

NSX インストール ガイド

Update 3

変更日：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

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

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

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

docfeedback@vmware.com

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

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

Copyright © 2010 年～2016 年 VMware, Inc. All rights reserved. [著作権および商標](#).

内容

NSX インストール ガイド 5

1 NSX の概要 6

NSX コンポーネント 7

NSX Edge 10

NSX Services 13

2 インストールの準備 15

NSX のシステム要件 15

NSX で必要となるポートおよびプロトコル 17

NSX と vSphere Distributed Switch 19

例 : vSphere Distributed Switch の操作 21

NSX のインストール ワークフローとトポロジの例 28

Cross-vCenter NSX および拡張リンク モード 31

3 NSX Manager 仮想アプライアンスのインストール 32

4 NSX Manager への vCenter Server の登録 37

5 Single Sign-On の設定 41

6 Syslog サーバの指定 44

7 NSX for vSphere のライセンスのインストールと割り当て 46

8 NSX コントローラ クラスタの展開 48

9 ファイアウォールによる保護からの仮想マシンの除外 51

10 NSX 用ホスト クラスタの準備 53

11 準備済みクラスタへのホストの追加 58

12 NSX を使用するクラスタからのホストの削除 59

13 VXLAN 転送パラメータの設定 60

14 セグメント ID プールとマルチキャスト アドレス範囲の割り当て 65

- 15 トランスポート ゾーン の追加 68
- 16 論理スイッチの追加 73
- 17 分散論理ルーターの追加 81
- 18 Edge Services Gateway の追加 94
- 19 論理（分散）ルーター上での OSPF の設定 105
- 20 Edge Services Gateway 上での OSPF の設定 111
- 21 ゲスト イントロスペクション のインストール 118
- 22 NSX Data Security のインストール 121
- 23 NSX コンポーネントのアンインストール 123
 - NSX Edge Services Gateway または分散論理ルーターのアンインストール 123
 - 論理スイッチのアンインストール 123
 - NSX インストールの安全な削除 124

NSX インストール ガイド

この『NSX インストール ガイド』では、vSphere Web Client を使用して VMware[®] NSX[™] システム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、VMware vCenter Server 環境で NSX をインストールまたは使用するユーザーを対象としています。本書に記載されている情報は、システム管理者としての経験があり、仮想マシン テクノロジーおよび仮想データセンターの操作に詳しい方を対象としています。また、本書は VMware ESX、vCenter Server、vSphere Web Client を含む VMware vSphere 5.5 または 6.0 についての知識も前提としています。

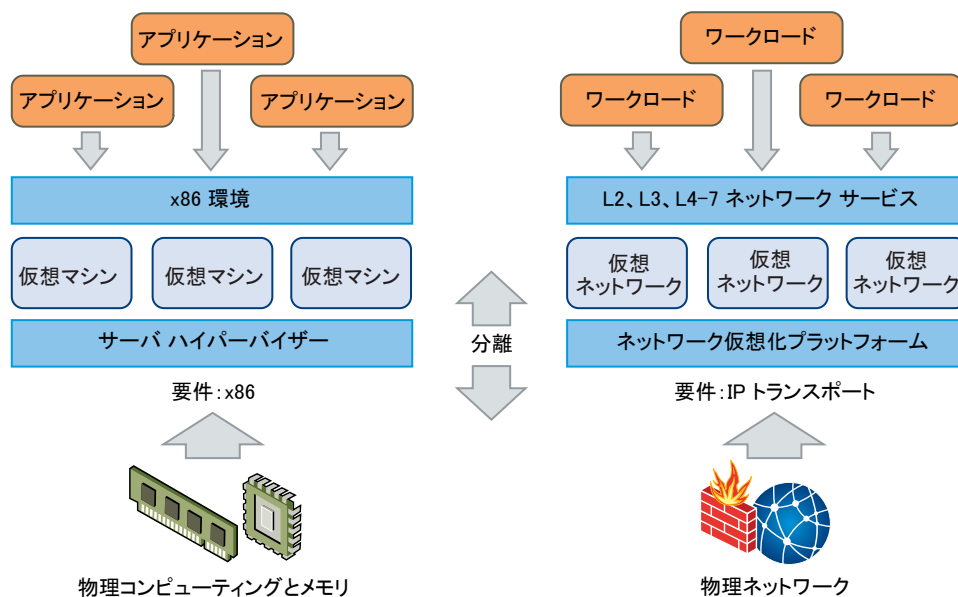
VMware の技術ドキュメントの用語集

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

NSX の概要

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

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



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

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

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

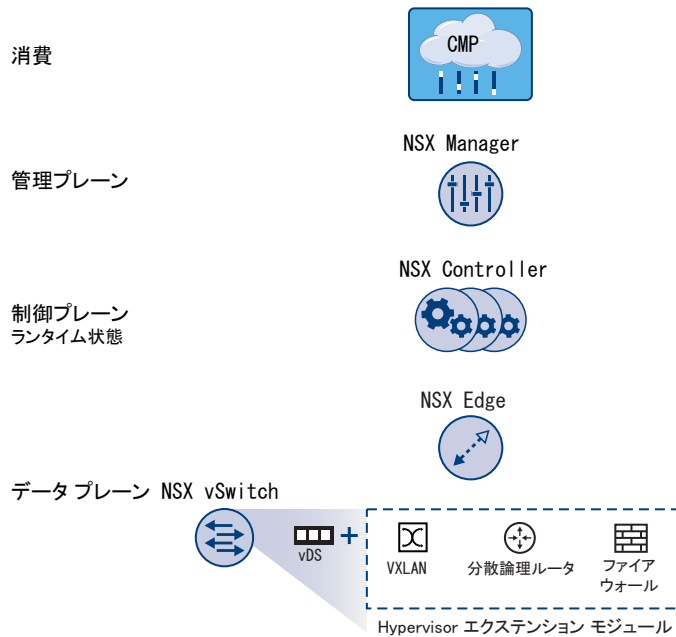
NSX は、vSphere Web Client、コマンドライン インターフェイス (CLI)、および REST API を使用して設定できます。

この章には、次のトピックが含まれています。

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

NSX コンポーネント

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



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

データ プレーン

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

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

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

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

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

制御プレーン

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

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

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

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

コントローラ クラスタには、以下に示すいくつかのロールがあります。

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

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

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

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

管理プレーン

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

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

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

使用プラットフォーム

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

NSX Edge

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

Edge Services Gateway

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

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

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

分散論理ルーター

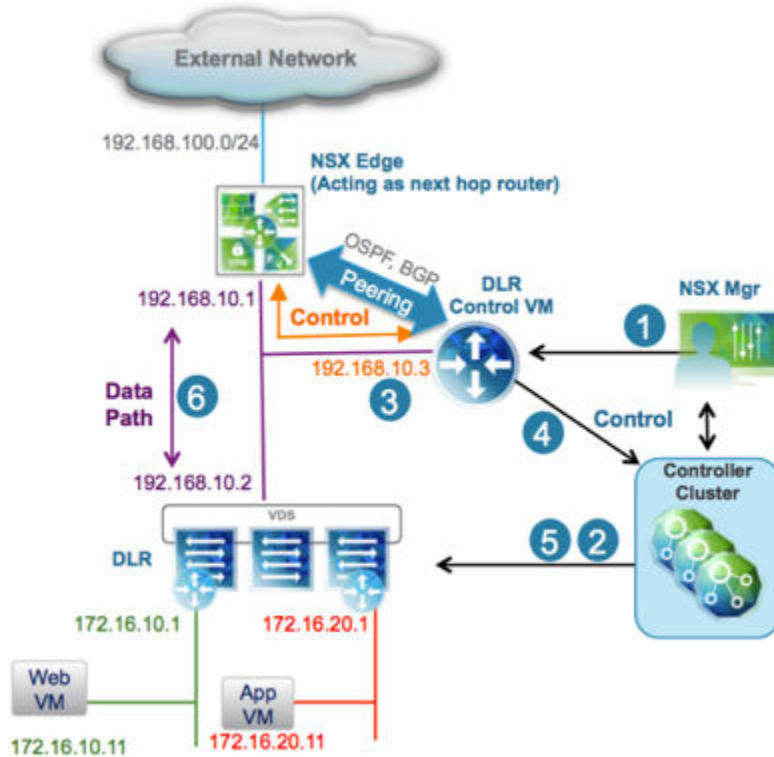
分散論理ルーターは、テナント IP アドレス空間とデータ パス分離による水平方向の分散ルーティングを提供します。複数のサブネットにわたっている同一ホスト上に存在する仮想マシンまたはワークロードは、従来のルーティング インターフェイスをトラバースすることなく相互に通信できます。

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

分散論理ルーターには、以下の 2 つの主なコンポーネントがあります。

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

図 1-1. 論理ルーティング コンポーネント



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

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

NSX Services

NSX コンポーネントは連携して、次の機能的なサービスを提供します。

論理スイッチ

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

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

分散論理ルーター

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

論理ファイアウォール

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

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

論理 Virtual Private Network (VPN)

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

論理ロード バランサ

NSX Edge ロード バランサは、単一の仮想 IP アドレス (VIP) を対象とするクライアント接続を、ロード バランシング プールのメンバーとして設定された複数のターゲットに分散します。受信サービス リクエストは、負荷配分がユーザーにとって透過的になるように、複数のサーバ間で均等に配分されます。このように、ロード バランシングは、最適なリソース使用率の実現、スループットの最大化、応答時間の最小化、過負荷の回避に役立ちます。

Service Composer

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

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

NSX の拡張性

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

インストールの準備

このセクションでは、NSX 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 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。1 台の vCenter Server につき NSX Manager が 1 台、1 台の ESXi™ ホストにつきゲスト イントロスペクションと Data Security のインスタンスが 1 つ、1 つのデータセンターにつき NSX Edge インスタンスを複数インストールできます。

ハードウェア

表 2-1. ハードウェア要件

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

表 2-1. 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
ゲスト イントロス ベクション	1 GB	2	4 GB
NSX Data Security	512 MB	1	ESXi ホスト 1 台あたり 6 GB

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

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

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

ソフトウェア

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

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

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

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

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

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

クライアントとユーザー アクセス

- vSphere インベントリに ESXi ホスト名を追加している場合は、正引き/逆引きの名前解決が機能していることを確認してください。機能していない場合、NSX Manager は IP アドレスを解決できません。
- 仮想マシンを追加、パワーオンの権限

- 仮想マシンのファイルを保存するデータストアへのアクセス、そのデータストアにファイルをコピーするためのアカウント権限
- NSX Manager ユーザー インターフェイスにアクセスするための Web ブラウザでの Cookie の有効化
- ESXi ホスト、vCenter Server、および展開する NSX アプライアンスからポート 443 にアクセスできることを、NSX Manager で確認します。このポートは、ESXi ホストから OVF ファイルをダウンロードして展開するために必要です。
- 使用している vSphere Web Client のバージョンでサポートされている Web ブラウザは次のとおりです。詳細については、『vCenter Server およびホスト管理』ドキュメントの「vSphere Web Client の使用」を参照してください。

NSX で必要となるポートおよびプロトコル

NSX が正常に機能するには、次のポートが開いている必要があります。

表 2-2. NSX で必要となるポートおよびプロトコル

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

表 2-2. NSX で必要となるポートおよびプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
NSX Manager	DNS サーバ	53	TCP	DNS クライアント接続	×	×	
NSX Manager	DNS サーバ	53	UDP	DNS クライアント接続	×	×	
NSX Manager	Syslog サーバ	514	TCP	Syslog 接続	×	×	
NSX Manager	Syslog サーバ	514	UDP	Syslog 接続	×	×	
NSX Manager	NTP タイム サーバ	123	TCP	NTP クライアント接続	×	○	
NSX Manager	NTP タイム サーバ	123	UDP	NTP クライアント接続	×	○	
vCenter Server	NSX Manager	80	TCP	ホストの準備	×	○	
REST Client	NSX Manager	443	TCP	NSX Manager REST API	×	○	ユーザー/パスワード
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (NSX 6.2.3 より前のデフォルト) または 4789 (NSX 6.2.3 以降の新規インストールのデフォルト)	UDP	VTEP 間の転送ネットワークのカプセル化	×	○	
ESXi ホスト	ESXi ホスト	6999	UDP	VLAN LIF 上の ARP	×	○	
ESXi ホスト	NSX Manager	8301, 8302	UDP	分散仮想スイッチ同期	×	○	
NSX Manager	ESXi ホスト	8301, 8302	UDP	分散仮想スイッチ同期	×	○	
ゲストイントロセクション仮想マシン	NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
プライマリ NSX Manager	セカンダリ NSX Manager	443	TCP	Cross-vCenter NSX ユニバーサル同期サービス	×	○	
プライマリ NSX Manager	vCenter Server	443	TCP	vSphere API	×	○	
セカンダリ NSX Manager	vCenter Server	443	TCP	vSphere API	×	○	
プライマリ NSX Manager	NSX ユニバーサルコントローラ クラスタ	443	TCP	NSX Controller REST API	×	○	ユーザー/パスワード

表 2-2. NSX で必要となるポートおよびプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
セカンダリ NSX Manager	NSX ユニバーサル コントローラ クラスタ	443	TCP	NSX Controller REST API	×	○	ユーザー/パスワード
ESXi ホスト	NSX ユニバーサル コントローラ クラスタ	1234	TCP	NSX 制御プレーン プロトコル	×	○	
ESXi ホスト	プライマリ NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
ESXi ホスト	セカンダリ NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード

Cross-vCenter NSX と拡張リンク モードのポート

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

NSX と vSphere Distributed Switch

NSX ドメインにおける NSX vSwitch は、サーバ 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 の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。

1 台のホストを複数の 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

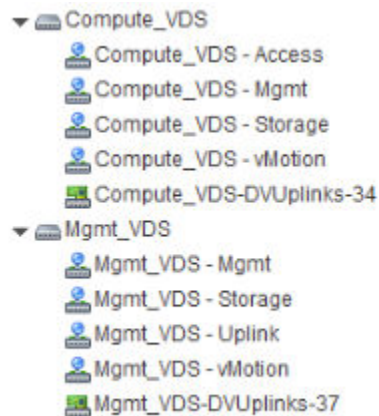
次の画面は、これらのクラスタが vCenter Server でどのように見えるかを示しています。



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。

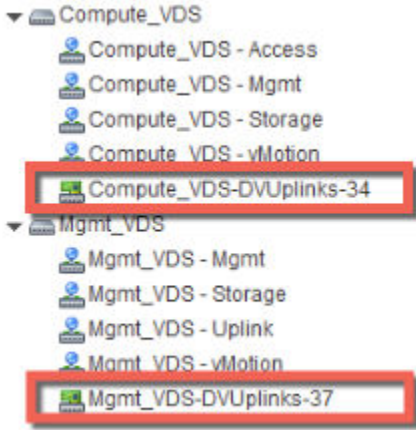
たとえば次の画面は、これらの Distributed Switch とポートが vCenter Server でどのように見えるかを示しています。



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します。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。

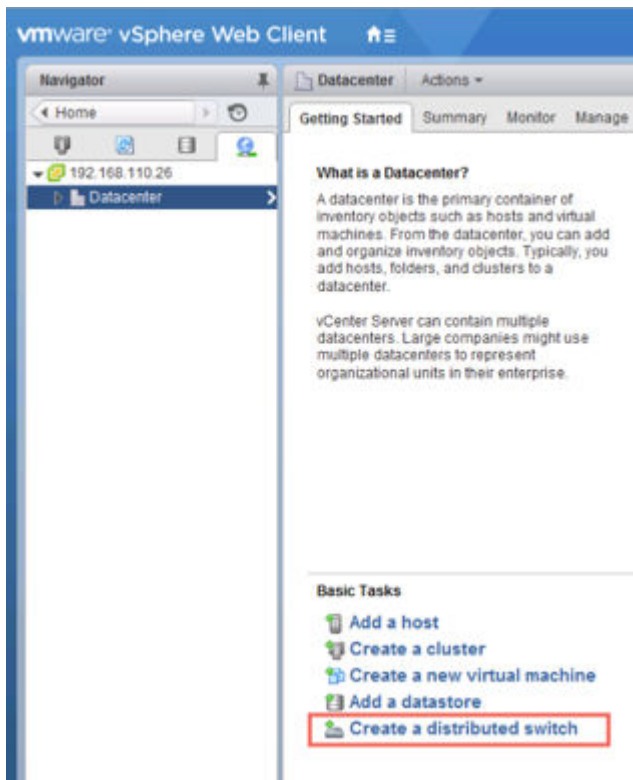
前提条件

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。



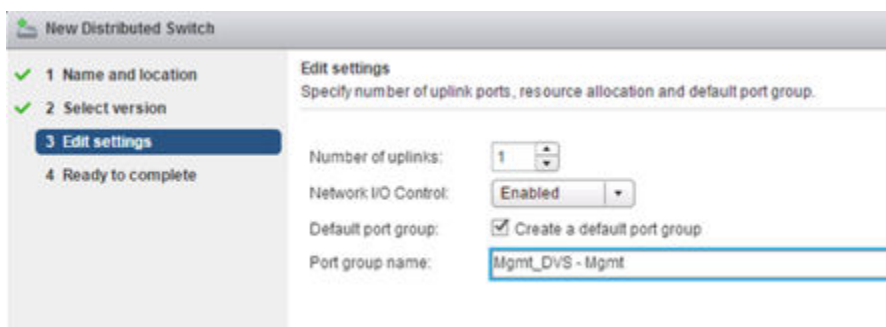
- 3 このスイッチに関連付けるホスト クラスタに基づいて、スイッチにわかりやすい名前を付けます。

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。

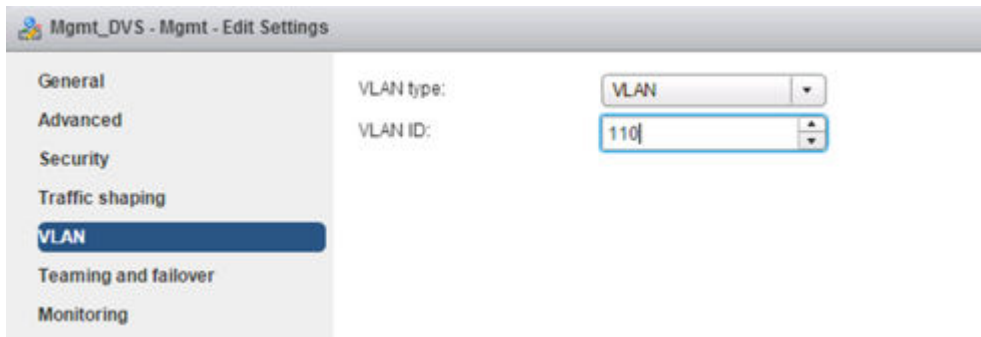
以下の画面は、管理ホスト クラスタでの管理トラフィックの設定例を示しています。



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。

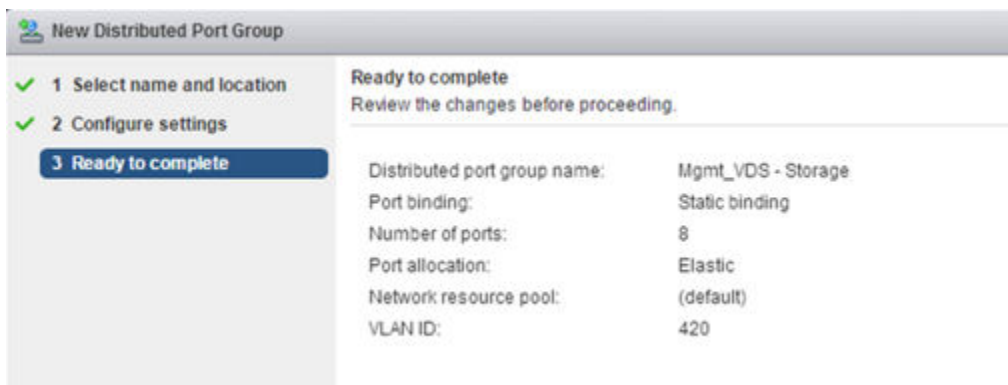
たとえば、ホストの管理インターフェイスが VLAN 110 内にある場合、デフォルト ポート グループを VLAN 110 に配置します。ホストの管理インターフェイスが VLAN 内にはない場合は、この手順をスキップします。



- 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。

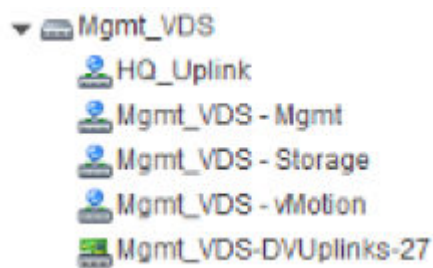
New Distributed Port Group

✓ 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

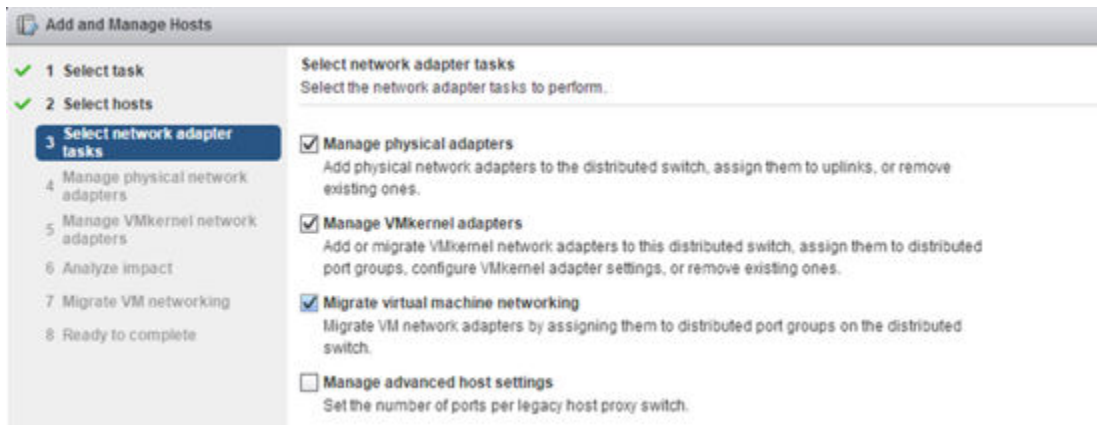
✓ 1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Select hosts
Select hosts to add to this distributed switch.

+ New hosts... | ✕ Remove

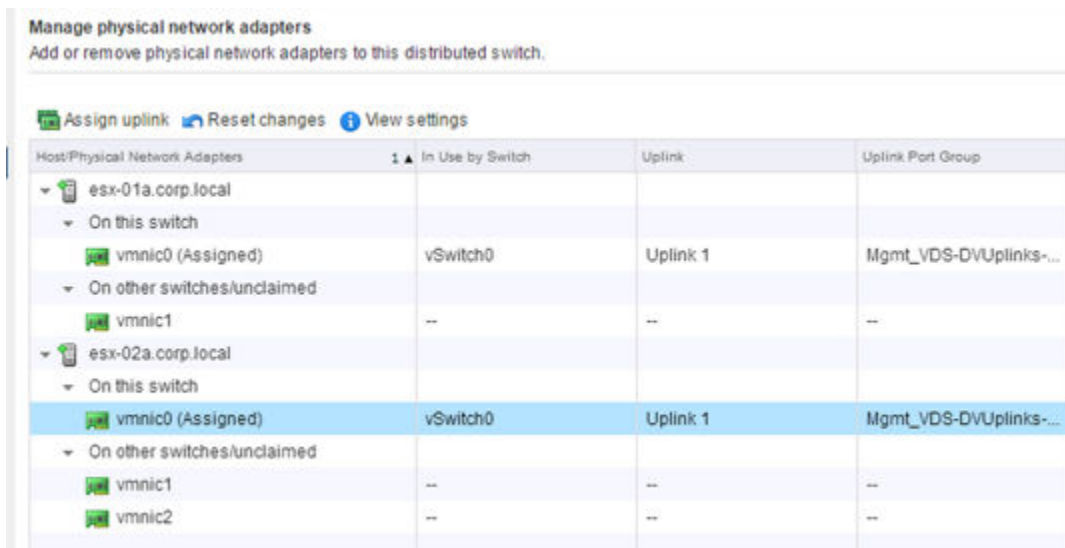
Host	Host Status
(New) esx-01a.corp.local	Connected
(New) esx-02a.corp.local	Connected

- 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。

Manage VMkernel network adapters
Manage and assign VMkernel network adapters to the distributed switch.

