuthorizationManager
certificateManager	ManagedObjectReference:CertificateManager	certificateManager
clusterProfileManager	ManagedObjectReference:ClusterProfileManager	ClusterProfileManager
complianceManager	ManagedObjectReference:ProfileComplianceManager	MoComplianceManager
customFieldsManager	ManagedObjectReference:CustomFieldsManager	CustomFieldsManager
customizationSpecManager	ManagedObjectReference:CustomizationSpecManager	CustomizationSpecManager
datastoreNamespaceManager	ManagedObjectReference:DatastoreNamespaceManager	DatastoreNamespaceManager
diagnosticManager	ManagedObjectReference:DiagnosticManager	DiagMgr
dvSwitchManager	ManagedObjectReference:DistributedVirtualSwitchManager	DVSManager
eventManager	ManagedObjectReference:EventManager	EventManager
extensionManager	ManagedObjectReference:ExtensionManager	ExtensionManager
fileManager	ManagedObjectReference:FileManager	FileManager
guestOperationsManager	ManagedObjectReference:GuestOperationsManager	guestOperationsManager
hostProfileManager	ManagedObjectReference:HostProfileManager	HostProfileManager

9 [UnregisterExtension] をクリックします。

Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ExtensionManagerIpAllocationUsage[]	QueryExtensionIpAllocationUsage
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

- 10 文字列 [com.vmware.vShieldManager] を入力して、[Invoke Method] をクリックします。

Managed Object Type:
ManagedObjectReference:ExtensionManager
 Managed Object ID: **ExtensionManager**
 Method: **UnregisterExtension**

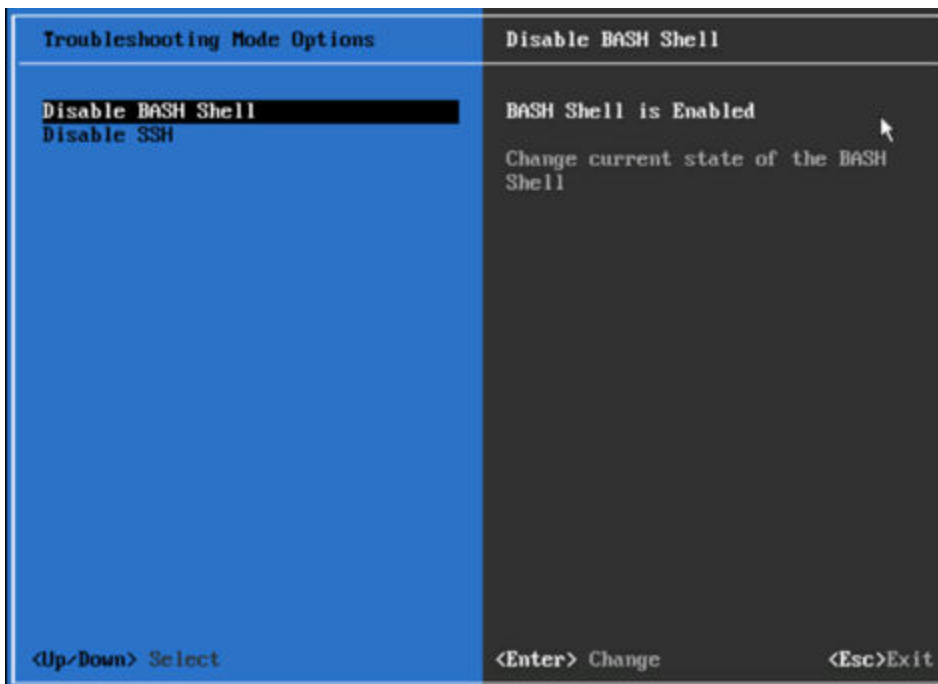
void UnregisterExtension

Parameters

NAME	TYPE	VALUE
extensionKey (required)	string	com.vmware.vShieldManager

[Invoke Method](#)