⚠ VMkernel network adapters with the warning sign might lose network connectivity unless they are migrated to the distributed switch. Select a destination port group to migrate them.

Assign port group New adapter Edit adapter Remove Reset changes View settings

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Group
esx-01a.corp.local			
On this switch			
vmk0 (Reassigned)	vSwitch0	Management Network	Mgmt_DVS - Mgmt
vmk1 (Reassigned)	vSwitch0	Storage	Mgmt_VDS - Storage
vmk2 (Reassigned)	vSwitch0	vMotion	Mgmt_VDS - vMotion
On other switches			
esx-02a.corp.local			
On this switch			
vmk0 (Reassigned)	vSwitch0	Management Network	Mgmt_DVS - Mgmt
vmk1 (Reassigned)	vSwitch0	Storage	Mgmt_VDS - Storage
vmk2 (Reassigned)	vSwitch0	vMotion	Mgmt_VDS - vMotion
On other switches			

- 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。

Migrate VM networking
Select virtual machines or network adapters to migrate to the distributed switch.

Assign VMs or network adapters to a destination port group to migrate them. Press and hold down the CTRL key, and then click the VMs to select multiple items.

Assign port group Reset changes View settings

Host/Virtual Machine/Network Adapter	NIC Count	Source Port Group	Destination Port Group
esx-01a.corp.local			
controlcenter	1		
Network adapter 1		VLAN110	Mgmt_DVS - Mgmt
vc-l-01a	1		
Network adapter 1		VLAN110	Mgmt_DVS - Mgmt

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

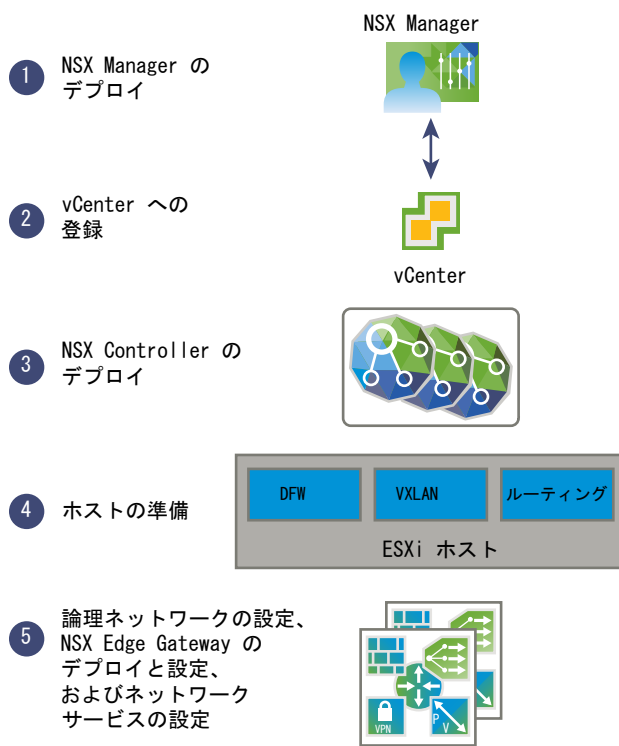
```

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

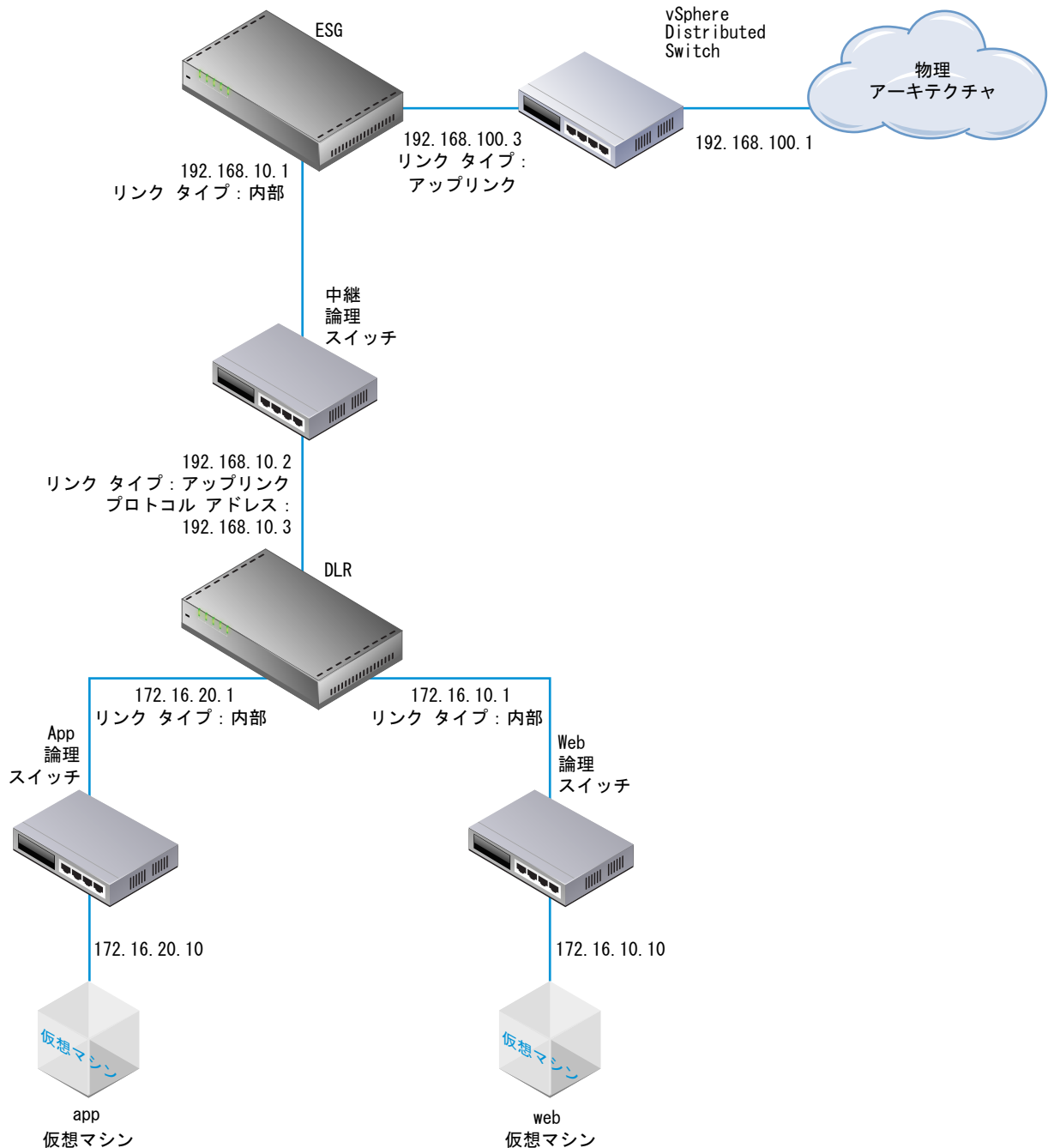
NSX のインストールでは、仮想アプライアンスのデプロイ、ESX ホストの準備、および物理デバイスと仮想デバイスすべてで通信を可能にする設定を行います。



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が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。

NSX Manager 仮想アプライアンスのインストール

3

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 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 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、HA 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 のカスタム 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 のカスタム 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 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。

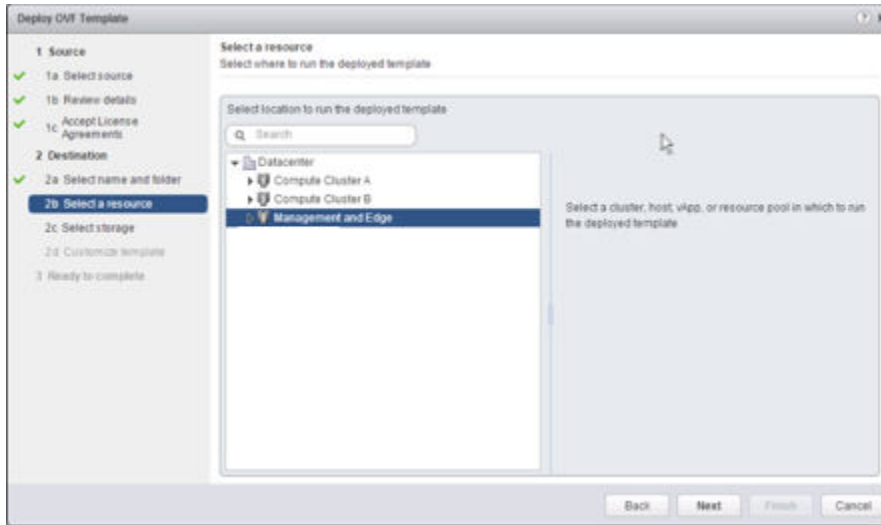
クライアント統合プラグインがすでにシステムにインストールされている場合は、同プラグインをダウンロードするためのリンクは表示されません。クライアント統合プラグインをアンインストールすると、同プラグインのダウンロード リンクが、vSphere Web Client のログイン ページに表示されます。

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。
- 5 [\[追加の構成オプションの承諾 \(Accept extra configuration options\)\]](#) 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 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。

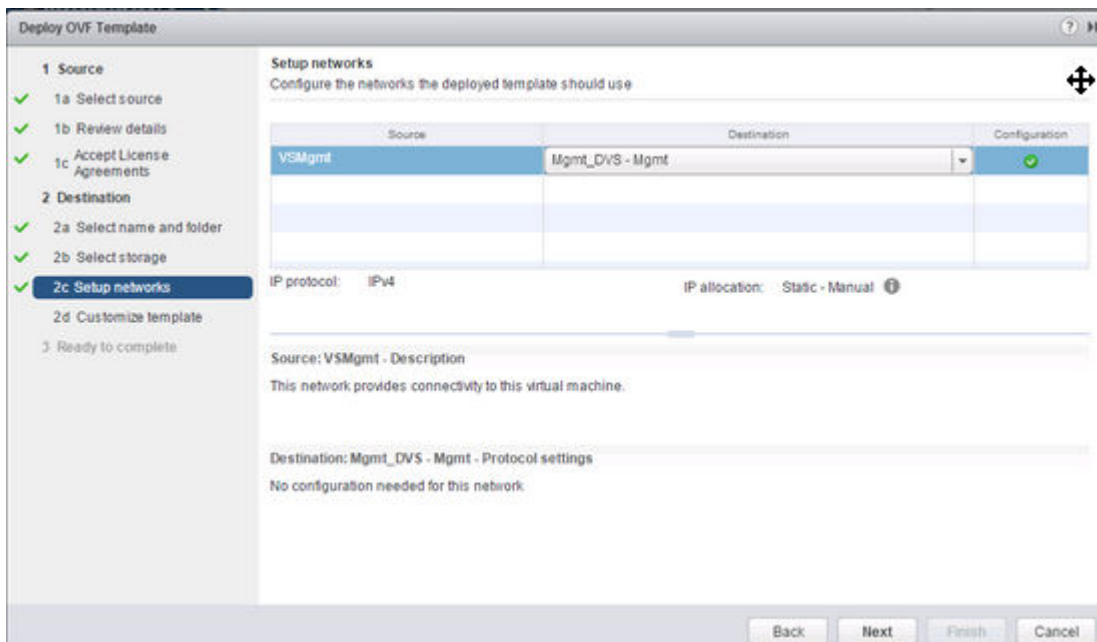
次はその例です。



- 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。

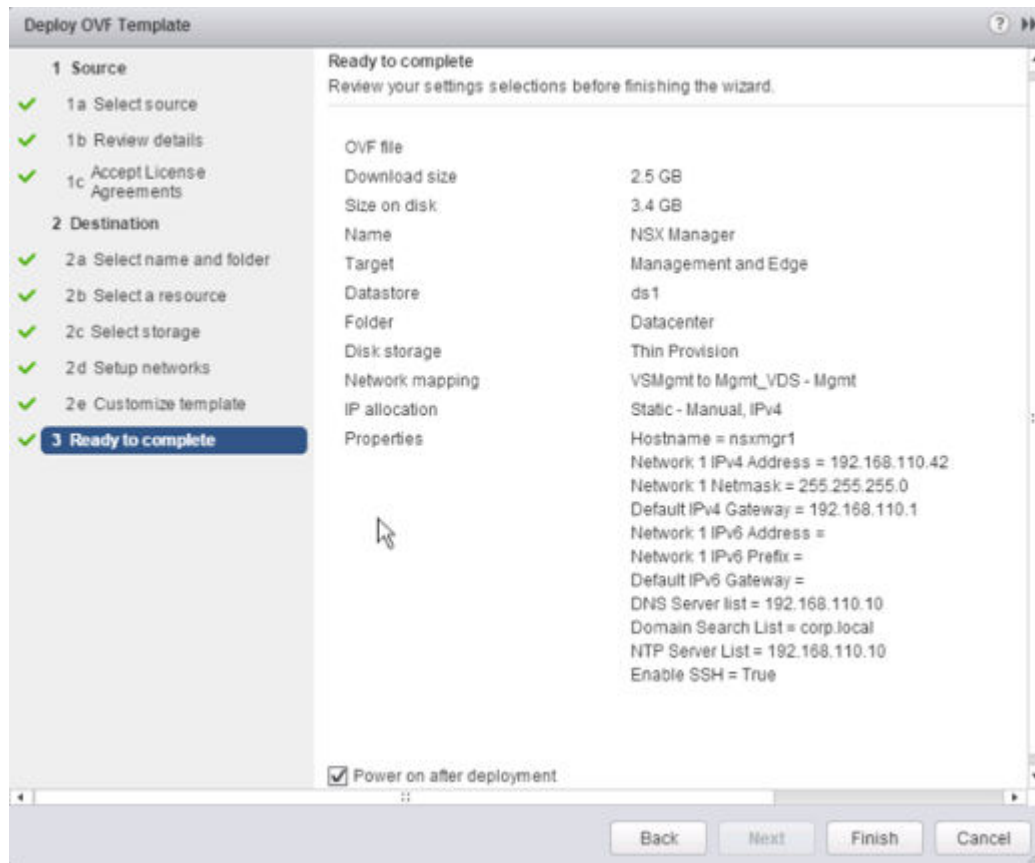
たとえば、このスクリーン ショットでは「Mgmt_DVS - Mgmt」ポートグループを選択しています。



- 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。



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。

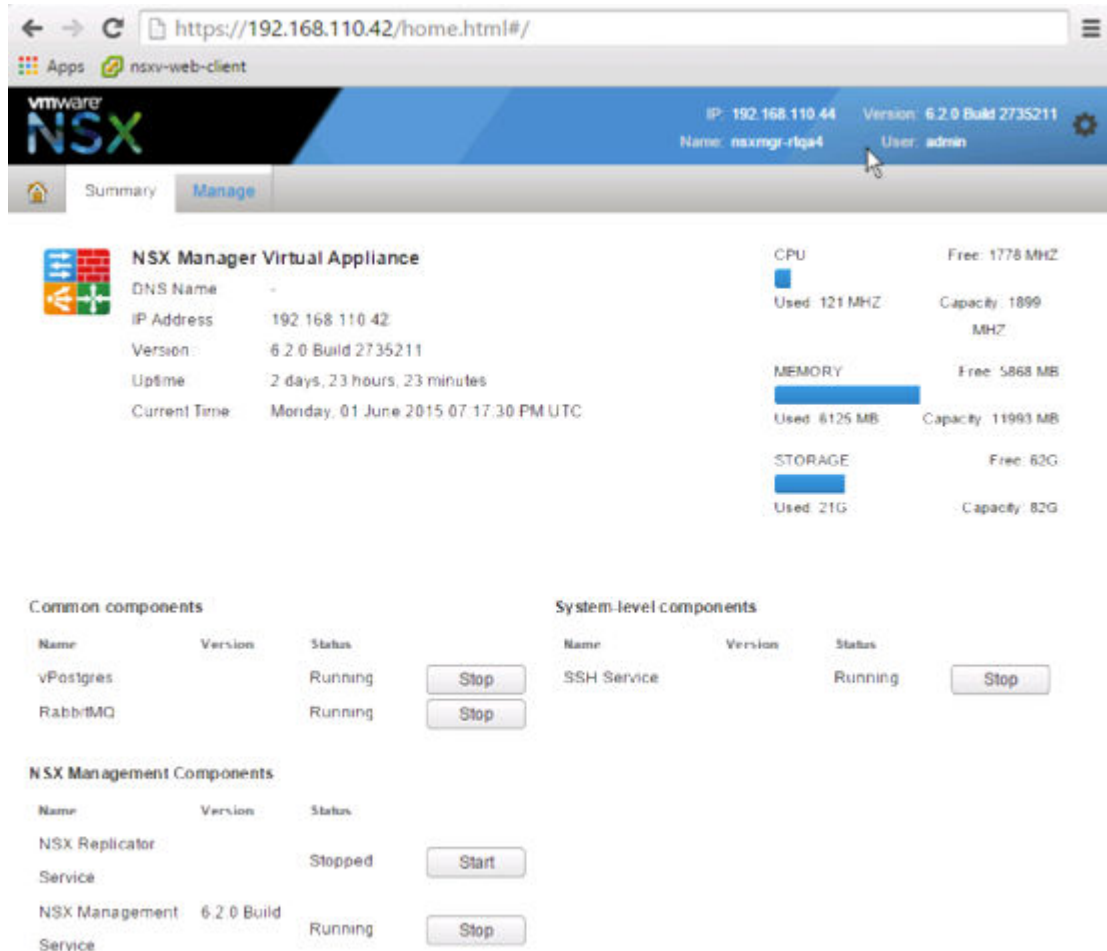
NSX Manager が完全に起動した後、CLI にログインし、**show interface** コマンドを実行して、IP アドレスが想定どおりに適用されていることを確認します。

```
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、[サマリの表示 (View Summary)] をクリックし、vPostgres、RabbitMQ、および NSX 管理サービスの各サービスが実行されていることを確認します。



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。

NSX Manager への vCenter Server の登録

4

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、NSX の Cross-vCenter 機能を使用している場合にもあてはまります。NSX Manager をインストールして、NSX 管理サービスが実行されていることを確認したら、次に vCenter Server を NSX Manager に登録します。

vCenter Server を登録できるのは、1 つの NSX Manager だけです。vCenter Server の登録を変更すると、影響を受けるすべての vCenter Server と NSX Manager に変更内容が正しく伝わらないという問題が発生することがあります。

たとえば、次のような初期構成の NSX Manager と vCenter Server があるとします。

- NSX1 ----> VC1
- NSX2 ----> VC2

NSX1 の構成を変更して vCenter Server を VC2 にした場合は、次のようになります。

- NSX1 は、vCenter Server が VC2 であると正しく報告します。
- VC2 は、NSX Manager が NSX1 であると正しく報告します。
- VC1 は、NSX Manager が NSX1 であると間違って報告します。
- NSX2 は、vCenter Server が VC2 であると間違って報告します。

つまり、vCenter Server がすでに 1 つの NSX Manager に登録され、次に別の NSX Manager が同じ vCenter Server を登録すると、vCenter Server は最初の NSX Manager との接続を自動的に解除して、新しい NSX Manager に接続します。しかし、最初の NSX Manager にログインしたときに、vCenter Server との接続は引き続き NSX Manager から報告されます。

この問題を回避するには、NSX Manager プラグインを VC2 に登録する前に VC1 から削除します。その手順については、[「NSX インストールの安全な削除」](#)を参照してください。

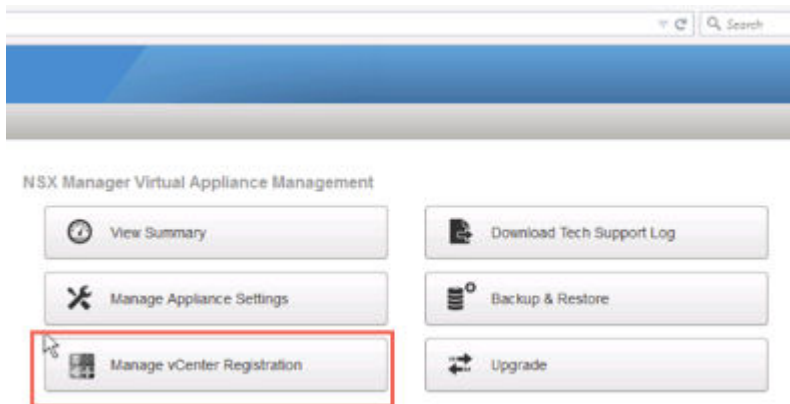
前提条件

- NSX 管理サービスが実行されている必要があります。Web ブラウザを使用して NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>>) を開き、[サマリ (Summary)] タブでこれを確認できます。
- NSX Manager と vCenter Server を同期するには、管理者ロールを持つ vCenter Server ユーザー アカウントが必要です。vCenter Server のパスワードに非 ASCII 文字が含まれている場合は、NSX Manager と vCenter Server 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。

手順

- 1 Web ブラウザで、NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>> または <https://<nsx-manager-hostname>>) 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 [アプライアンス管理] で、[vCenter 登録の管理 (Manage vCenter Registration)] をクリックします。

次はその例です。



- 3 vCenter Server の IP アドレスまたはホスト名を参照するように vCenter Server 要素を編集し、vCenter Server のユーザー名とパスワードを入力します。

ユーザー名のベスト プラクティスは、administrator@vsphere.local か、作成しておいた代替アカウントを入力することです。ルート アカウントは使用しないでください。

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

CA サーバに CA 署名付き証明書をインストールした場合は、CA 署名付き証明書のサムプリントが表示されます。CA 署名付き証明書をインストールしていない場合は、自己署名証明書が表示されます。

- 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。NSX Manager をこのタイプのファイアウォールの背後に置くことは推奨されていないので注意してください。

6 vCenter Server 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。



7 vSphere Web Client を開いている場合は、vCenter Server からログアウトし、NSX Manager を vCenter Server に登録するために使用した管理者ロールを使用してログインし直します。

これを行わない場合、vSphere Web Client の [ホーム (Home)] タブに [Networking and Security (Networking & Security)] アイコンが表示されません。

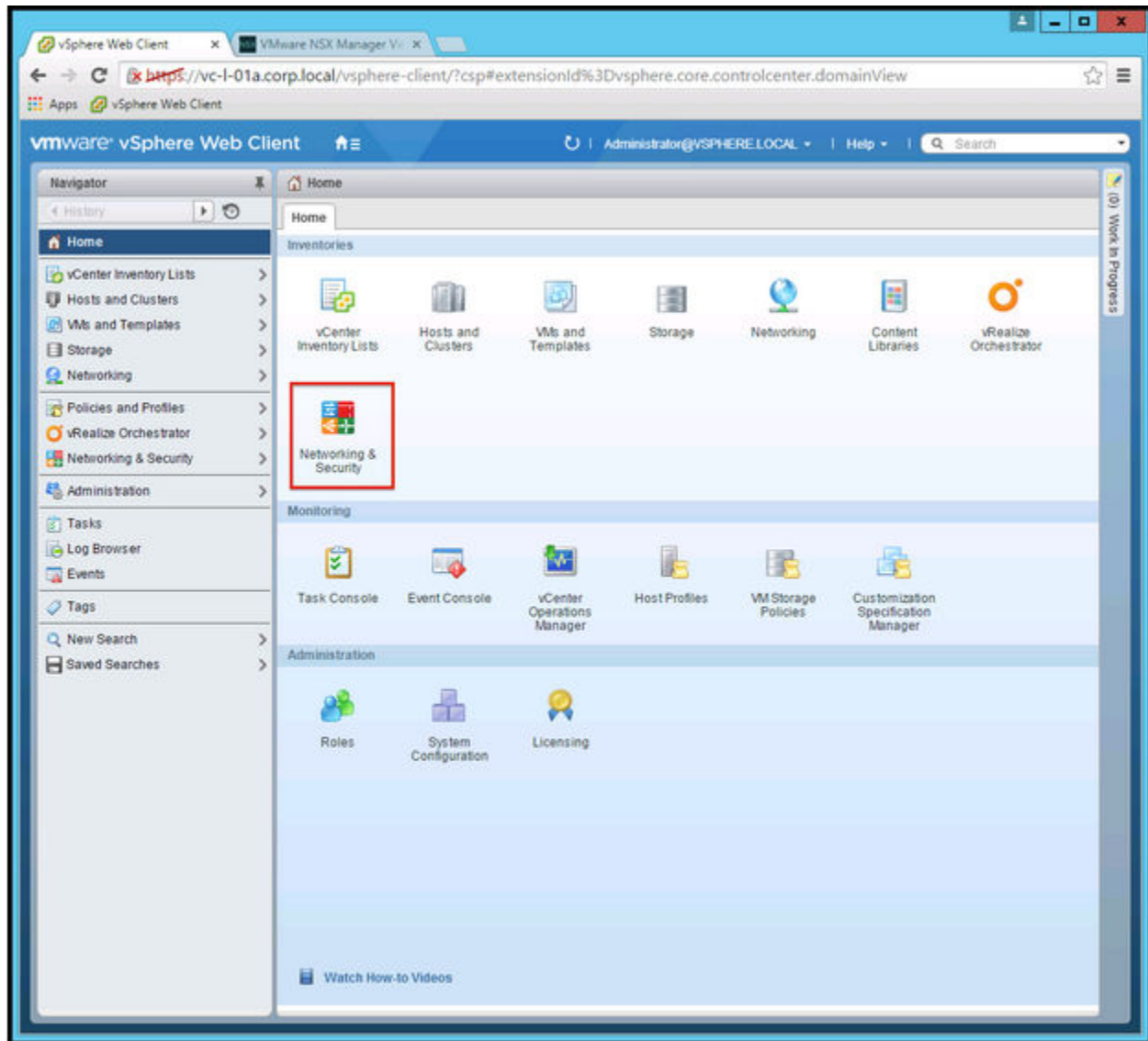
[Networking and Security (Networking & Security)] アイコンをクリックして、新しくデプロイした NSX Manager が表示されることを確認します。

次のステップ

NSX Manager をインストールした直後に NSX Manager データをバックアップするようにスケジュール設定することをお勧めします。

NSX 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。

vSphere Web Client にログインし、[Networking and Security (Networking & Security)] アイコンが [ホーム (Home)] タブに表示されていることを確認します。すでにログインしている場合、このアイコンは表示されません。この新しいアイコンを表示するには、vSphere Web Client に再度ログインします。



これで、NSX コンポーネントをインストールして構成することができます。

Single Sign-On の設定

SSO を使用することで、さまざまなコンポーネントがセキュアなトークン交換メカニズムを介した相互通信を行えるため、各コンポーネントが個別にユーザーを認証する必要がなく、vSphere と NSX のセキュリティを高めることができます。NSX Manager で Lookup Service を設定し、SSO 管理者の認証情報を入力して、NSX 管理サービスを SSO ユーザーとして登録することができます。Single Sign On (SSO) サービスを NSX に統合すると、vCenter ユーザーに対するユーザー認証のセキュリティが強化され、NSX が AD、NIS、LDAP など他の ID サービスからユーザーを認証できるようになります。

SSO により NSX は、REST API 呼び出しを介して、信頼されるソースからの認証済み Security Assertion Markup Language (SAML) トークンを使用する認証をサポートします。また NSX Manager では、他の VMware ソリューションで使用する認証 SAML トークンを取得できます。

NSX は、SSO ユーザーのグループ情報をキャッシュします。グループメンバーシップを変更すると、ID プロバイダ (Active Directory など) から NSX への伝達に最大 60 分かかります。

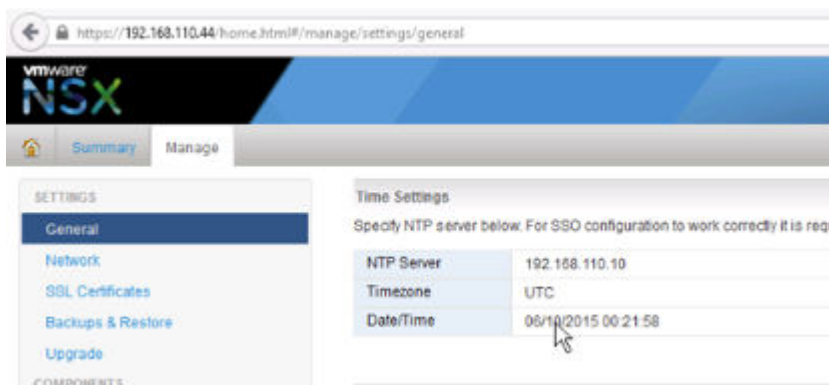
前提条件

- NSX Manager で SSO を使用するには、vCenter Server 5.5 以降が必要であり、vCenter Server に Single Sign-On (SSO) 認証サービスがインストールされている必要があります。これは組み込みの SSO が対象であることに注意してください。代わりに、デプロイで、外部の一元化された SSO サーバが使用される場合があります。

vSphere が提供する SSO サービスの詳細については、<http://kb.vmware.com/kb/2072435> および <http://kb.vmware.com/kb/2113115> を参照してください。

- SSO サーバの時間と NSX Manager の時間が同期するよう、NTP サーバを指定する必要があります。

次はその例です。



手順

- 1 NSX Manager 仮想アプライアンスにログインします。

Web ブラウザで、NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>> または <https://<nsx-manager-hostname>>) に移動し、NSX Manager のインストール時に設定したパスワードを使用して admin としてログインします。

- 2 [管理 (Manage)] タブをクリックして、[NSX 管理サービス (NSX Management Service)] をクリックします。
- 3 Lookup Service が実行されるホストの名前または IP アドレスを入力します。

vCenter Server を使用して Lookup Service を実行する場合は、vCenter Server の IP アドレスまたはホスト名を入力し、vCenter Server のユーザー名とパスワードを入力します。

- 4 ポート番号を入力します。

vSphere 6.0 を使用している場合はポート 443 を入力し、vSphere 5.5 を使用している場合はポート 7444 を使用します。

Lookup Service の URL は、指定されたホストおよびポートに基づいて表示されます。

次はその例です。

Lookup Service

For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service IP: 192.168.110.25

Lookup Service Port: 443

Lookup Service: https://192.168.110.25:443/lookupservice/sdk

SSO Administrator User Name: administrator@vsphere.local

Password: *****

OK Cancel

- 5 証明書のサム プリントが vCenter Server の証明書と一致することを確認します。

CA サーバに CA 署名付き証明書をインストールした場合は、CA 署名付き証明書のサムプリントが表示されます。CA 署名付き証明書をインストールしていない場合は、自己署名証明書が表示されます。

- 6 Lookup Service のステータスが [接続中 (Connected)] になっていることを確認します。

次はその例です。

Lookup Service

For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service:	https://192.168.110.25:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	● Connected ↻

次のステップ

SSO ユーザーにロールを割り当てます。

Syslog サーバの指定

Syslog サーバを指定すると、NSX Manager は、その Syslog サーバにすべての監査ログとシステム イベントを送信します。

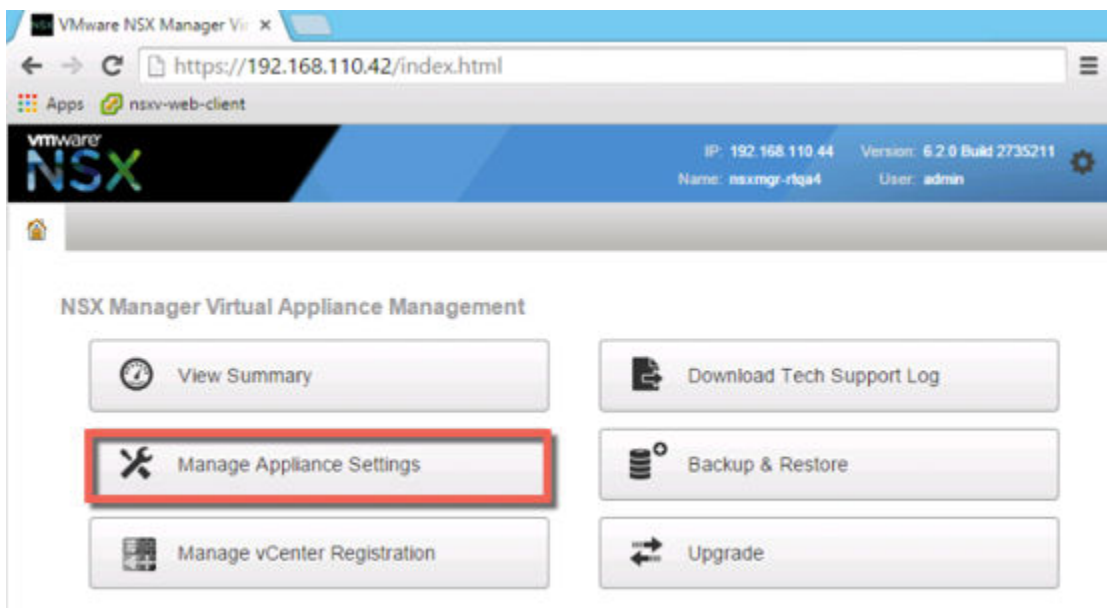
Syslog データは、トラブルシューティングや、インストールおよび構成中、ログに記録されたデータを確認する際に役立ちます。

NSX Edge は 2 台の Syslog サーバをサポートします。NSX Manager と NSX コントローラは 1 台の Syslog サーバをサポートします。

手順

- 1 Web ブラウザで、NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>> または <https://<nsx-manager-hostname>>) の順に移動します。
- 2 NSX Manager のインストール時に設定したパスワードを使用して admin としてログインします。
- 3 [アプライアンス設定の管理 (Manage Appliance Settings)] をクリックします。

次はその例です。

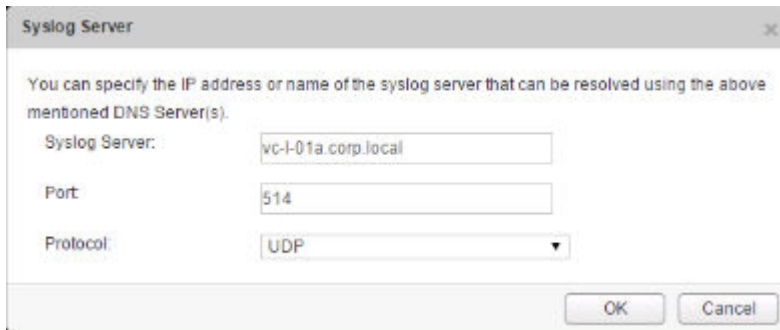


- 4 [設定] パネルから [全般 (General)] をクリックします。
- 5 [Syslog サーバ (Edit)] の横にある [編集 (Syslog Server)] をクリックします。

6 Syslog サーバの IP アドレス/ホスト名、ポート、およびプロトコルを入力します。

ポートを指定しないと、Syslog サーバの IP アドレス/ホスト名用のデフォルトの UDP ポートが使用されます。

次はその例です。



The screenshot shows a dialog box titled "Syslog Server". Inside the dialog, there is a text label that reads: "You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).". Below this text, there are three input fields: "Syslog Server:" with the value "vc-l-01a.corp.local", "Port" with the value "514", and "Protocol" with a dropdown menu showing "UDP". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

7 [OK] をクリックします。

vCenter Server のリモート ログが有効になり、ログがスタンドアロンの Syslog サーバに格納されます。

NSX for vSphere のライセンスのインストールと割り当て

7

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、論理ルーター、Distributed Firewall、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 ライセンスに関する FAQ (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>) 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。

NSX コントローラ クラスタの展開

NSX コントローラは、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。

NSX デプロイのサイズに関係なく、VMware では、各 NSX コントローラ 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、システムが停止する原因となる場合があります。

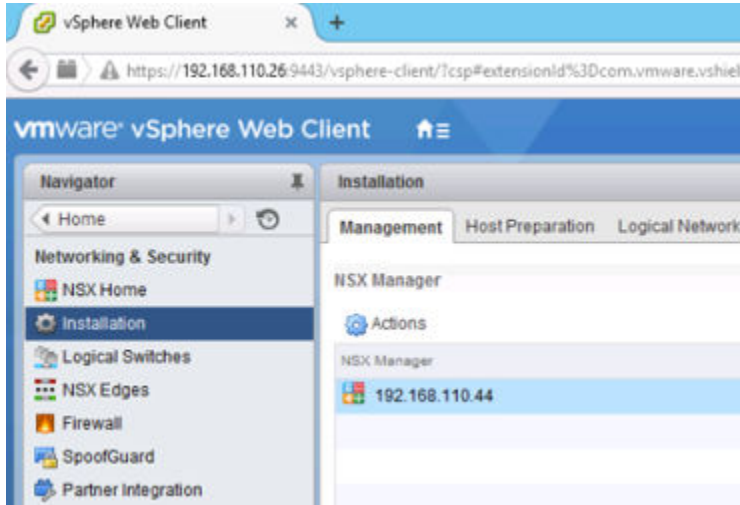
前提条件

- NSX コントローラを展開する前に、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 コントローラの 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 で [ホーム] > [Networking and Security] > [インストール] の順に移動し、[管理] タブを選択します。

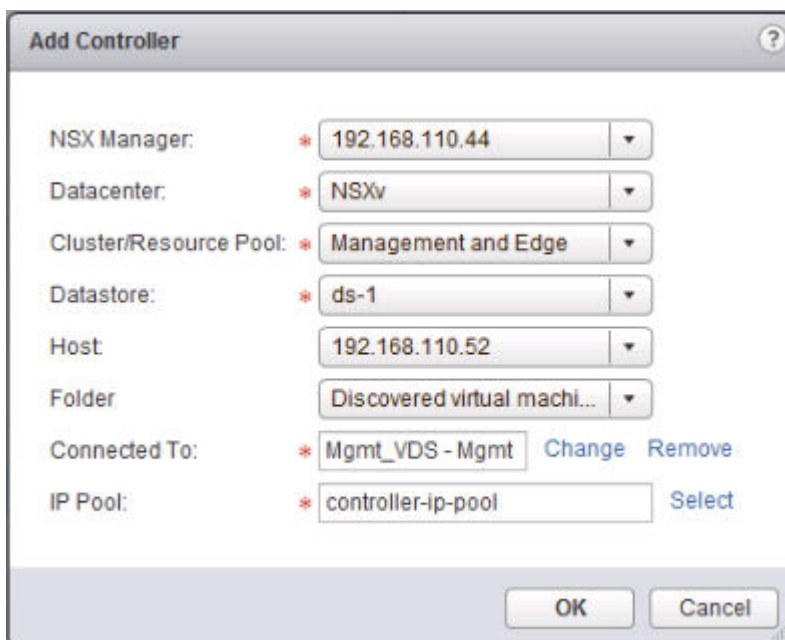
次はその例です。



- 2 [NSX コントローラ ノード] セクションで、[ノードの追加] (+) アイコンをクリックします。
- 3 環境に適した NSX コントローラ設定を入力します。

NSX コントローラは、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。

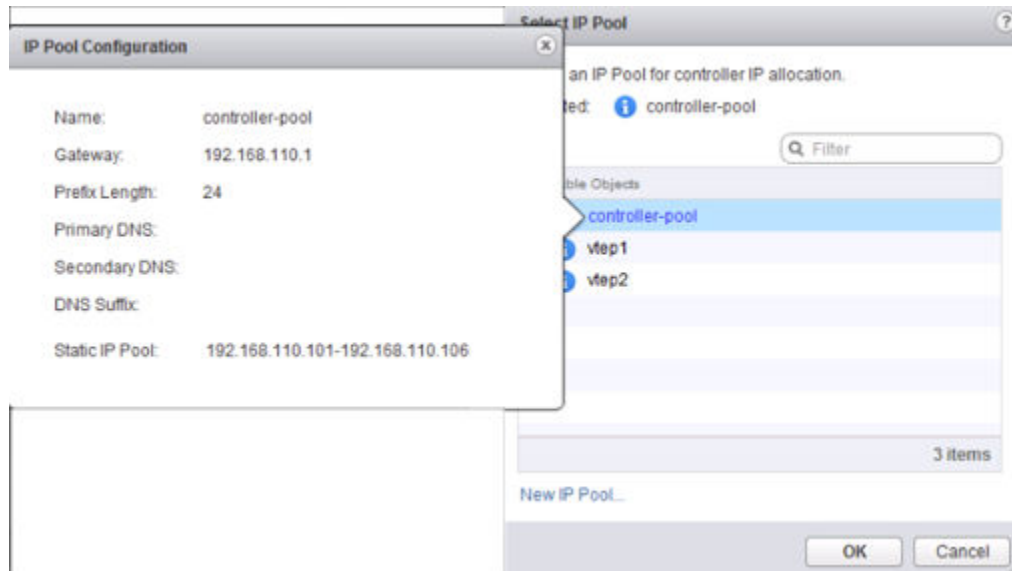
次はその例です。



- 4 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 プール] 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。



- 5 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

- 6 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。

ファイアウォールによる保護からの仮想マシンの除外


9

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

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

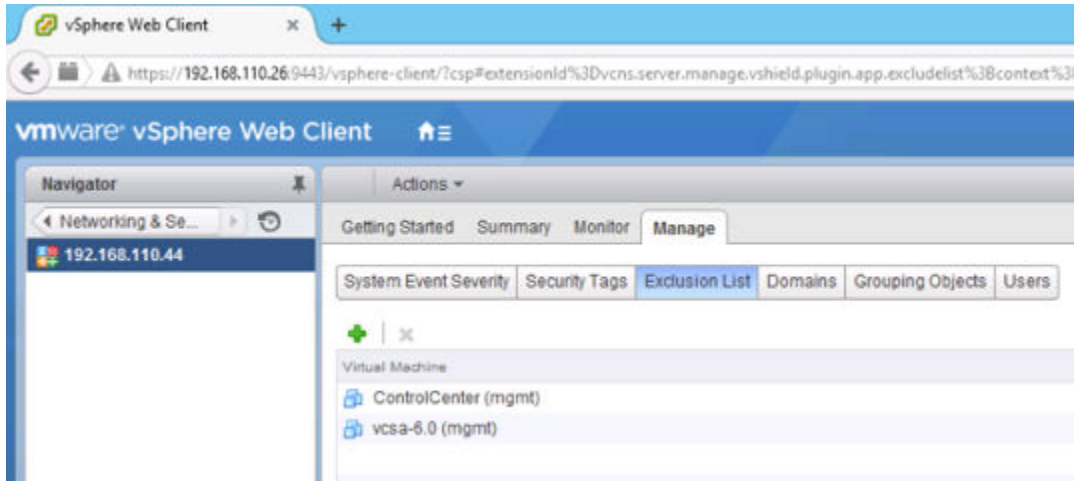
- vCenter Server。vCenter Server は Firewall によって保護されているクラスタに移動できますが、これを前もって除外リストに追加しておき、接続の問題を防止する必要があります。
- パートナーのサービス仮想マシン。
- 無差別モードを必要とする仮想マシン。この仮想マシンを NSX Distributed Firewall で保護した場合、仮想マシンのパフォーマンスに悪影響が及ぶ可能性があります。
- Windows ベースの vCenter Server で使用する SQL Server。
- vCenter Web サーバ（個別に実行している場合）。

手順

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

6 除外する仮想マシンの名前を入力し、[追加 (Add)] をクリックします。

次はその例です。



7 [OK] をクリックします。

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

NSX 用ホスト クラスタの準備

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 コントローラをデプロイします。
- 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-1-01a.corp.local
Address:    192.168.110.42
```

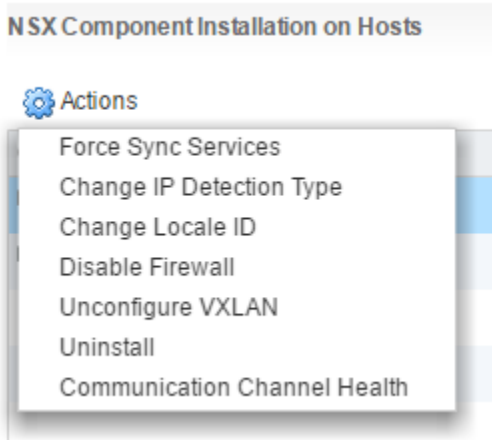
- ホストが vCenter Server の DNS 名を解決できることを確認します。
- ホストが vCenter Server のポート 80 に接続できることを確認します。
- vCenter Server と ESXi ホスト間でネットワーク時刻が同期されることを確認します。

- NSX に参加する各ホスト クラスタで、クラスタ内のホストが共通の分散仮想スイッチ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。

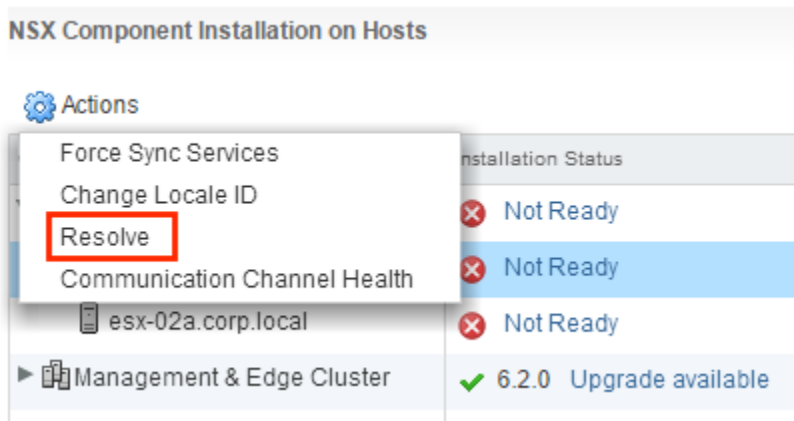
- お使いの環境に vSphere Update Manager (VUM) がある場合は、クラスタでネットワーク仮想化の準備をする前に、VUM を無効にしておく必要があります。VUM が有効かどうかを確認する方法と、必要に応じて VUM を無効にする方法については、<http://kb.vmware.com/kb/2053782> を参照してください。
- NSX ホストの準備プロセスを開始する前に、クラスタのステータスが解決済みであること、つまり [解決 (Resolve)] オプションがクラスタの [アクション (Actions)] リストに表示されていないことを必ず確認してください。

次はその例です。

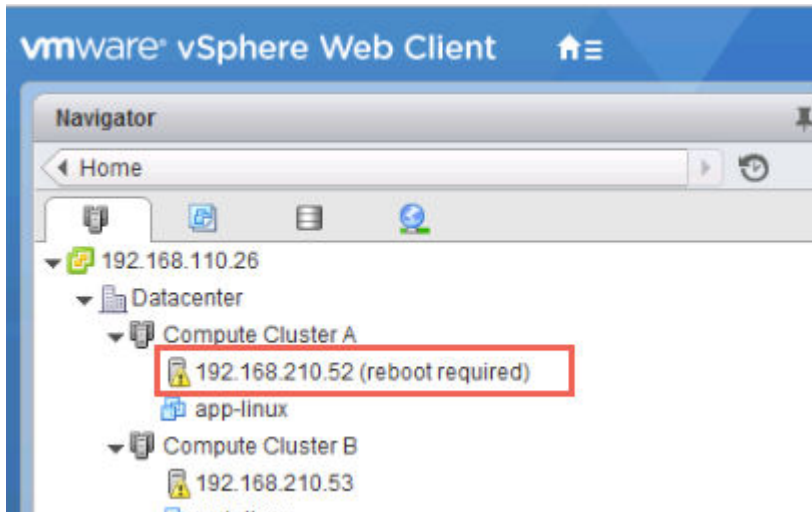


クラスタ内のホストを再起動する必要がある場合に、[解決 (Resolve)] オプションが表示されることがあります。

また、解決しなければならないエラーが発生したために、[解決法 (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。



ホストから VIB を削除するプロセスでは、ホストを再起動する必要があります。VIB を削除するプロセスは、NSX のアップグレード、vCenter Server からの NSX Manager プラグインの削除、NSX の準備ができていないクラスタからのホストの削除、ホストからの NSX VIB の手動削除で設定されます。ホストを再起動する必要がある場合は、ホストおよびクラスタービューに [再起動要求 (reboot required)] タグが表示されます。次はその例です。

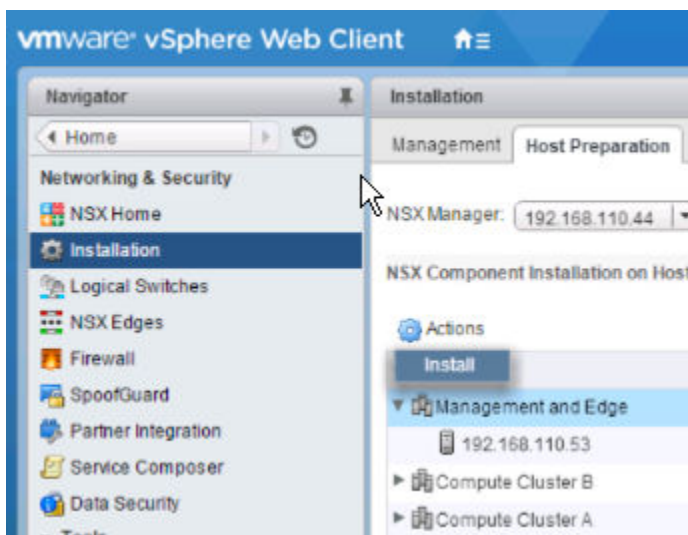


必要な再起動は、自動的に行われません。ホストを再起動する前に、ホストの仮想マシンをパワーオフまたは移動します（または DRS に仮想マシンの移動を許可します）。次に [ホストの準備] タブの [アクション (Actions)] リストで、[解決 (Resolve)] オプションをクリックします。[解決 (Resolve)] アクションでは、ホストをメンテナンス モードにし、ホストを再起動した後、メンテナンス モードを解除します。ホストの仮想マシンをパワーオフした場合は、手動でパワーオンする必要があります。

手順

- 1 vSphere Web Client で [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] に移動し、[ホストの準備 (Host Preparation)] タブを選択します。

次はその例です。



- 2 NSX の論理スイッチング、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、歯車アイコンをクリックし、[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（ペイロード 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。

- 3 [インストールの状態 (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。

[インストールの状態 (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、[6.2 アンインストール (6.2 Uninstall)] と表示され、[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。

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。

- esx-vsip
- esx-vxlan

確認のために、各ホストに SSH 接続し、**esxcli software vib list | grep esx** コマンドを実行します。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-vsip      6.0.0-0.0.2732470  VMware  VMwareCertified  2015-05-29
esx-vxlan     6.0.0-0.0.2732470  VMware  VMwareCertified  2015-05-29
...
```