- 11 vSphere 6 vCenter Server Appliance が動作している場合は、コンソールを起動し、[トラブルシューティング モード オプション (Troubleshooting Mode Options)] で BASH シェルを有効にしてください。



root としてログインし、`shell.set --enabled true` コマンドを実行する方法もあります。

- 12 NSX の vSphere Web Client ディレクトリを削除して、Web Client サービスを再起動します。

NSX の vSphere Web Client ディレクトリは `com.vmware.vShieldManager.**` であり、次の場所にあります。

- vCenter Server 5.x
 - Windows 2003 – %ALLUSERSPROFILE%\Application Data\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\

- Windows 2008/2012 – %ALLUSERSPROFILE%\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\
- VMware vCenter Server Appliance – /var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
- vCenter Server 6.0.x
 - Windows 2008/2012 – C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\
 - VMware vCenter Server Appliance – /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/

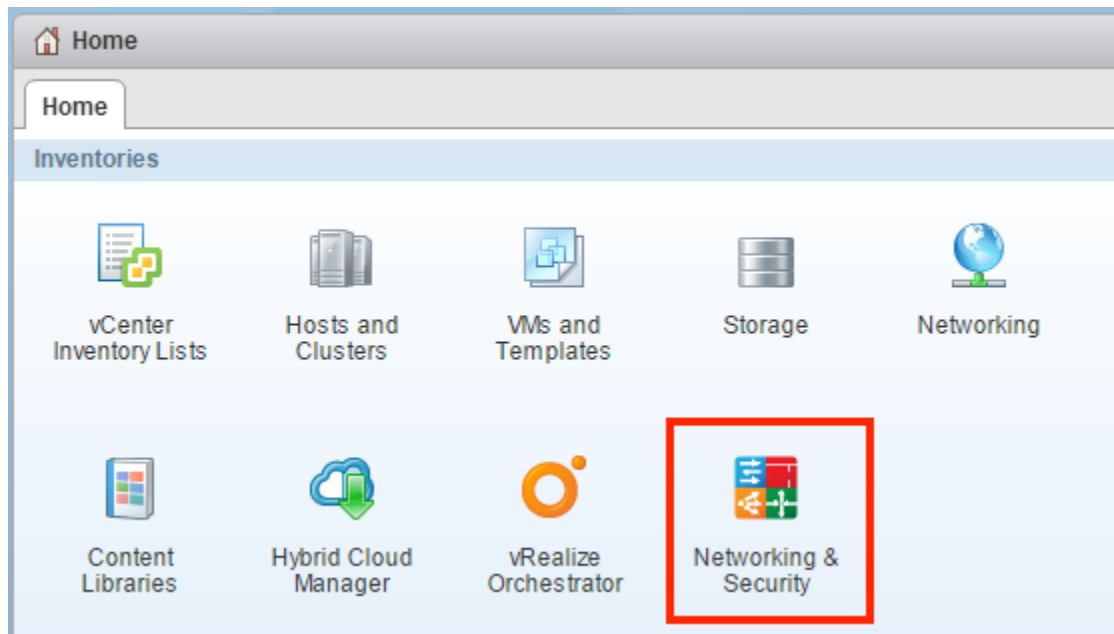
vCenter Server Appliance の場合は、アプライアンス シェルで `service vsphere-client restart` コマンドを実行します。

Windows ベースの vCenter Server の場合は、`services.msc` を実行して、[vSphere Web Client] を右クリックし、[開始 (Start)] をクリックします。

結果

NSX Manager プラグインは vCenter Server から削除されます。確認するには、vCenter Server をログアウトして、再度ログインします。

NSX Manager プラグイン [Networking and Security (Networking & Security)] アイコンが、vSphere Web Client のホーム画面に表示されなくなります。



[管理 (Administration)] > [クライアント プラグイン (Client Plug-Ins)] に移動して、プラグインのリストに [NSX ユーザー インターフェイス プラグイン (NSX User Interface plugin)] が含まれていないことを確認します。