ホストの準備後は、ホストを再起動する必要はありません。

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。

未準備の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。この場合、アンインストール プロセスを完了するには、ホストを再起動する必要があります。

準備済みクラスタへのホストの追加

このセクションでは、ネットワーク仮想化の準備が整っているクラスタにホストを追加する方法について説明します。

手順

- 1 ホストを vCenter Server にスタンドアロン ホストとして追加します。

ESXi および vCenter Server 5.5 のドキュメントを参照してください。

- 2 ホストを追加するクラスタにマップされた vSphere Distributed Switch にホストを追加します。

クラスタ内のすべてのホストは、NSX で利用される vSphere Distributed Switch に含まれている必要があります。

- 3 ホストをメンテナンス モードにします。

- 4 クラスタにホストを追加します。

これは準備済みクラスタであるため、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。

- 5 ホストのメンテナンス モードを解除します。

DRS は、仮想マシンをホストにバランスよく配置します。

NSX を使用するクラスタからのホストの削除

12

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 に参加させないことを決めた場合などに、削除することができます。

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、ネットワーク仮想化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 変更を有効にするには、すべての仮想マシンを移動または停止し、ホストをメンテナンス モードにしてから、ホストを再起動します。

必要に応じて、再起動をメンテナンス用時間枠まで延期できます。

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 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-vsip
- 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判断できます。

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-vsip**

重要: これらのコマンドの実行後は、変更を有効にするために、ホストを再起動する必要があります。

VXLAN 転送パラメータの設定

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。Distributed Firewall 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。

前提条件

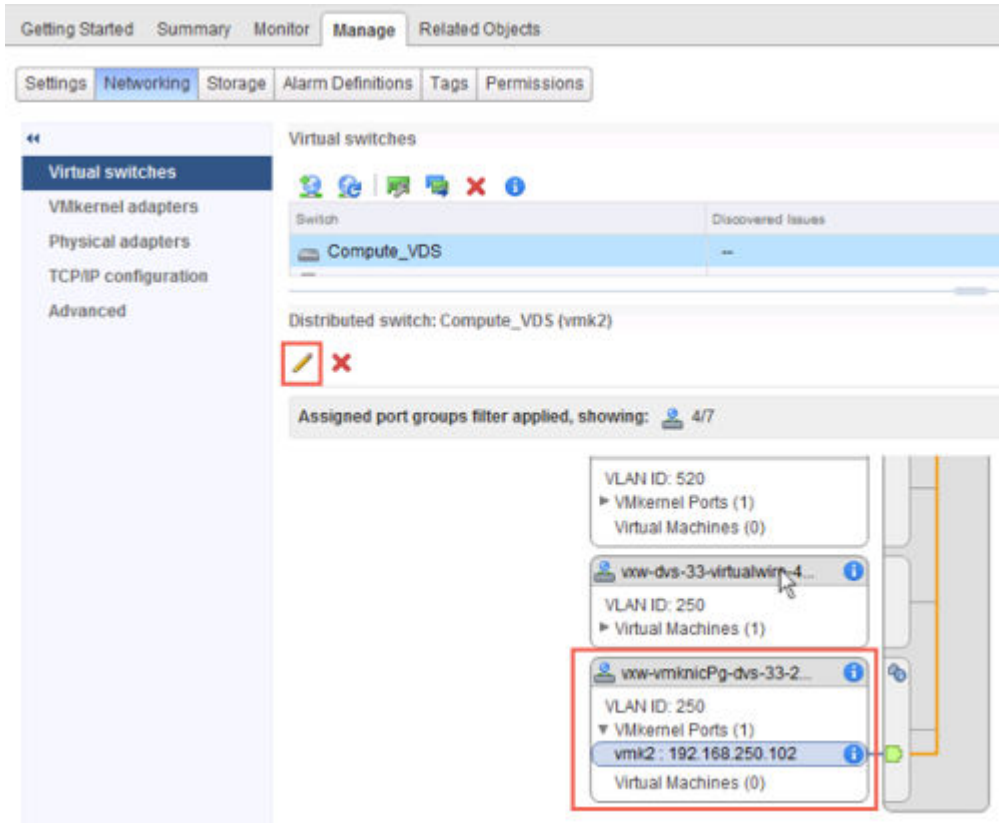
- クラスタ内のすべてのホストが、共通の VDS に接続されている必要があります。
- NSX Manager をインストールがインストールされている。
- 制御プレーンにマルチキャスト レプリケーション モードを使用していない場合は、NSX コントローラをインストールする必要があります。
- NIC チーミング ポリシーを計画します。NIC チーミング ポリシーによって、VDS のロード バランシングおよびフェイルオーバー設定が決まります。

特定の VDS 上の各ポートグループに異なるチーミング ポリシーを混在させないでください。すなわち、一部のポートグループには、イーサチャネル、LACPv1、または LACPv2 を使用し、その他のポートグループには異なるチーミング 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。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、VDS 上のすべてのアップリンクをチーム内で使用することです。その VDS 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でください。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 ヘッダで使われる、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 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) MAC アドレスを DHCP サーバ内の特定の IP アドレスにマップする、DHCP 固定アドレスまたは予約を使用するか、2) IP プールを使用して、[管理 (Manage)] > [ネットワーク (Networking)] > [仮想スイッチ (Virtual Switches)] で vmknic に割り当てた VTEP IP アドレスを手動で編集することができます。次はその例です。



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。

- 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。
- ベスト プラクティスとして、VXLAN のクラスタを準備する前に、VDS 設定をエクスポートします。
<http://kb.vmware.com/kb/2034602> を参照してください。

手順

- 1 vSphere Web Client で [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] に移動し、[ホストの準備 (Host Preparation)] タブを選択します。
- 2 [VXLAN] 列の [未構成 (Not Configured)] をクリックします。
- 3 論理ネットワークを設定します。

この設定では、VDS、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。

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 (VDS) の MTU サイズが VXLAN の MTU より大きい場合、VDS の MTU が下方に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、VDS 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 にすると、VDS の MTU は変更されません。VDS の MTU が 1500 で VXLAN の MTU が 1600 である場合は、VDS の MTU が 1600 に変更されます。

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 でのバッキング、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: * 192.168.150.1-192.168.150.100

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される可能性はまずありません。

VXLAN を設定すると、新しい分散ポート グループが作成されます。

次はその例です。

The screenshot displays the VMware vSphere Web Client interface. The left-hand 'Navigator' pane shows a tree structure of the vCenter environment. Two items are highlighted with red boxes: 'vww-vmknickPg-dvs-317-250-54942da9-a775-444d-9b08-3e31276da815' under the 'Compute_DVS' folder, and 'vww-vmknickPg-dvs-103-150-2...' under the 'Mgmt_VDS' folder. The main pane shows the 'Summary' tab for the selected port group. A red box highlights the port group's name and its MAC address. Below this, the 'Distributed Port Group Details' section shows the distributed switch as 'Compute_DVS', network protocol profile as '--', 4 hosts, and 0 virtual machines. The 'Tags' section is empty. At the bottom, the 'Recent Tasks' table lists several completed tasks.

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time
Update network configuration	comp-01b.corp.local	Completed	VSPHERE LOCALIL..	4 ms	5/1/2015 4:01:54 PM	5/1/2015 4:01:55 PM
Update network configuration	comp-02b.corp.local	Completed	VSPHERE LOCALIL..	4 ms	5/1/2015 4:01:53 PM	5/1/2015 4:01:54 PM
Add virtual NIC	comp-01b.corp.local	Completed	VSPHERE LOCALIL..	3 ms	5/1/2015 4:01:53 PM	5/1/2015 4:01:54 PM
Add virtual NIC	comp-02b.corp.local	Completed	VSPHERE LOCALIL..	5 ms	5/1/2015 4:01:53 PM	5/1/2015 4:01:53 PM
Update opaque data for set of entities		Completed	VSPHERE LOCALIL..	13 ms	5/1/2015 4:01:53 PM	5/1/2015 4:01:53 PM
Update opaque data for set of entities		Completed	VSPHERE LOCALIL..	4 ms	5/1/2015 4:01:53 PM	5/1/2015 4:01:53 PM

セグメント ID プールとマルチキャスト アドレス範囲の割り当て

14

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。代表的な VTEP の一例がハイパーバイザー ホストです。各 VXLAN トンネルにはセグメント ID があります。NSX Manager ごとにセグメント 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 コントローラ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があります。

1 つの vCenter Server で複数のセグメント ID 範囲 (たとえば 5000~5999、7000~7999) を設定したい場合、vSphere Web Client ユーザー インターフェースでは現時点でそのような設定がサポートされていませんが、NSX API を使用して設定することができます。

```
POST https://<nsxmgr-ip>/api/2.0/vdn/config/segments
```

```
<segmentRange>
<name>Segment ID Pool 1</name>
<begin>5000</begin>
<end>5999</end>
</segmentRange>
```

```
POST https://<nsxmgr-ip>/api/2.0/vdn/config/segments
```

```
<segmentRange>
<name>Segment ID Pool 2</name>
<begin>7000</begin>
<end>7999</end>
</segmentRange>
```

前提条件

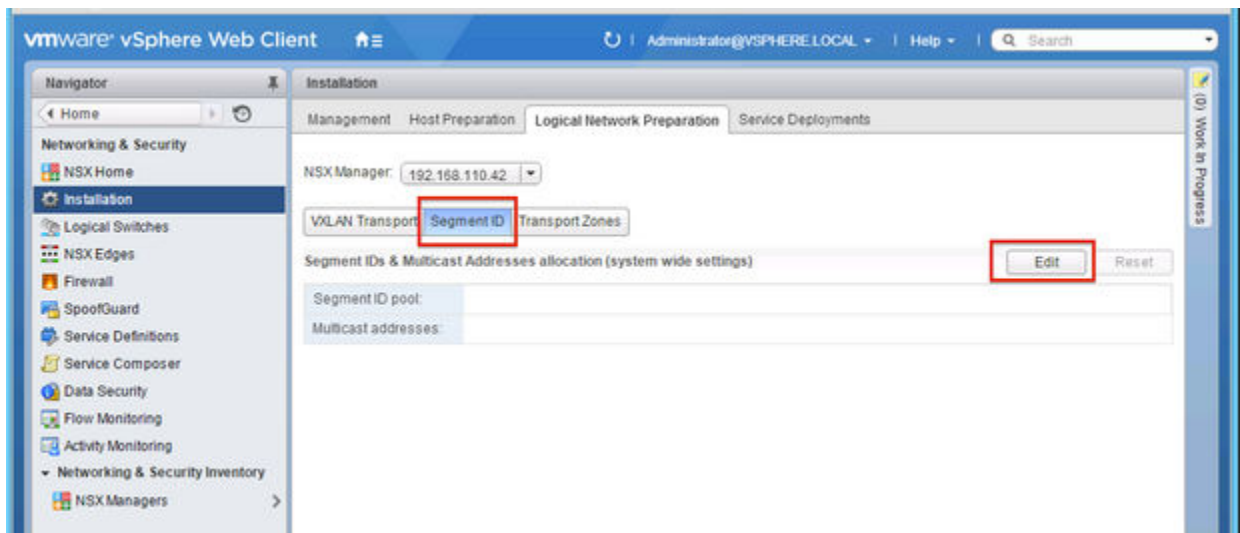
各セグメント ID プールのサイズを決める場合、セグメント ID 範囲で、作成できる論理スイッチの数が決まることに注意してください。16,000,000 個の VNI 候補から少量のサブセットを選択します。vCenter Server では、dvPortgroup の数が 10,000 個に制限されているため、1 つの vCenter Server で 10,000 個を超える VNI を設定しないでください。

VXLAN が別の NSX デプロイ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。重複しない VNI は追跡に便利です。また、デプロイで Cross-vCenter 環境の準備ができていることを確認するのに役立ちます。

手順

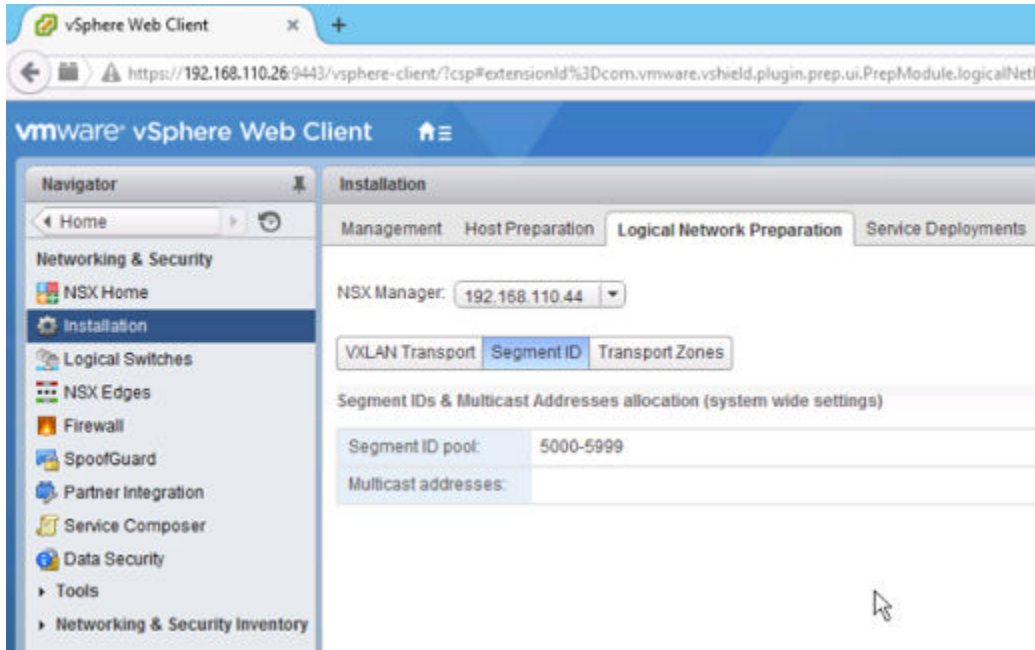
- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール手順 (Installation)] に移動し、[論理ネットワークの準備 (Logical Network Preparation)] タブを選択します。
- 2 [セグメント ID (Segment ID)] > [編集 (Edit)] をクリックします。

次はその例です。



3 セグメント ID の範囲（5000–5999 など）を入力します。

次はその例です。



4 トランスポート ゾーンのいずれかが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します。

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拡散し、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ことができ、適切な BUM レプリケーションが含まれるようになります。

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ディングされます。このようなフラ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。

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。

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。

トランスポート ゾーンの追加

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

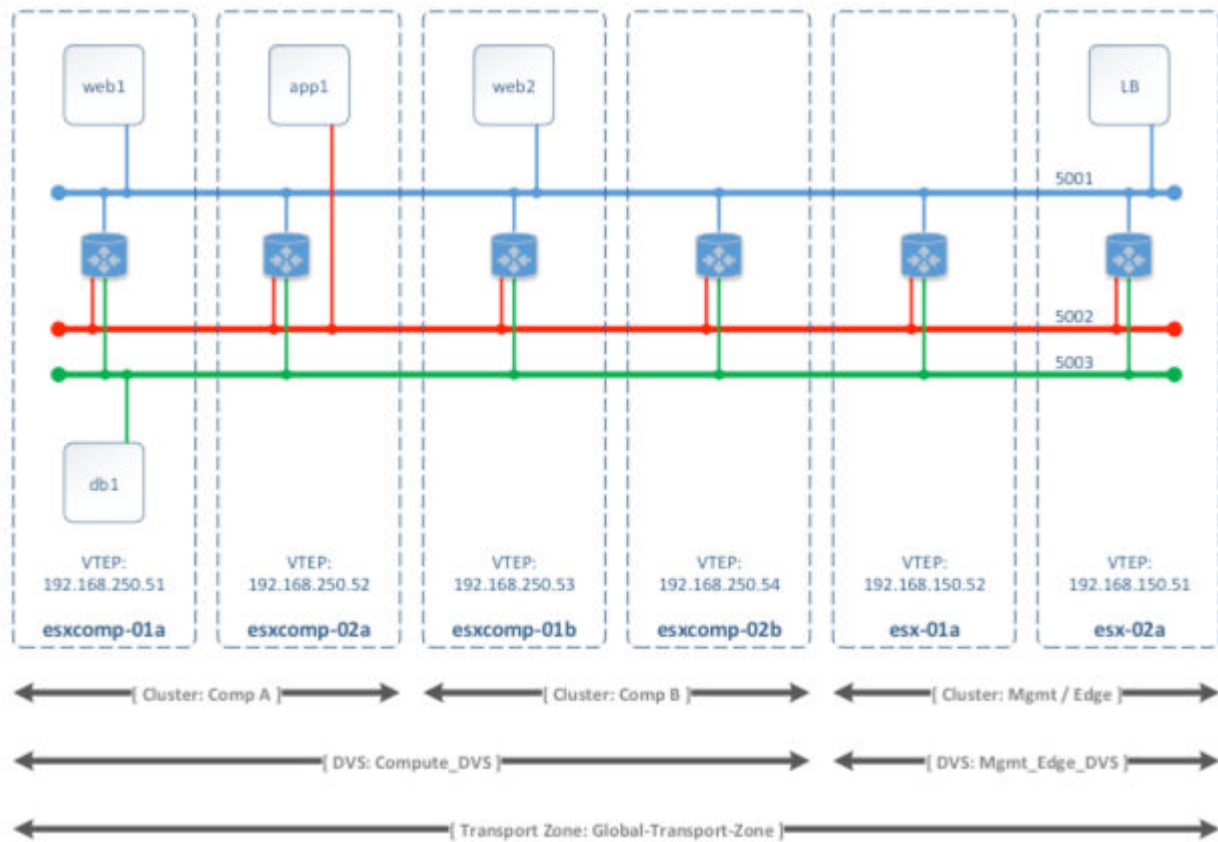
NSX 環境には、要件に基づいて 1 つ以上のトランスポート ゾーンを設定できます。ホスト クラスタは、複数のトランスポート ゾーンに属することができます。論理スイッチは、1 つのトランスポート ゾーンのみに属することができます。

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

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

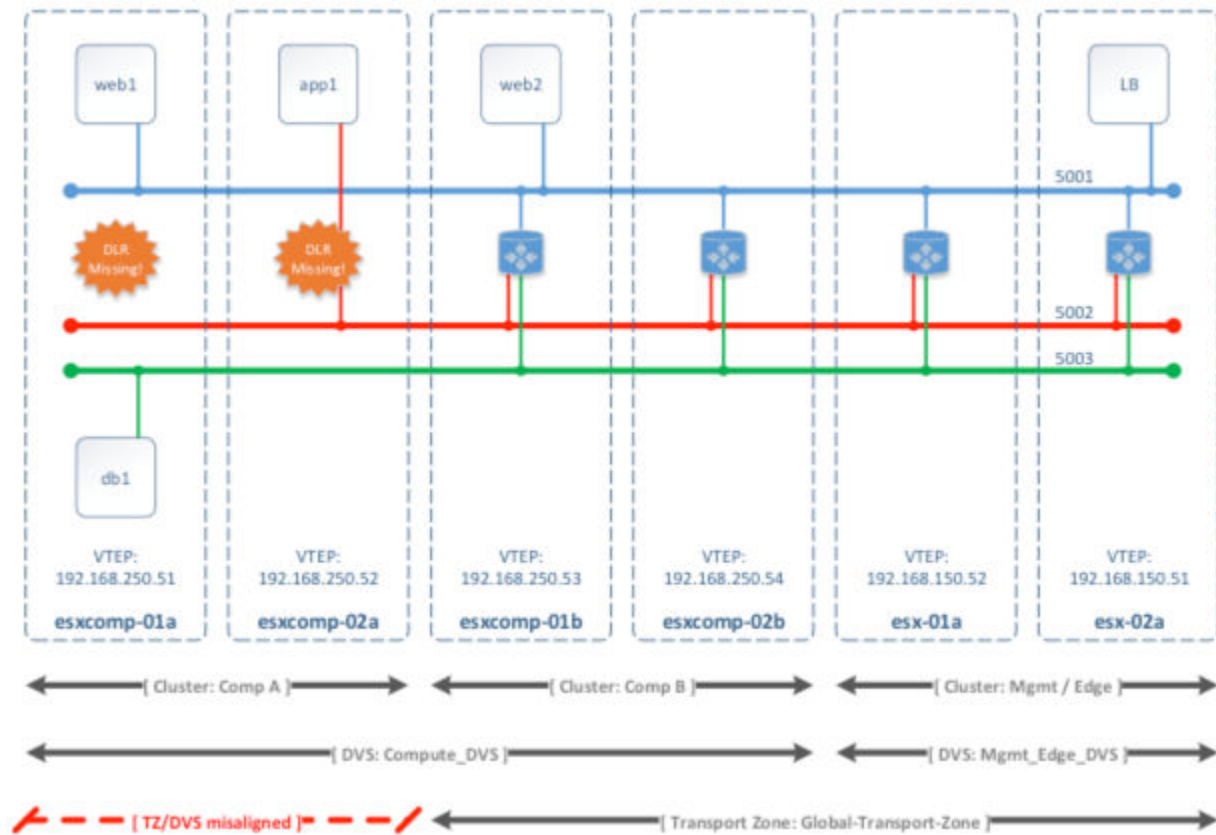
- レイヤー 3 接続が必要なクラスタは、Edge クラスタ（レイヤー 3 Edge デバイス（分散論理ルーターや Edge Services Gateway）があるクラスタ）と同じトランスポート ゾーンに属している必要があります。
- Web サービス用とアプリケーション サービス用の 2 つのクラスタがあるとします。これらの 2 つのクラスタの仮想マシン間で VXLAN 接続を行うには、両方のクラスタが同じトランスポート ゾーンに属している必要があります。
- 同じトランスポート ゾーンに属しているすべての論理スイッチは、そのトランスポート ゾーンに属しているクラスタ内のすべての仮想マシンで認識され、使用することができます。セキュリティで保護された環境がクラスタに含まれている場合、他のクラスタの仮想マシンがその環境を使用できることは望ましくありません。この場合は、セキュリティで保護されたクラスタを隔離されたトランスポート ゾーンに配置できます。
- vSphere Distributed Switch (VDS または DVS) の範囲は、トランスポート ゾーンの範囲と一致している必要があります。マルチクラスタ VDS 構成でトランスポート ゾーンを作成する場合、選択した VDS 内のすべてのクラスタがそのトランスポート ゾーンに属していることを確認します。これにより、VDS dvPortgroup が使用可能なすべてのクラスタで DLR が使用できるようになります。

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



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

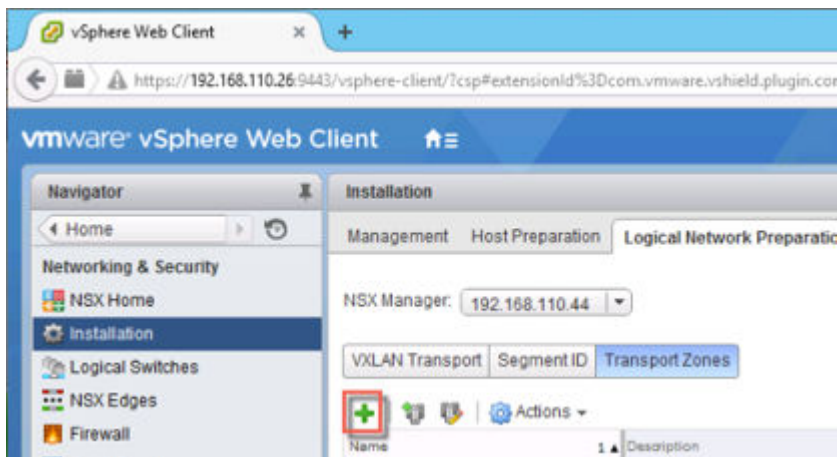
たとえば、トランスポート ゾーンが VDS 境界と合っていないと、論理スイッチ（5001、5002、5003）とそれらの論理スイッチが接続される DLR インスタンスの範囲の結合が解除されて、クラスタ Comp A 内の仮想マシンが DLR 論理インターフェイス (LIF) にアクセスできなくなります。



手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール手順 (Installation)] に移動し、[論理ネットワークの準備 (Logical Network Preparation)] タブを選択します。
- 2 [トランスポートゾーン (Transport Zones)] をクリックし、[新規トランスポートゾーン (New Transport Zone)] (+) アイコンをクリックします。

次はその例です。



- 3 [新規トランスポート ゾーン] ダイアログ ボックスで、トランスポート ゾーンの名前を入力し、オプションで説明を入力します。
- 4 環境にコントローラ ノードがあるかどうか、またはマルチキャスト アドレスを使用するかどうかに応じて、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 コントローラによって処理されます。すべてのユニキャスト トラフィックで、最適化されたヘッドエンド レプリケーションを利用します。マルチキャスト IP アドレスや特別なネットワーク設定は必要ありません。
 - [ハイブリッド (Hybrid)] : ローカル トラフィック レプリケーションを物理ネットワーク (L2 マルチキャスト) にオフロードします。最初のホップのスイッチで IGMP スヌーピング、各 VTEP サブネット で 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。

5 トランスポート ゾーンに追加するクラスタを選択します。

次はその例です。

New Transport Zone

Name:

Description:

Replication mode:

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

Select clusters that will be part of the Transport Zone

	Name	NSX vSwitch	Status
<input checked="" type="checkbox"/>	Compute Cluster A	Compute_DVS	✓ Normal
<input checked="" type="checkbox"/>	Compute Cluster B	Compute_DVS	✓ Normal
<input checked="" type="checkbox"/>	Management and Edge Clust...	Mgmt_VDS	✓ Normal
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

OK Cancel

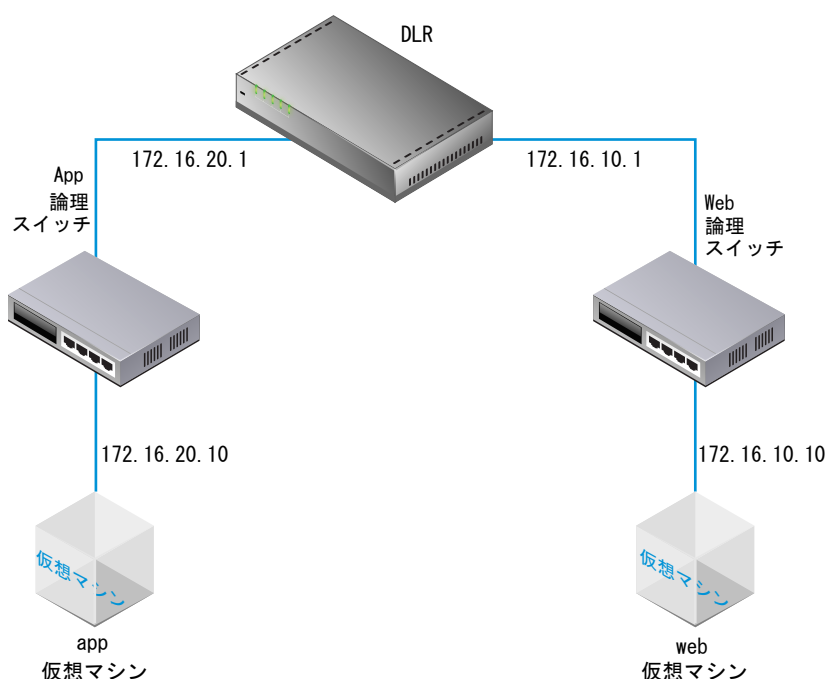
次のステップ

これで、トランスポート ゾーンを設定できたので、論理スイッチを追加できます。

論理スイッチの追加

NSX 論理スイッチは、基盤となるハードウェアから完全に分離された仮想環境内で、切り替え機能（ユニキャスト、マルチキャスト、ブロードキャスト）を再現します。論理スイッチは、仮想マシンを接続できるネットワーク接続を提供する点で、VLAN と似ています。同じ論理スイッチに接続された仮想マシンは、VXLAN 経由で互いに通信できます。各論理スイッチは、VLAN ID に似た セグメント ID を持っています。ただし VLAN ID とは異なり、セグメント ID は最大 1,600 万個まで設定できます。

論理スイッチを追加する場合、構築する特定のトポロジを考慮することが重要です。たとえば、次の単純なトポロジでは、2つの論理スイッチが1つの分散論理ルーター (DLR) に接続されています。この図では、各論理スイッチが1つの仮想マシンに接続されています。2つの仮想マシンのホストやホスト クラスタは同じにすることも、別々にすることもできます。DLR で仮想マシンを分離しない場合、仮想マシンで設定された、基になる IP アドレスのサブネットを同じにすることができます。DLR で仮想マシンを分離する場合、（この例のように）仮想マシンの IP アドレスのサブネットを別々にする必要があります。



前提条件

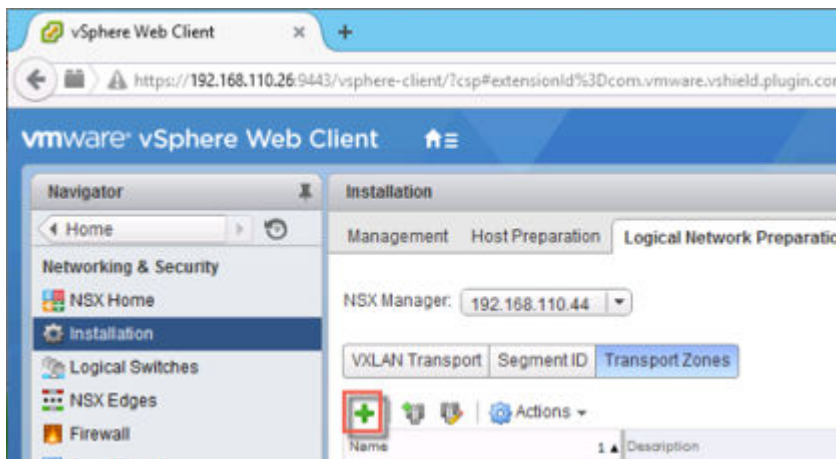
- vSphere Distributed Switch が設定されている
- NSX Manager をインストールがインストールされている

- コントローラがデプロイされている
- ホスト クラスタが NSX 用に準備されている
- VXLAN が設定されている
- セグメント ID プールが設定されている
- トランスポート ゾーンが作成されている

手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [論理スイッチ (Logical Switches)] の順に移動します。
- 2 [新規論理スイッチ (New Logical Switch)] (+) アイコンをクリックします。

次はその例です。



- 3 論理スイッチの名前と説明（説明は任意）を入力します。
- 4 論理スイッチを作成するトランスポート ゾーンを選択します。

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

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あることがあります。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。

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

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

- 6 (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 をトラッキングしている仮想 NIC を仮想マシンで使用している場合は、[MAC ラーニングの有効化 (Enable MAC learning)] をクリックします。

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

この例には、デフォルト設定の app 論理スイッチが表示されています。

New Logical Switch

Name: * app

Description:

Transport Zone: * tz1 Change Remove

Replication mode:

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

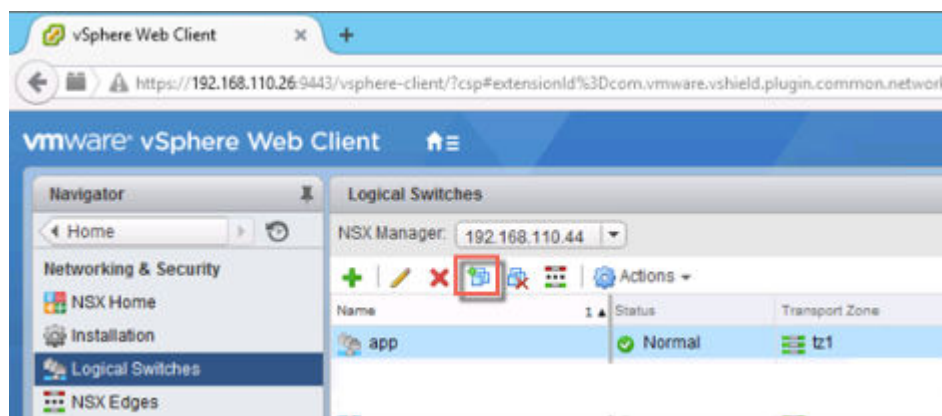
☒ Enable IP Discovery

☐ Enable MAC Learning

OK Cancel

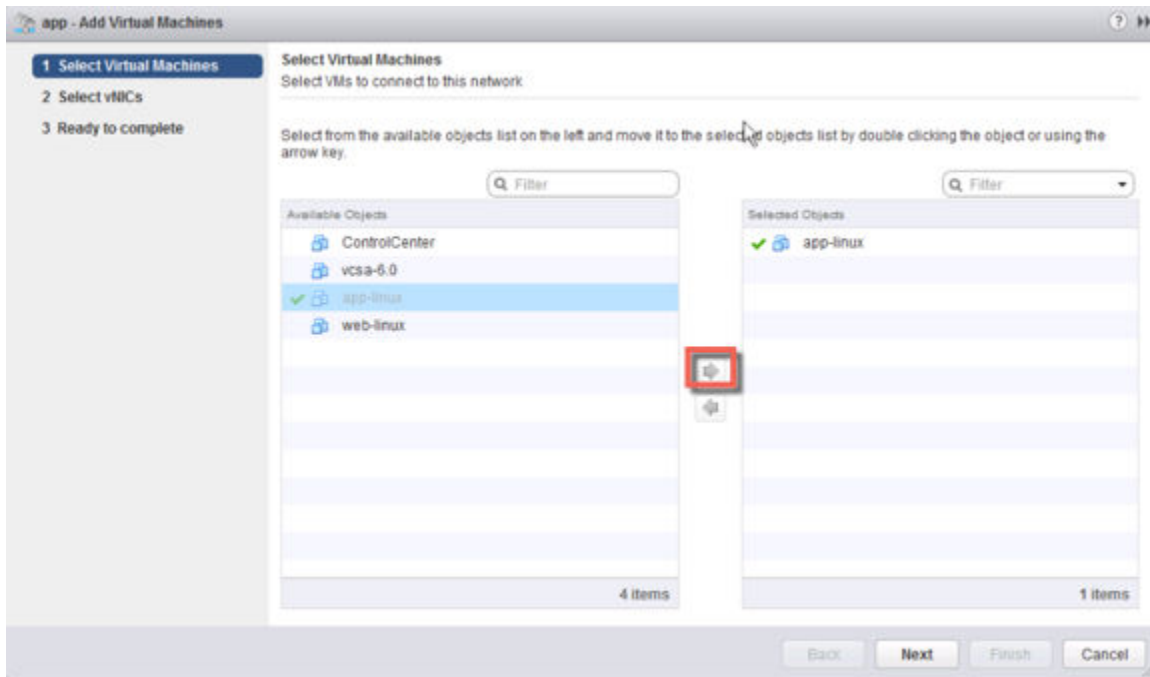
- 7 スイッチを選択して [仮想マシンの追加 (Add Virtual Machine)] (🔗) アイコンをクリックし、仮想マシンを論理スイッチに接続します。

次はその例です。



8 仮想マシンを選択して右矢印ボタンをクリックします。

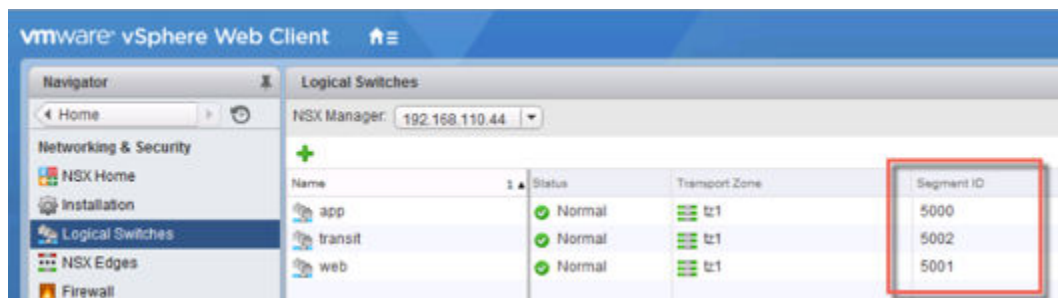
次はその例です。



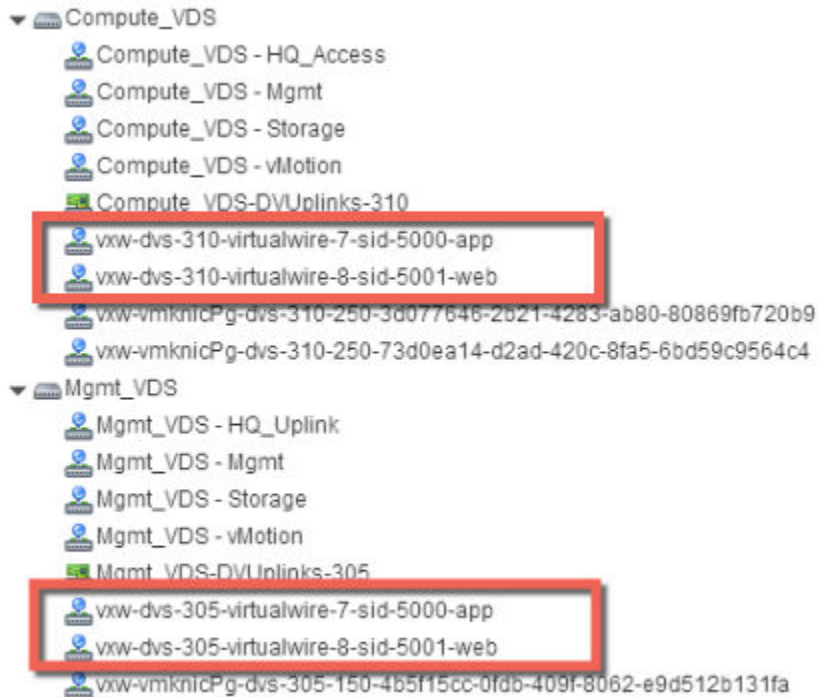
9 vNIC を選択します。

作成した各論理スイッチはセグメント ID プールから ID を受け取り、仮想ワイヤが作成されます。仮想ワイヤは、各 vSphere Distributed Switch で作成される dvPortgroup です。仮想ワイヤ記述子には、論理スイッチの名前と論理スイッチのセグメント ID が含まれます。割り当てられたセグメント ID は、次の例に示すように複数の場所に表示されます。

[ホーム (Home)] > [Networking and Security (Networking & Security)] > [論理スイッチ (Logical Switches)] :

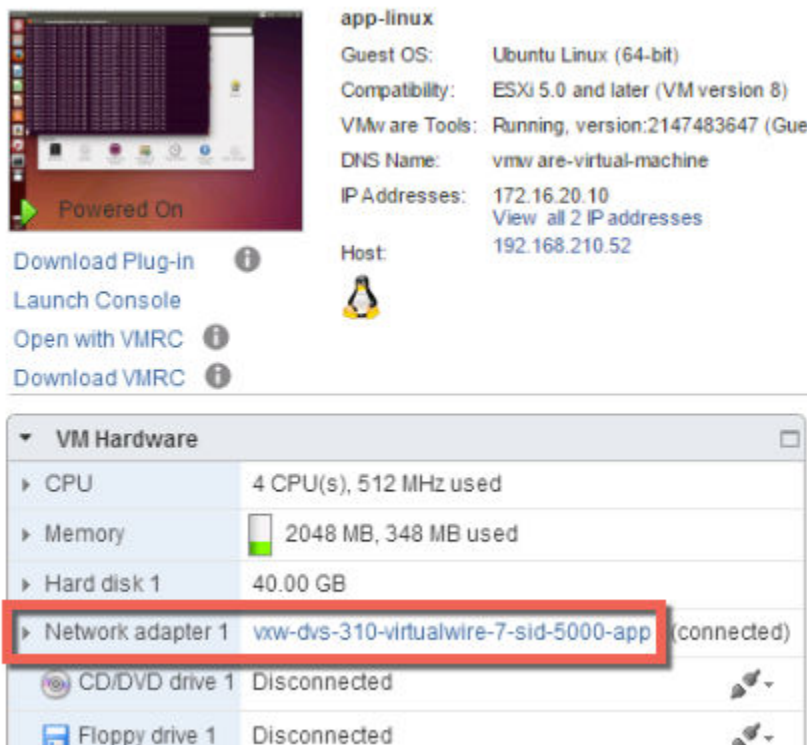


[ホーム (Home)] > [ネットワーク (Networking)] :



両方の vSphere Distributed Switch (Compute_VDS と Mgmt_VDS) で仮想ワイヤが作成されています。これは、これらの両方の vSphere Distributed Switch が、Web および app 論理スイッチに関連付けられているトランスポート ゾーンのメンバーであるためです。

[ホーム (Home)] > [ホストおよびクラスター (Hosts and Clusters)] > [仮想マシン (VM)] > [サマリ (Summary)] :



論理スイッチに接続された仮想マシンを実行しているホストで、ログインして次のコマンドを実行し、ローカル VXLAN の設定および状態情報を表示します。

- ホスト固有の VXLAN の詳細を表示します。

```
~ # esxcli network vswitch dvs vmware vxlan list
```

VDS ID	VDS Name	MTU	Segment ID	Gateway
IP	Gateway MAC	Network Count	Vmknics Count	
88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49	Compute_VDS	1600	192.168.250.0	
192.168.250.1 ff:ff:ff:ff:ff:ff	0	1		

注: `esxcli network vswitch dvs vmware vxlan` コマンドで「Unknown command or namespace」というエラー メッセージが表示された場合、ホストで `/etc/init.d/hostd restart` コマンドを実行して、もう一度やり直してください。

VDS Name には、ホストが接続されている vSphere Distributed Switch が表示されます。

Segment ID は、VXLAN が使用する IP ネットワークです。

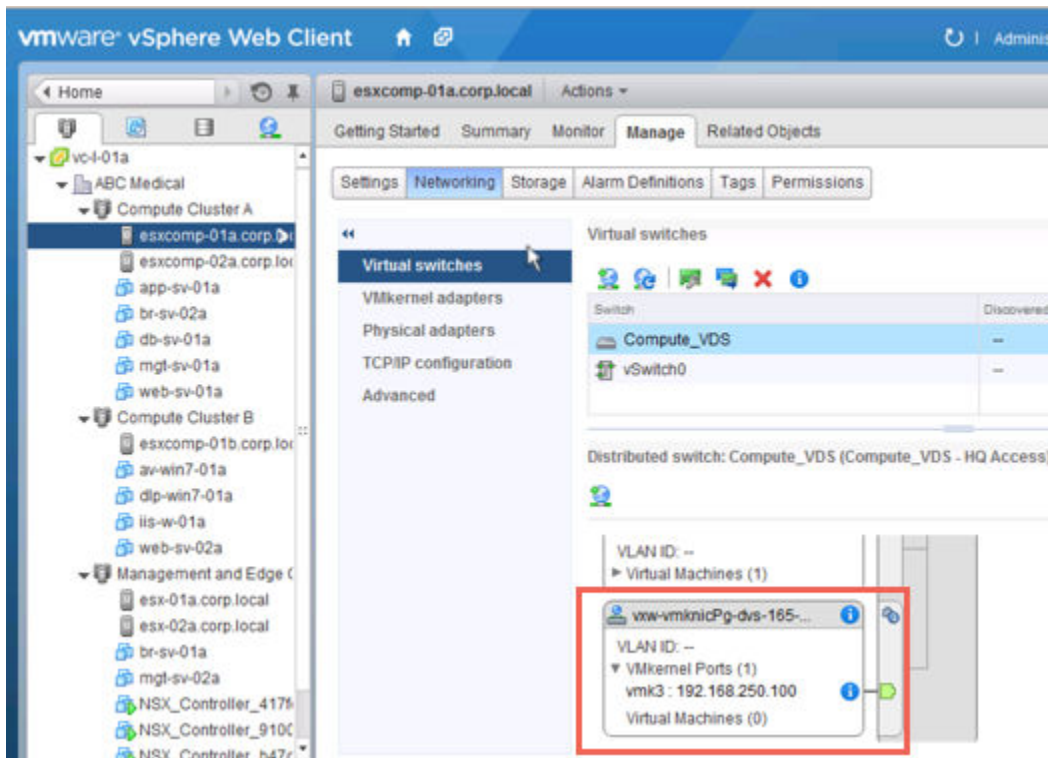
Gateway IP は、VXLAN が使用するゲートウェイ IP アドレスです。

[Gateway MAC (ゲートウェイ MAC)] アドレスは、ff:ff:ff:ff:ff:ff のままです。

Network Count は、DLR が論理スイッチに接続されない限り 0 のままです。

Vmknics Count は、論理スイッチに接続されている仮想マシンの数と一致します。

- IP VTEP インターフェイスの接続をテストし、VXLAN のカプセル化に対応して MTU が増えたことを確認します。vmknic インターフェイスの IP アドレスに ping します。このアドレスは、ホストの vSphere Web Client の [管理 (Manage)] > [ネットワーク (Networking)] > [仮想スイッチ (Virtual switches)] ページで確認できます。



-d フラグを使用すると、IPv4 パケットに DF（フラグメント禁止）ビットが設定されます。-s フラグを使用すると、パケット サイズが設定されます。

```
root@esxcomp-02a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.100
PING 192.168.250.100 (192.168.250.100): 1570 data bytes
1578 bytes from 192.168.250.100: icmp_seq=0 ttl=64 time=1.294 ms
1578 bytes from 192.168.250.100: icmp_seq=1 ttl=64 time=0.686 ms
1578 bytes from 192.168.250.100: icmp_seq=2 ttl=64 time=0.758 ms

--- 192.168.250.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.686/0.913/1.294 ms
~ #
```

```
root@esxcomp-01a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.101
PING 192.168.250.101 (192.168.250.101): 1570 data bytes
1578 bytes from 192.168.250.101: icmp_seq=0 ttl=64 time=0.065 ms
1578 bytes from 192.168.250.101: icmp_seq=1 ttl=64 time=0.118 ms

--- 192.168.250.101 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.065/0.091/0.118 ms
```

次のステップ

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

分散論理ルーターの追加


分散論理ルーター (DLR) は、ルーティング制御プレーンを搭載する一方で、カーネル モジュールのデータ プレーンを各ハイパーバイザー ホストに分散する仮想アプライアンスです。DLR の制御プレーン機能は、NSX コントローラ クラスタを使用して、ルーティングの更新をカーネル モジュールにプッシュします。

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

- NSX バージョン 6.0 および 6.1 とは異なり、NSX バージョン 6.2 では、論理ルーターでルーティングされる論理インターフェイス (LIF) を VLAN にブリッジされている VXLAN に接続できます。
- ECMP セットアップで ESG を使用している場合は、論理ルーター仮想アプライアンスの配置を選択する際に、そのアップストリーム ESG のいずれかと同じホストに配置しないようにしてください。これを実現するために DRS 非アフィニティ ルールを使用できます。これにより、論理ルーター転送時のホスト障害の影響を軽減できます。1 つのアップストリーム ESG を単独で使用する場合またはその ESG が HA モードの場合は、このガイドラインが適用されません。詳細については、『VMware NSX for vSphere Network Virtualization Design Guide』 (<https://communities.vmware.com/docs/DOC-27683>) を参照してください。

手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [NSX Edges] の順に移動します。
- 2 [追加 (Add)] () アイコンをクリックします。
- 3 [論理 (分散) ルーター (Logical (Distributed) Router)] を選択し、デバイスの名前を入力します。
この名前は vCenter インベントリに表示されます。1 つのテナントのすべての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。

次はその例です。

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Ready to complete

Name and description

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

☒ **Logical (Distributed) Router**
Provides Distributed Routing and Bridging capabilities.

Name:

Hostname:

Description:

Tenant:

☒ **Deploy Edge Appliance**
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.

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

Back Next Finish Cancel

4 (オプション) Edge Appliance をデプロイします。

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

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

5 (オプション) 高可用性を有効にします。

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

6 論理ルーターのパスワードを入力し、再入力します。

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

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

7 (オプション) SSH を有効にして、ログ レベルを設定します。

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

デフォルトでは、ログ レベルが「緊急」に設定されます。

次はその例です。

New NSX Edge

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

Settings

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

User Name: * admin

Password: *

Confirm password: *

☒ Enable SSH access

☐ Enable High Availability


Enable HA, for enabling and configuring High Availability.

Edge Control Level Logging EMERGENCY

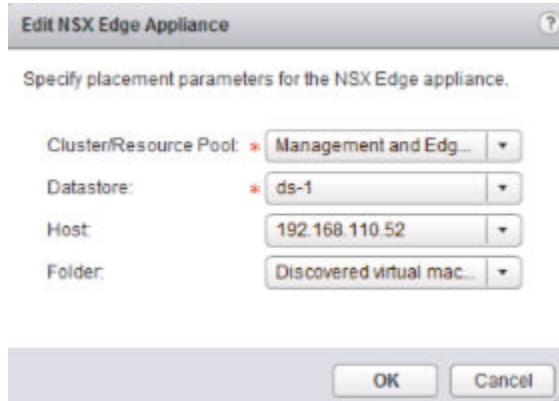
Set the Edge Control Level Logging

Back Next Finish Cancel

8 展開設定を行います。

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

次はその例です。



9 インターフェイスを設定します。

論理ルーターでは、IPv4 アドレスのみがサポートされます。

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

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

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

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

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

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

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

New NSX Edge

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

Configure interfaces

HA Interface Configuration

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

+ ✎ ✕

IP Address	Subnet Prefix Length
192.168.110.60*	24

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

Configure interfaces of this NSX Edge

+ ✎ ✕

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

Back Next Finish Cancel

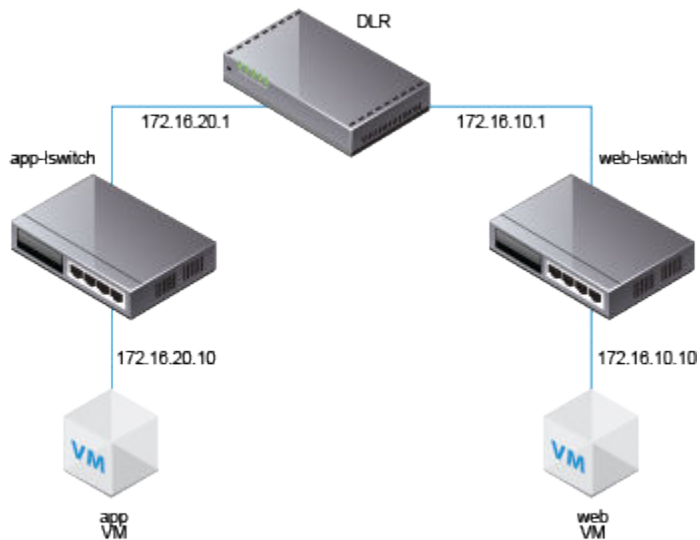
10 デフォルト ゲートウェイを設定します。

次はその例です。

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

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

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



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

- すべての論理ルーター インスタンス情報をリストします。

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

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

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

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

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

出力には、指定した論理ルーター（この例では edge-1）に接続されている論理スイッチが属するトランスポート ゾーンの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。

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

```
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、ルータに関する追加情報をリストします。これは、ホストと通信しているコントローラを把握するのに便利です。

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

VDR Instance Information :

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

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

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

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

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

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

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

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

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

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

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

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

app 仮想マシンから Web 仮想マシン：

```
vmware@vmware-virtual-machine:~$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_seq=1 ttl=63 time=2.15 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=63 time=1.60 ms
```

MAC テーブルを確認します。

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

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

ARP テーブルを確認します。

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

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

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

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

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

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

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

LR-Id を書き留め、次のコマンドで使します。

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

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

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

- コントローラから特定の VNI への接続を表示します。

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

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

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

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

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

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

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

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

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

- [Control 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 検出が無効になっていてもリストされます。

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

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

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

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

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

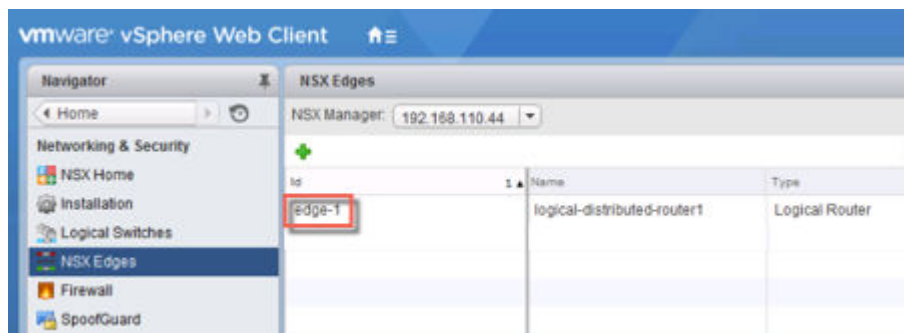
次のステップ

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

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

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

次はその例です。



Edge Services Gateway の追加

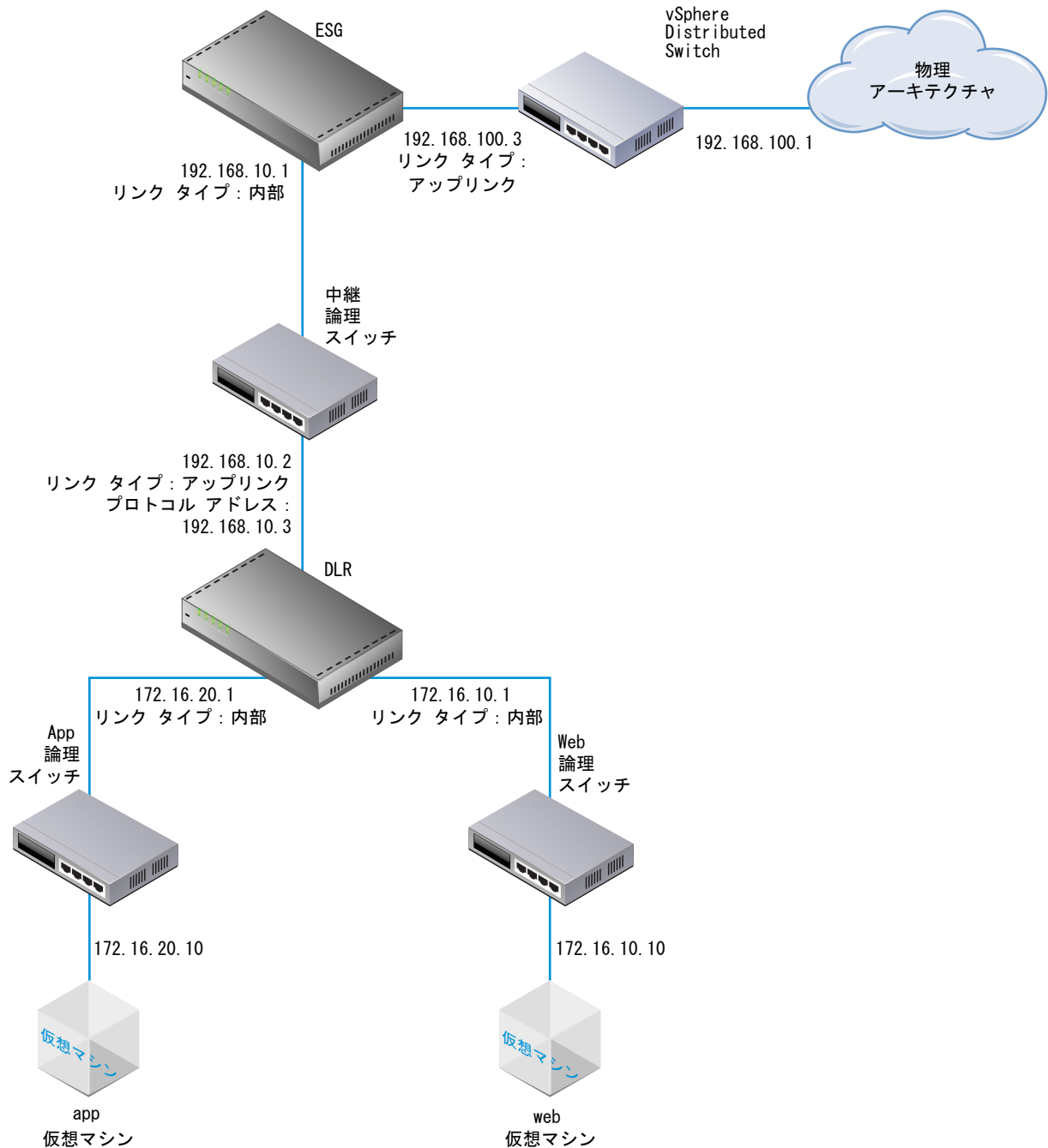
データセンターには、複数の NSX Edge Services Gateway 仮想アプライアンスをインストールできます。各 NSX Edge 仮想アプライアンスには、アップリンクと内部のネットワーク インターフェイスを合計で 10 個指定できます。内部インターフェイスは保護されたポート グループに接続され、そのポート グループ内の保護された仮想マシンすべてのゲートウェイとして機能します。内部インターフェイスに割り当てられたサブネットは、パブリックにルーティングされる IP アドレス空間にも、ネットワーク アドレス変換またはルーティングされる RFC 1918 専用空間にもなります。ファイアウ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

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

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

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

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




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

前提条件

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

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

手順

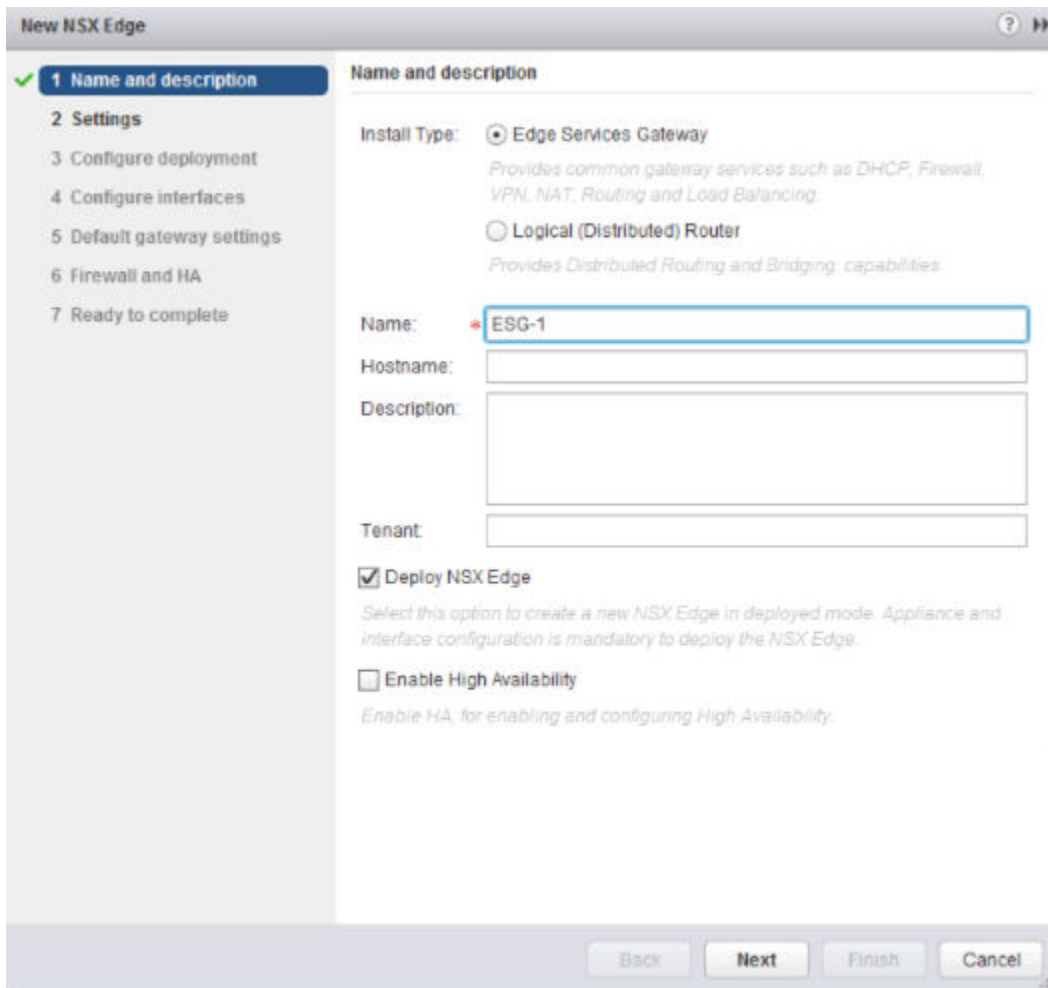
- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [NSX Edges] に移動し、[追加 (Add)] () アイコンをクリックします。
- 2 [Edge Services Gateway] を選択し、デバイスの名前を入力します。

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

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

オプションで、説明とテナントを入力し、高可用性を有効にできます。

次はその例です。



The screenshot shows the 'New NSX Edge' configuration window. On the left, a sidebar lists steps: 1 Name and description (selected), 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings, 6 Firewall and HA, and 7 Ready to complete. The main area is titled 'Name and description'. It contains the following fields and options:

- Install Type:** Two radio buttons. 'Edge Services Gateway' is selected, with a description: 'Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.' The other option is 'Logical (Distributed) Router' with a description: 'Provides Distributed Routing and Bridging capabilities.'
- Name:** A text box containing 'ESG-1'.
- Hostname:** An empty text box.
- Description:** A large empty text area.
- Tenant:** An empty text box.
- Deploy NSX Edge:** A checked checkbox with a description: 'Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.'
- Enable High Availability:** An unchecked checkbox with a description: 'Enable HA, for enabling and configuring High Availability.'

At the bottom, there are four buttons: 'Back', 'Next' (highlighted), 'Finish', and 'Cancel'.

- 3 ESG のパスワードを入力し、再入力します。

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

- 1 文字以上の大文字
- 1 文字以上の小文字

- 1 文字以上の数字
- 1 文字以上の特殊文字

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

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

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

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

次はその例です。

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

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

[「NSX のシステム要件」](#) を参照してください。

6 Edge Appliance を作成します。

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

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

次はその例です。

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

- 8 インターフェイスを設定します。

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

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

1 つのインターフェイスには、重複しない複数のサブネットを設定できます。

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

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

オプションで、インターフェイスの MAC アドレスを入力できます。

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

オプションで、MTU を変更することができます。

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

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

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

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

次はその例です。

Edit NSX Edge Interface

vNIC#: 1

Name: * Internal

Type: ☒ Internal ☐ Uplink

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

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

IP Address	Subnet Prefix Length
192.168.10.1*	29

MAC Addresses:

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

MTU:

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

Fence Parameters:

Example: ethernet0.filter1.param1=1

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

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

New NSX Edge

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

Configure interfaces

Configure interfaces of this NSX Edge

+ ✎ ✕

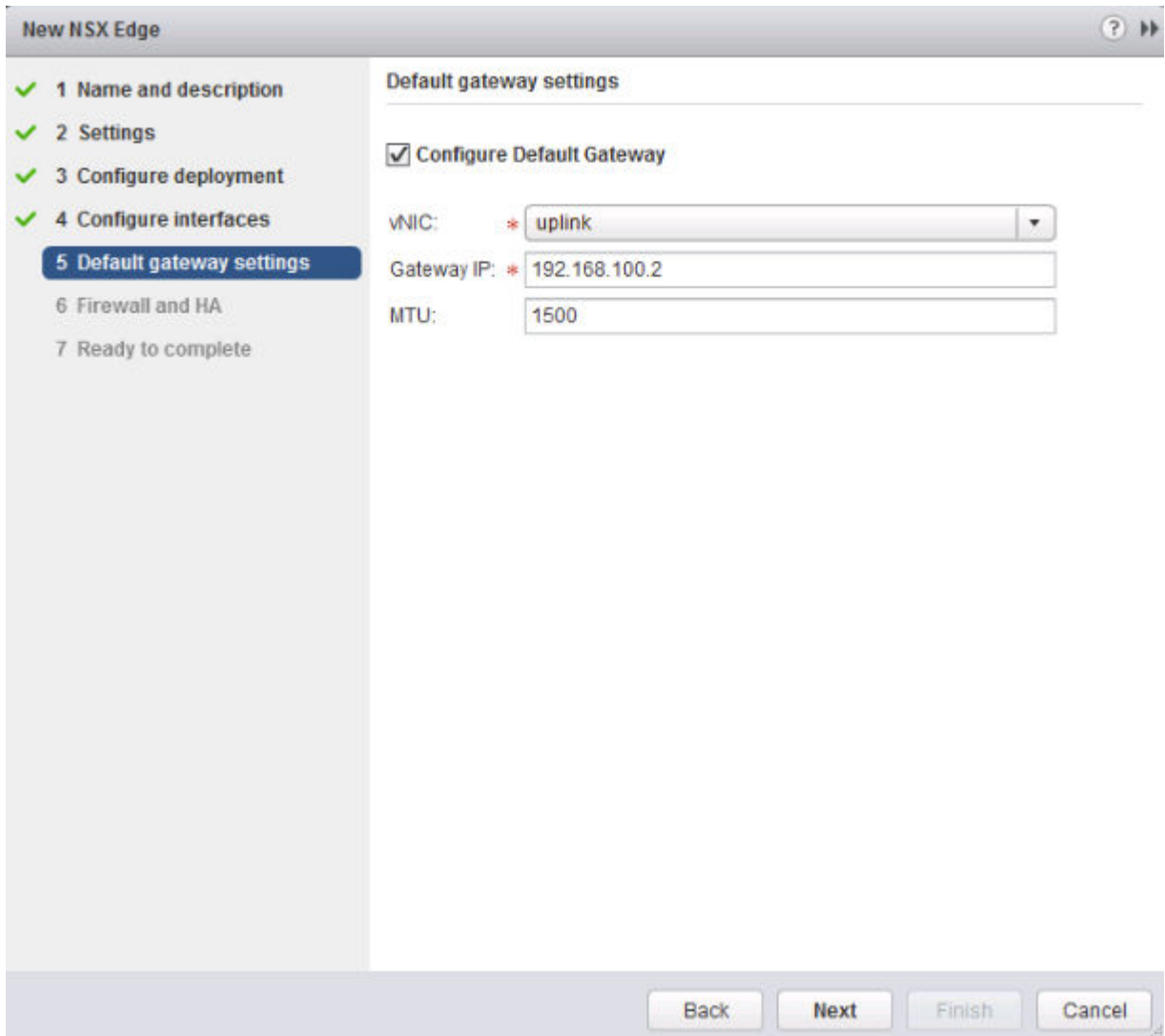
vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	uplink	192.168.100.3	24	Mgmt_VDS - HQ_Uplink
1	internal	192.168.10.1	29	transit-switch

Back Next Finish Cancel

9 デフォルト ゲートウェイを設定します。

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

次はその例です。



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



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

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

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

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

次はその例です。

New NSX Edge

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

Firewall and HA

☒ **Configure Firewall default policy**

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: * internal

Declare Dead Time: 15 (seconds)

Management IPs:

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

Back Next Finish Cancel

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

次のステップ

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

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

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

論理（分散）ルーター上での OSPF の設定

19

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

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

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

エリアはエリア ID で識別されます。

前提条件

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

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

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 論理ルーターをダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[OSPF] をクリックします。
- 5 OSPF を有効にします。
 - a ウィンドウの右上にある [編集 (Edit)] をクリックして、[OSPF の有効化 (Enable OSPF)] をクリックします。
 - b [転送アドレス (Forwarding Address)] に、データパス パケットを転送するために、ホスト内のルーターのデータパス モジュールで使用する IP アドレスを入力します。
 - c [プロトコル アドレス (Protocol Address)] に、[転送アドレス (Forwarding Address)] と同じサブネット内の一意的 IP アドレスを入力します。プロトコル アドレスは、ピアと隣接するために、プロトコルによって使用されます。

6 OSPF エリアを設定します。

- a オプションで、デフォルトで設定されている Not-So-Stubby Area (NSSA) 51 を削除します。
- b [エリア定義 (Area Definitions)] で、[追加 (Add)] アイコンをクリックします。
- c エリア ID を入力します。NSX Edge では、IP アドレスまたは 10 進数形式のエリア ID を使用できます。
- d [タイプ (Type)] で、[標準 (Normal)] または [NSSA] を選択します。

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

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

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

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

8 エリアにインターフェイスをマッピングします。

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

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

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

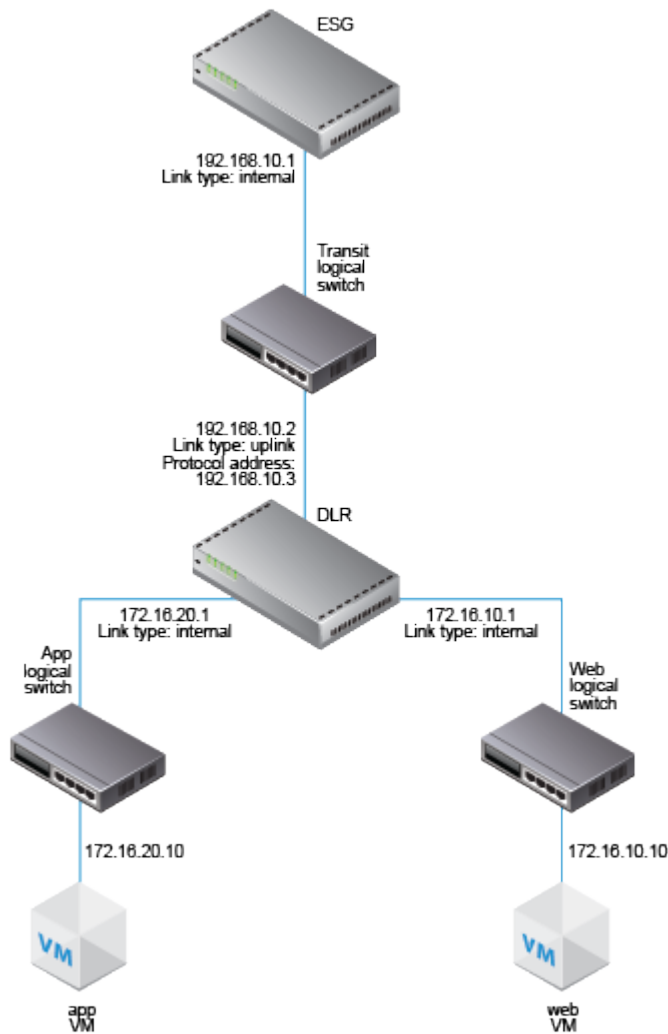
- a [Hello 間隔 (Hello Interval)] には、インターフェイスで送信されるハロー パケット間のデフォルト間隔が表示されます。
- b [Dead 間隔 (Dead Interval)] には、1 つ以上のハロー パケットをネイバーから受信しないとルーターでネイバーの停止が宣言されるデフォルト間隔が表示されます。
- c [優先順位 (Priority)] には、インターフェイスのデフォルトの優先順位が表示されます。優先順位の最も高いインターフェイスが指定ルーターになります。
- d インターフェイスの [コスト (Cost)] には、そのインターフェイスを通じてパケット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

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

例：論理（分散）ルーター上で設定されている OSPF

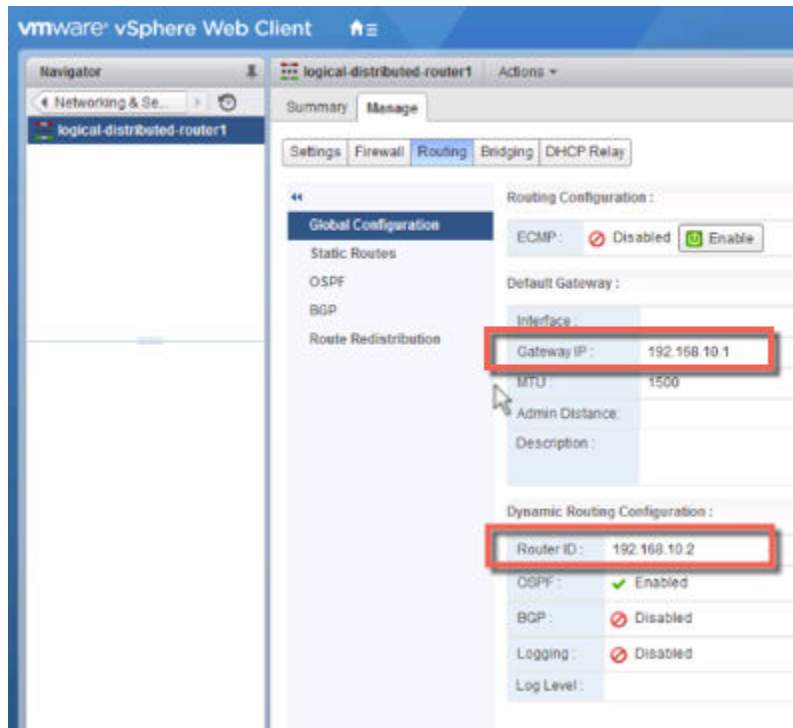
次に示す、OSPF を使用する単純な NSX シナリオでは、論理ルーター (DLR) と Edge Services Gateway (ESG) が OSPF のネイバー関係になっています。

図 19-1. NSX トポロジ



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

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



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

The screenshot shows the configuration page for a logical distributed router named 'logical-distributed-router1'. The 'Routing' tab is selected in the top navigation bar. On the left, the 'OSPF' option is highlighted in the configuration menu. The main area displays the 'OSPF Configuration' and 'Area Definitions' sections.

OSPF Configuration:

Status :	✓ Enabled
Protocol Address :	192.168.10.3
Forwarding Address :	192.168.10.2
Graceful Restart :	✓ Enabled
Default Originate :	✗ Disabled

Area Definitions:

Area ID	Type	Authentication
0	Normal	None

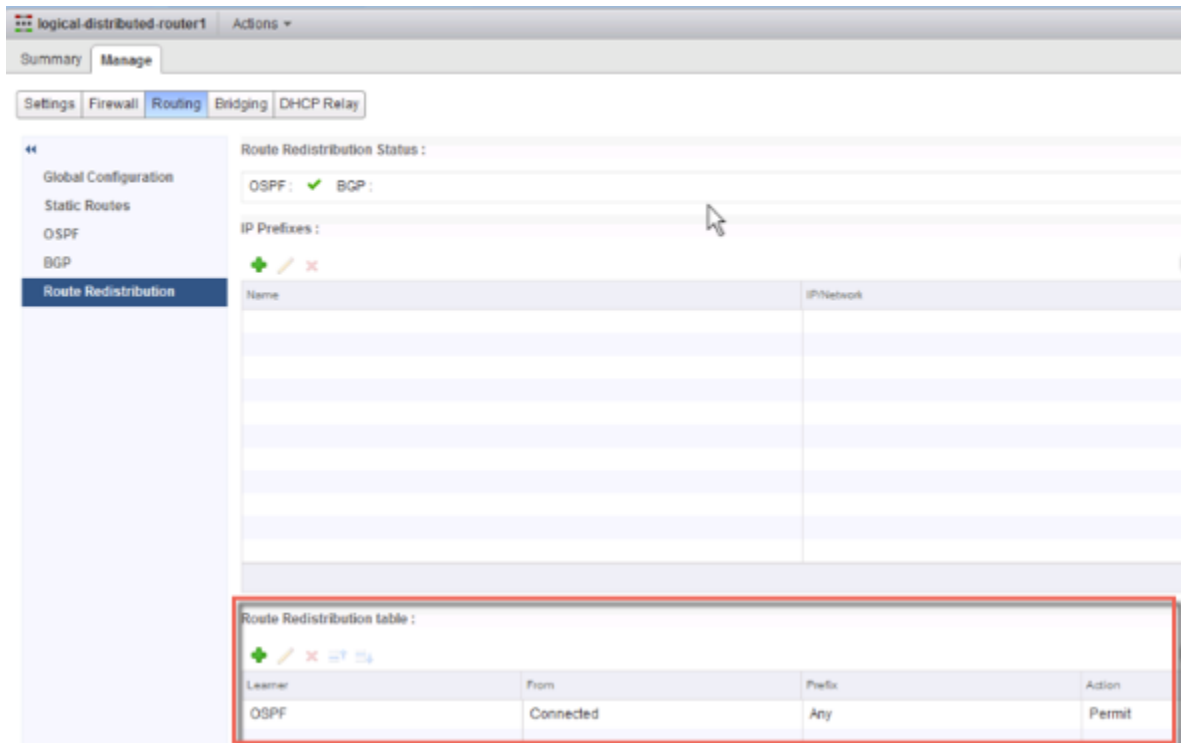
Area to Interface Mapping:

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

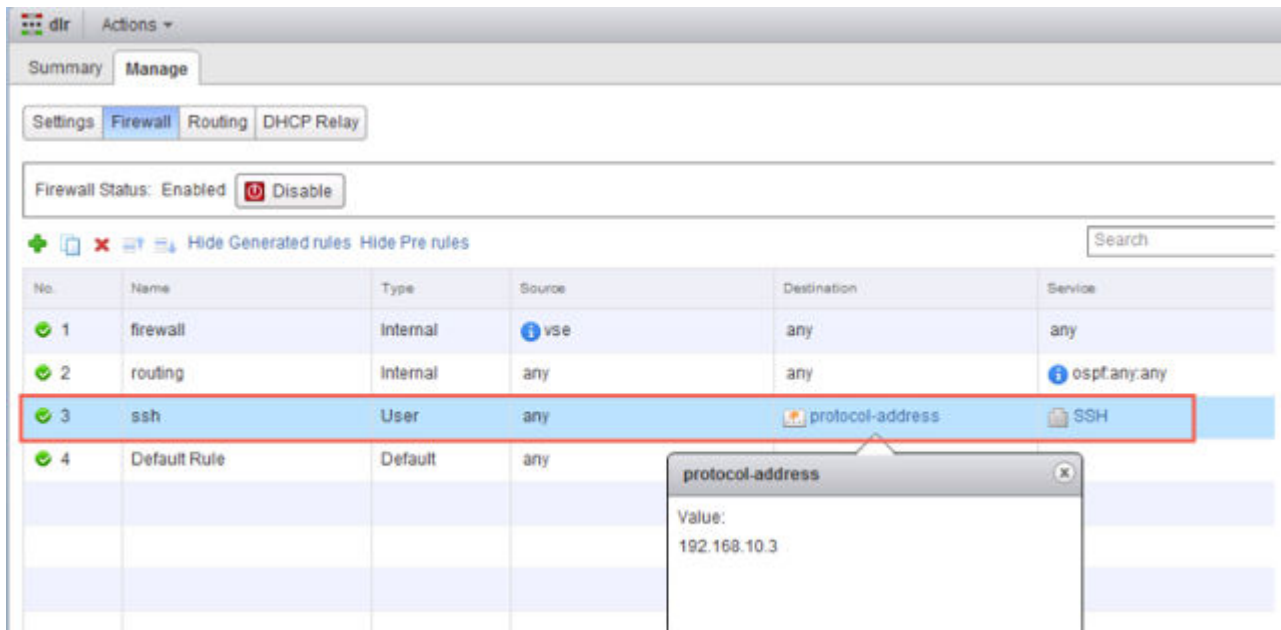
次のステップ

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

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



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



Edge Services Gateway 上での OSPF の設定

20

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

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

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

エリアはエリア ID で識別されます。

前提条件

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

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

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 ESG をダブルクリックします。
- 4 [ルーティング (Routing)] をクリックし、[OSPF] をクリックします。
- 5 OSPF を有効にします。
 - a ウィンドウの右上にある [編集 (Edit)] をクリックして、[OSPF の有効化 (Enable OSPF)] をクリックします。
 - b (オプション) OSPF サービスの再起動時にパケット転送が中断されないようにするには、[グレースフル リスタートの有効化 (Enable Graceful Restart)] をクリックします。
 - c (オプション) ESG が自身をデフォルト ゲートウェイとしてピアにアドバタイズできるようにするには、[デフォルトの発信元の有効化 (Enable Default Originate)] をクリックします。

6 OSPF エリアを設定します。

- a (オプション) デフォルトで設定されている Not-So-Stubby Area (NSSA) 51 を削除します。
- b [エリア定義 (Area Definitions)] で、[追加 (Add)] アイコンをクリックします。
- c エリア ID を入力します。NSX Edge では、IP アドレスまたは 10 進数形式のエリア ID を使用できます。
- d [タイプ (Type)] で、[標準 (Normal)] または [NSSA] を選択します。

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

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

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

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

8 エリアにインターフェイスをマッピングします。

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

9 (オプション) デフォルトの OSPF 設定を編集します。

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

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

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

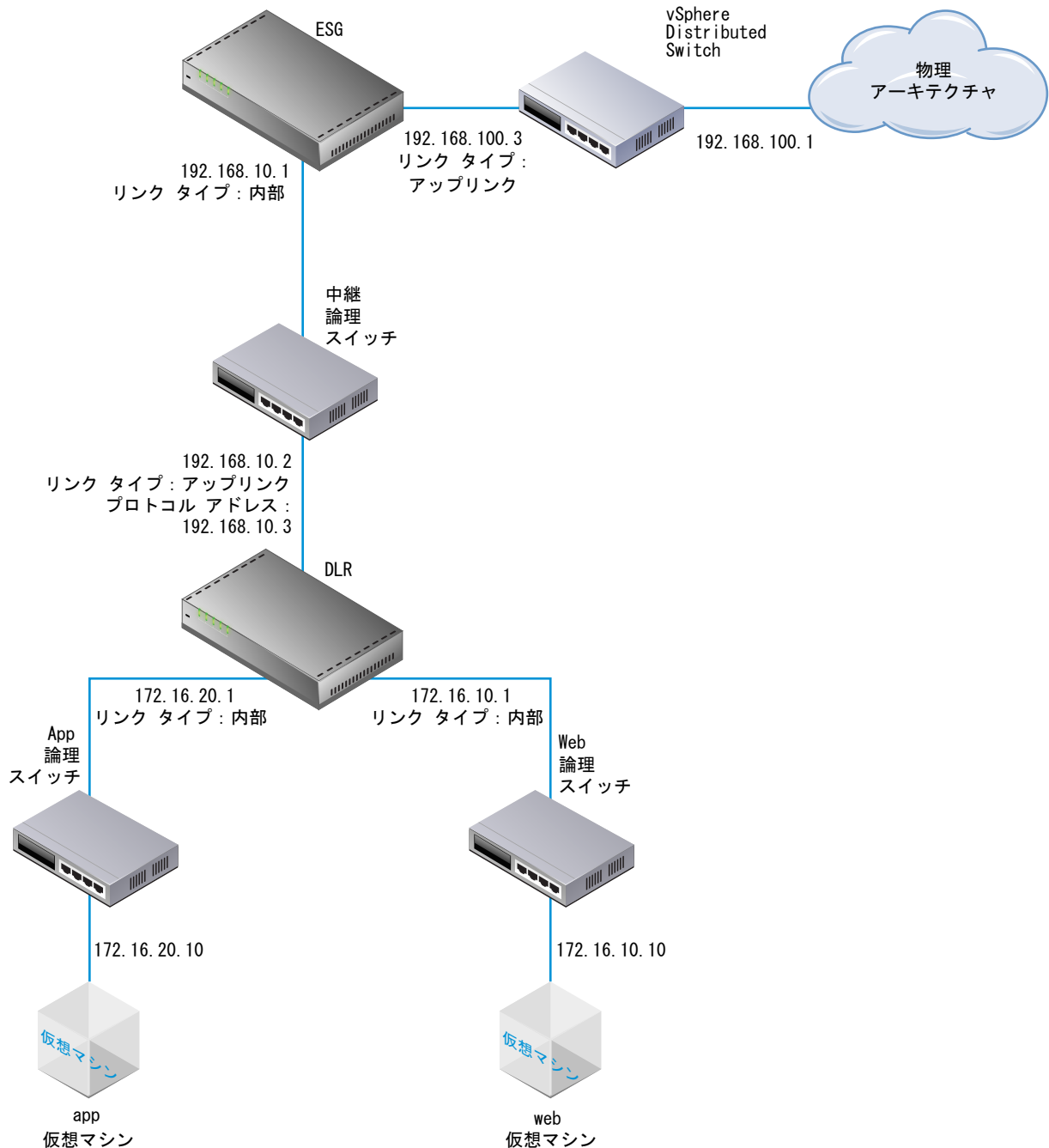
11 ルート再配分とファイアウォールの設定により、正しいルートがアドバタイズされることを確認します。

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

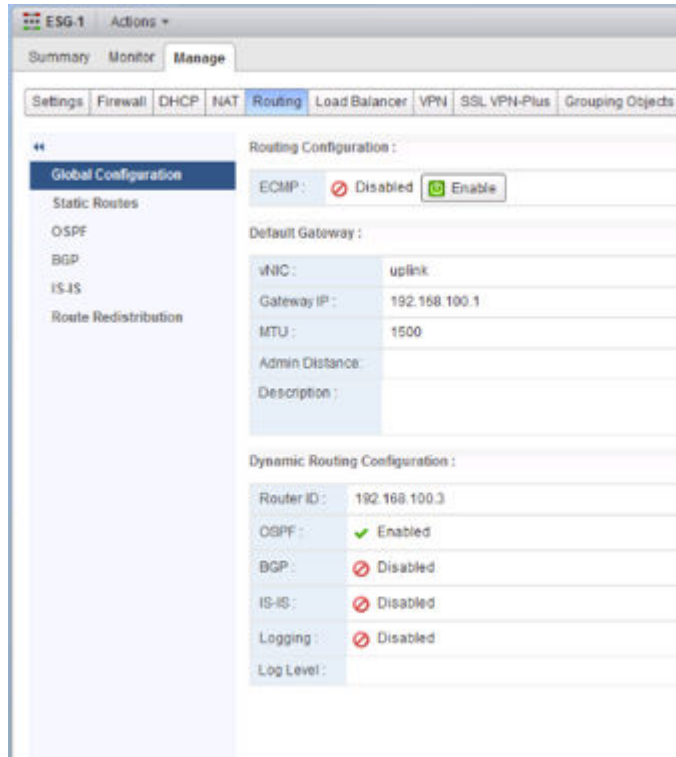
OSPF を使用する単純な NSX シナリオの 1 つとして、論理ルーターと Edge Services Gateway が OSPF のネイバー関係になっている例をここに示します。

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

図 20-1. NSX トポロジ



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



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

The screenshot displays the ESG-1 configuration interface, specifically the OSPF configuration page. The left sidebar shows a tree view with 'OSPF' selected. The main content area is divided into two sections: 'OSPF Configuration' and 'Area Definitions'.

OSPF Configuration:

- Status: ☒ Enabled
- Graceful Restart: ☒ Enabled
- Default Originate: ☐ Disabled

Area Definitions:

Area ID	Type	Authentication
0	Normal	None

Area to Interface Mapping:

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

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

Summary Monitor Manage

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

Global Configuration
Static Routes
OSPF
BGP
IS-IS
Route Redistribution

Route Redistribution Status :

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes :

+ - ✎ ✖

Name	IP Network

Route Redistribution table :

+ - ✎ ✖

Learned	From	Prefix	Action
OSPF	Connected	Any	Permit

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

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

```

NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
M1 - OSPF NSSA external type 1, M2 - OSPF NSSA external type 2

Total number of routes: 5

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

```

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

次はその例です。

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

```

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

```

```

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

```

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

```

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

```

```

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

```

ゲスト イントロスペクション のインストール

21

ゲスト イントロスペクション をインストールすると、クラスタ内の各ホストに新しい VIB とサービス仮想マシンが自動的にインストールされます。ゲスト イントロスペクション は、NSX Data Security、アクティビティ モニタリング、およびいくつかのサードパーティ セキュリティ ソリューションで必要になります。

ステートレス ホストでの自動デプロイ セットアップの場合、ESXi ホストの再起動後に、VMware NSX for vSphere 6.x サービス仮想マシン (SVM) を手動で再起動する必要があります。詳細については、ナレッジベースの記事 <http://kb.vmware.com/kb/2120649> を参照してください。



警告: VMware NSX for vSphere 6.x の環境では、サービス仮想マシン (SVM) の移行時 (vMotion/SvMotion) に、次の問題が発生することがあります。

- サービス仮想マシン (SVM) のデータ提供先となるサービス (ワークロード仮想マシン) が中断する
- ESXi ホストに障害が発生し、診断画面に次のようなバックトレースを含むパープル スクリーンが表示される

```
@BlueScreen: #PF Exception 14 in world www:WorldName IP 0xffffffff addr 0x0
PTes:0xffffffff;0xffffffff;0x0;
0xffffffff:[0xffffffff]VmMemPin_DecCount@vmkernel#nover+0x1b
0xffffffff:[0xffffffff]VmMemPinUnpinPages@vmkernel#nover+0x65
0xffffffff:[0xffffffff]VmMemPin_ReleaseMainMemRange@vmkernel#nover+0x6
0xffffffff:[0xffffffff]P2MCache_ReleasePages@vmkernel#nover+0x2a
0xffffffff:[0xffffffff]DVFilterVmciUnmapGuestPage@com.vmware.vmkapi#v2_2_0_0+0x34
```

これは、VMware ESXi 5.5.x および 6.x のホストに影響する既知の問題です。この問題を回避するには、サービス仮想マシン (SVM) をクラスタ内の別の ESXi ホストに手動で移行 (vMotion/SvMotion) しないでください。SVM を別のデータストアに移行 (svMotion) する場合は、SVM をオフにしてから別のデータストアに移行するコールドマイグレーションを使用することをお勧めします。

前提条件

このインストール手順の前提条件として、下記のシステムが必要です。

- データセンター内のクラスタの各ホストに、サポート対象のバージョンの vCenter Server および ESXi がインストールされている
- クラスタ内のホストが vCenter Server バージョン 5.0 から 5.5 にアップグレードされた場合は、それらのホストでポート 80 とポート 443 が開かれている


- ゲスト イントロスペクションをインストールするクラスタのホストで、NSX の準備が完了している『NSX インストール ガイド』で、「NSX 用ホスト クラスタの準備」セクションを参照してください。ゲスト イントロスペクション はスタンドアローン ホストにはインストールできません。アンチウイルスのオフロード機能を使用する目的で、ゲスト イントロスペクションを展開および管理するために NSX を使用する場合、ホストで NSX の準備を行う必要はありません。また、NSX for vShield Endpoint ライセンスでは、このような使い方は許可されません。
- NSX Manager 6.2 がインストールおよび実行されていること。
- NSX Manager と、ゲスト イントロスペクション サービスを実行する準備済みホストが同じ NTP サーバにリンクされ、時刻が同期されていることを確認します。これを行わない場合、ゲスト イントロスペクションとサードパーティ サービスに対して、クラスタのステータスが問題がないことを示す緑で表示されているにもかかわらず、仮想マシンがアンチウイルス サービスによって保護されていないことがあります。

NTP サーバを追加した場合、ゲスト イントロスペクションとすべてのサードパーティ サービスを再デプロイすることをお勧めします。

NSX ゲスト イントロスペクション サービス仮想マシンに IP アドレス プールから IP アドレスを割り当てる場合は、NSX ゲスト イントロスペクション をインストールする前に IP アドレス プールを作成します。『NSX 管理ガイド』の「IP アドレス プールの操作」セクションを参照してください。

vSphere Fault Tolerance は、ゲスト イントロスペクション とは連携しません。

手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 [新しいサービスのデプロイ (New Service Deployment)] () アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログ ボックスで、[ゲスト イントロスペクション (Guest Introspection)] を選択します。
- 4 [スケジュールを指定する (Specify schedule)] (ダイアログ ボックス下部) で、[今すぐデプロイする (Deploy now)] を選択して ゲスト イントロスペクション がインストールされたらすぐにデプロイするか、またはデプロイの日付と時間を選択します。
- 5 [次へ (Next)] をクリックします。
- 6 ゲスト イントロスペクションをインストールするデータセンターおよびクラスタを選択し、[次へ (Next)] をクリックします。
- 7 [ストレージおよび管理ネットワークの選択] ページで、サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み (Specified on host)] を選択します。デプロイ ワークフローを自動化するためには、[ホスト上が選択済み] ではなく、共有のデータストアとネットワークを使用することをお勧めします。

選択したデータストアは、選択したクラスタ内のすべてのホストで利用可能である必要があります。

[ホスト上が指定済み (Specified on host)] を選択した場合は、クラスタ内の各ホストに対して次のステップを実行します。

- a vSphere Web Client のホーム ページで、[vCenter] をクリックし、[ホスト (Hosts)] をクリックします。
- b [名前 (Name)] 列のホストをクリックし、[管理 (Manage)] タブをクリックします。

- c [エージェント仮想マシンの設定 (Agent VM Settings)] をクリックし、[編集 (Edit)] をクリックします。
 - d データストアを選択し、[OK] をクリックします。
- 8 管理インターフェイスをホストする分散仮想ポート グループを選択します。データストアが [ホスト上が指定済み (Specified on host)] に設定されている場合は、ネットワークも [ホスト上が指定済み (Specified on host)] に設定する必要があります。

選択したポート グループは、NSX Manager のポート グループにアクセスできる必要があります、選択したクラスタ内のすべてのホストで利用できる必要があります。

[ホスト上が指定済み (Specified on host)] を選択した場合は、ステップ 7 のサブステップを実行してホスト上のネットワークを選択します。クラスタに 1 台以上のホストを追加する場合は、データストアおよびネットワークを設定してからクラスタに追加する必要があります。

- 9 [IP 割り当て] で、次のいずれかを選択します。

選択	宛先
DHCP	DHCP (Dynamic Host Configuration Protocol) を使用して NSX ゲスト イントロスペクション サービス仮想マシンに IP アドレスを割り当てます。ホストが異なるサブネット上にある場合に、このオプションを選択します。
IP アドレス プール	選択された IP アドレス プール内の IP アドレスを NSX ゲスト イントロスペクション サービス仮想マシンに割り当てます。

- 10 [次へ (Next)] をクリックし、[設定内容の確認] ページで [終了 (Finish)] をクリックします。
- 11 [インストールの状態 (Installation Status)] 列に [成功 (Succeeded)] と表示されるまで、状況を監視します。
- 12 [インストールの状態 (Installation Status)] 列に [失敗 (Failed)] と表示された場合は、[失敗] の横にあるアイコンをクリックします。すべてのデプロイ エラーが表示されます。[解決 (Resolve)] をクリックしてエラーを修正します。エラーを解決すると、別のエラーが表示されることがあります。必要な操作を行い、再度 [解決 (Resolve)] をクリックします。

次のステップ

ゲスト仮想マシンに VMware Tools をインストールします。

NSX Data Security のインストール

注: NSX Data Security は、NSX 6.2.3 のリリースでは推奨されない機能です。NSX 6.2.3 では、ユーザーの判断でこの機能を引き続き使用できます。ただし、この機能は NSX の今後のリリースでは削除されることにご注意ください。

前提条件

Data Security をインストールするクラスタには、NSX ゲスト イントロスペクション がインストールされている必要があります。

Data Security サービス仮想マシンに IP プールから IP アドレスを割り当てる場合は、Data Security をインストールする前に IP プールを作成します。『NSX 管理ガイド』のグループ オブジェクトに関するページを参照してください。

手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 [新しいサービスの展開 (New Service Deployment)] () アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログ ボックスで、[Data Security] を選択し、[次へ (Next)] をクリックします。
- 4 [スケジュールを指定する (Specify schedule)] (ダイアログ ボックス下部) で、[今すぐデプロイする (Deploy now)] を選択して Data Security がインストールされたらすぐにデプロイするか、またはデプロイの日付と時間を選択します。
- 5 [次へ (Next)] をクリックします。
- 6 Data Security をインストールするデータセンターおよびクラスタを選択し、[次へ (Next)] をクリックします。
- 7 [ストレージおよび管理ネットワークの選択] ページで、サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み (Specified on host)] を選択します。

選択したデータストアは、選択したクラスタ内のすべてのホストで利用可能である必要があります。

[ホスト上が指定済み (Specified on host)] を選択した場合、そのホストの [エージェント仮想マシンの設定 (AgentVM Settings)] で ESX ホストのデータストアを指定してから、ホストをクラスタに追加する必要があります。vSphere API/SDK のドキュメントを参照してください。

- 8 管理インターフェイスをホストする分散仮想ポート グループを選択します。このポート グループには NSX Manager のポート グループへのアクセスが必要です。

データストアが [ホスト上が指定済み (Specified on host)] に設定されている場合、使用するネットワークは、クラスタの各ホストの [agentVmNetwork] プロパティで指定されている必要があります。vSphere API/SDK のドキュメントを参照してください。

クラスタにホストを追加するときは、ホストの [agentVmNetwork] プロパティを設定してからクラスタにホストを追加する必要があります。

選択したポート グループは、選択したクラスタのすべてのホストで利用できる必要があります。

- 9 [IP 割り当て] で、次のいずれかを選択します。

選択	宛先
DHCP	DHCP (Dynamic Host Configuration Protocol) を使用して Data Security サービス仮想マシンに IP アドレスを割り当てます。
IP アドレス プール	選択された IP プールから、Data Security サービス仮想マシンに IP アドレスを割り当てます。

固定 IP アドレスはサポートされていないことに注意してください。

- 10 [次へ (Next)] をクリックし、[設定内容の確認] ページで [終了 (Finish)] をクリックします。
- 11 [インストール ステータス (Installation Status)] 列に [成功 (Succeeded)] と表示されるまで、デプロイを監視します。
- 12 [インストール ステータス (Installation Status)] 列に [失敗 (Failed)] と表示された場合は、[失敗] の横にあるアイコンをクリックします。すべてのデプロイ エラーが表示されます。[解決法 (Resolve)] をクリックしてエラーを修正します。エラーを解決すると、別のエラーが表示されることがあります。必要な操作を行い、再度 [解決法 (Resolve)] をクリックします。

NSX コンポーネントのアンインストール

23

この章では、vCenter 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 アプライアンスを 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] 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 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](#)
- [NSX インストールの安全な削除](#)

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

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

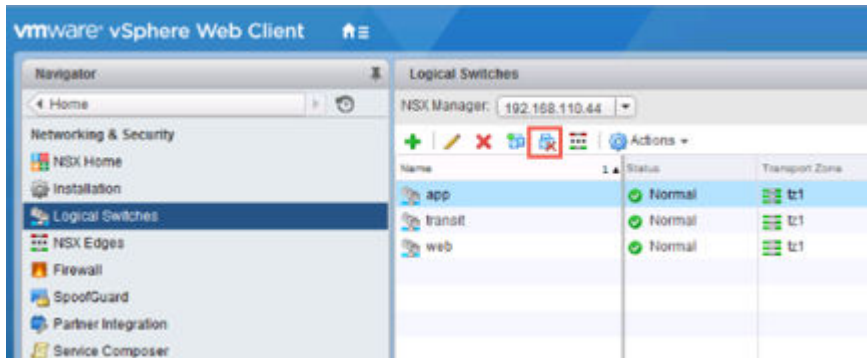
論理スイッチは vSphere Web Client を使用してアンインストールできます。

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 で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [論理スイッチ (Logical Switches)] の順に移動します。
- 2 論理スイッチを選択し、[仮想マシンの削除] アイコンをクリックして、接続されている仮想マシンを削除します。次はその例です。



- 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。

NSX インストールの安全な削除

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、論理ルーター、NSX ファイアウォール、および vCenter 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。クラスタからのネットワーク仮想化コンポーネントのアンインストールは、vCenter Server から NSX プラグインを削除する前に行うことをお勧めします。

NSX を完全に削除するには、ホストを 2 回再起動する必要があります。1 回目の再起動は、NSX VIB をアンインストールした後に必要です。2 回目の再起動は、ホスト VTEP、および VTEP で使用されている dvPortgroup を削除した後に必要です。

注: NSX アプライアンスを 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] タブから行ってください。

NSX を個々のホストから（クラスタ全体からではなく）削除する場合は、[章 12 「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

- 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 Endpoint 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спорт 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。

手順

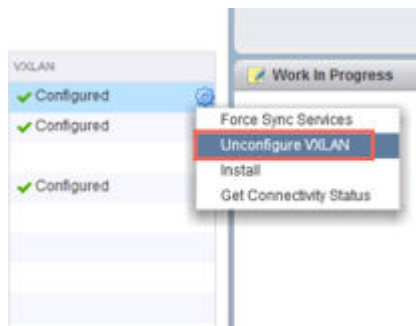
- 1 トランスポート ゾーンからクラスタを削除します。

[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 コントローラ 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 トランスポート ゾーンを削除します。
- 3 クラスタの VXLAN の設定を解除します。

次はその例です。

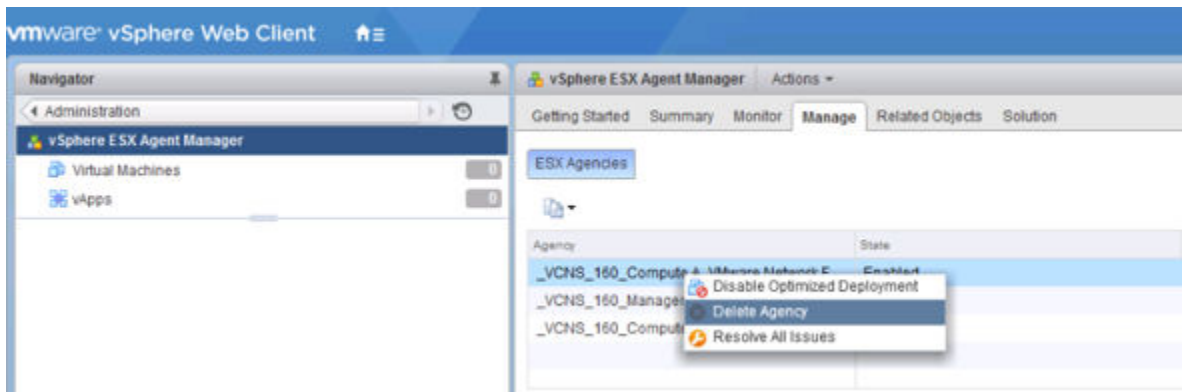


- 4 NSX VIB をアンインストールして、ホストの準備を取り消します。

次のいずれかの方法を選択して、NSX VIB をアンインストールします。最初の 2 つの方法では、クラスタ内のすべてのホストから NSX VIB がアンインストールされます。後の 2 つの方法では、1 度に 1 つのホストから VIB がアンインストールされます。

- vSphere Web Client で [Networking and Security (Networking & Security)] > [インストール (Installation)] > [ホストの準備 (Host Preparation)] の順に移動して、[アンインストール (Uninstall)] をクリックします。
- vSphere Web Client で [管理 (Administration)] > [vCenter Server の拡張機能 (vCenter Server Extensions)] > [vSphere ESX Agent Manager] に移動します。[管理 (Management)] タブで vCNS エージェントを右クリックして、[エージェントの削除 (Delete Agency)] を選択します。

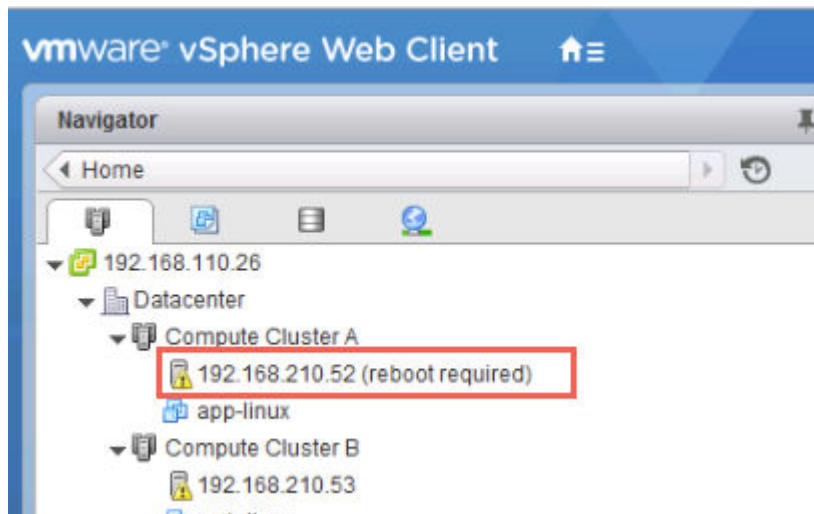
次はその例です。



- 準備済みのクラスタから準備されていないクラスタにホストを移動します。
- ホストで、次のコマンドを実行します。
 - `esxcli software vib remove --vibName=esx-vxlan`
 - `esxcli software vib remove --vibName=esx-vsip`

5 ホストを再起動します。

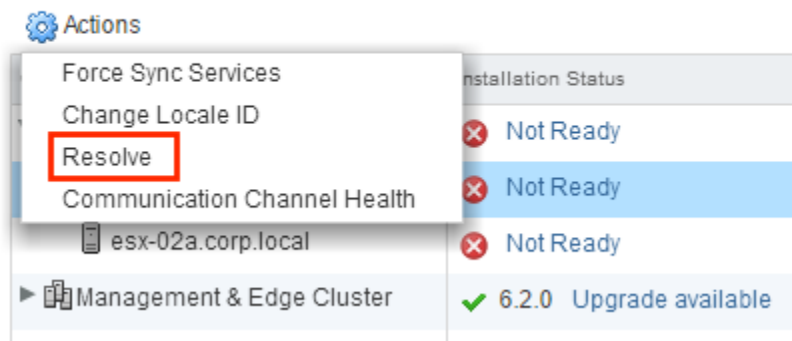
ホストから VIB を削除するには、ホストを再起動する必要があります。必要な再起動は、自動的に行われません。ホストの再起動が必要である場合は、[ホストおよびクラスタ] ビューに [(再起動が必要です) ((reboot required))] タグが表示されます。次はその例です。



以下のいずれかの手順を使用して、ホストを再起動します。

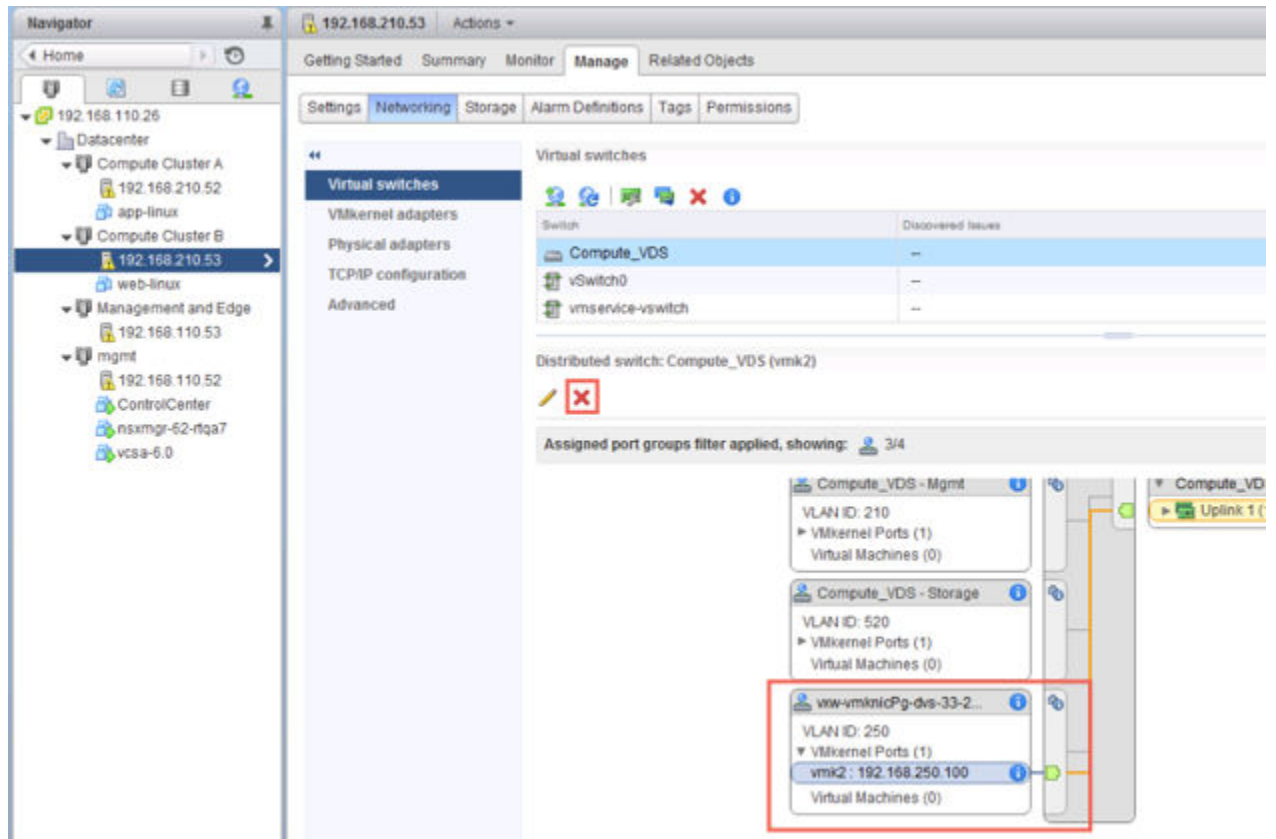
- ホストを手動で再起動します。
- クラスタを選択して、[解決 (Resolve)] アクションをクリックします。このアクションにより、クラスタ内のすべてのホストが再起動されます。クラスタで DRS が有効になっている場合は、DRS は、仮想マシンの動作を停止しない制御された方法で、ホストの再起動を試みます。何らかの理由で DRS の操作が失敗した場合、[解決 (Resolve)] アクションは停止します。この場合、仮想マシンを手動で移動して、[解決 (Resolve)] アクションをもう一度実行するか、ホストを手動で再起動する必要があります。

NSX Component Installation on Hosts



- 6 NSX Manager アプライアンス、およびすべての NSX コントローラ アプライアンス仮想マシンをディスクから削除します。
- 7 残りの VTEP VMkernel インターフェイスを削除します。

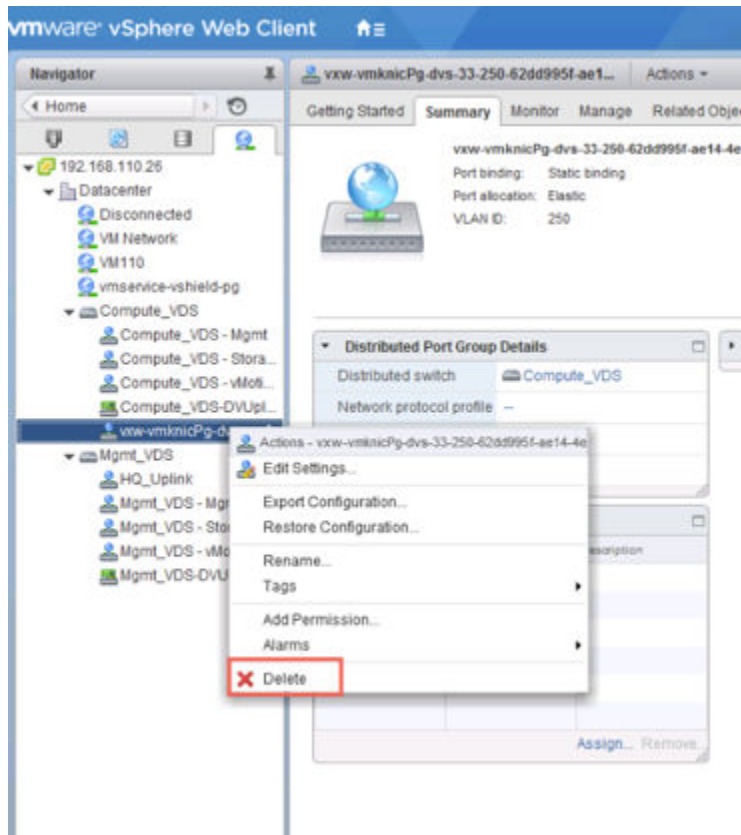
次はその例です。



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。

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

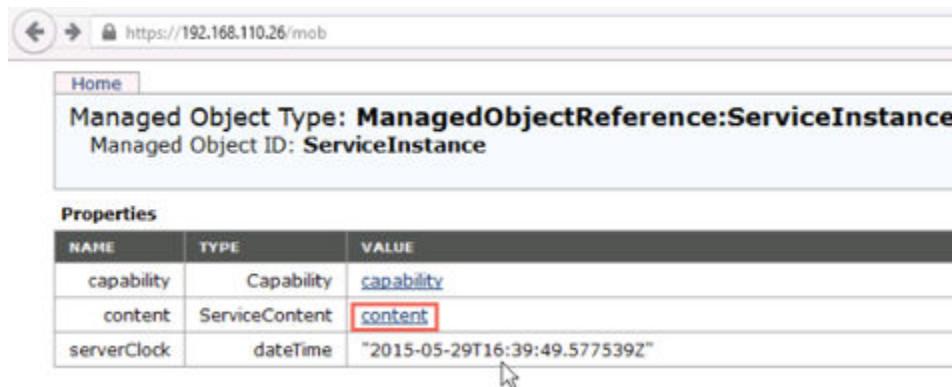
次はその例です。



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。

- 9 ホストを再起動します。
- 10 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。
- 11 **[Content]** をクリックします。

次はその例です。



12 [ExtensionManager] をクリックします。

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	DVSwitchManager
eventManager	ManagedObjectReference:EventManager	EventManager
extensionManager	ManagedObjectReference:ExtensionManager	ExtensionManager
fileManager	ManagedObjectReference:FileManager	FileManager
guestOperationsManager	ManagedObjectReference:GuestOperationsManager	guestOperationsManager
hostProfileManager	ManagedObjectReference:HostProfileManager	HostProfileManager

13 [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

- 14 文字列 [com.vmware.vShieldManager] を入力して、[メソッドの起動 (Invoke Method)] をクリックします。

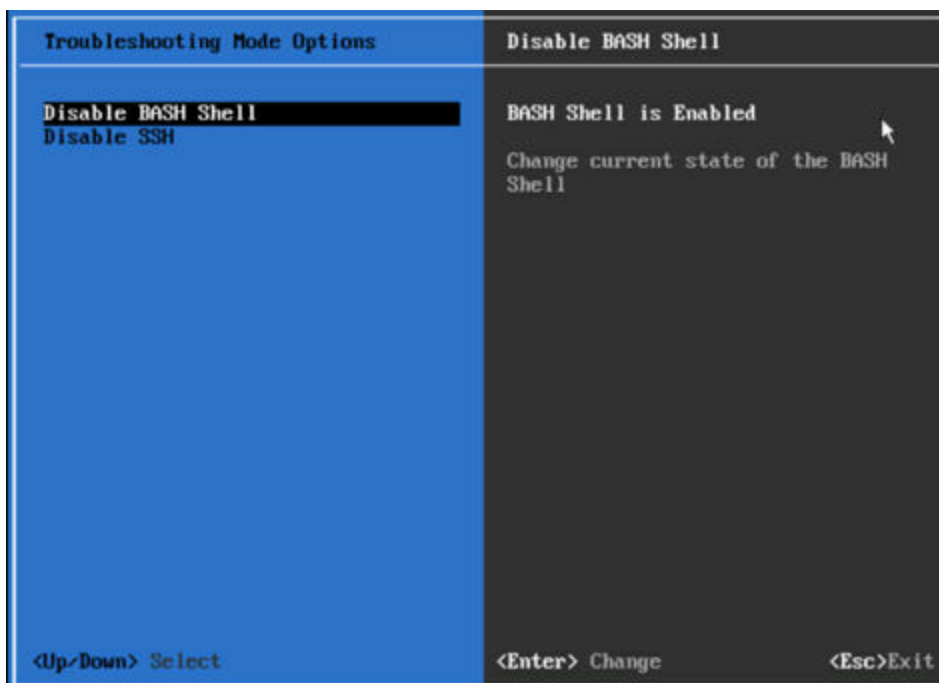
Managed Object Type:
ManagedObjectReference:ExtensionManager
 Managed Object ID: **ExtensionManager**
 Method: **UnregisterExtension**

void UnregisterExtension

Parameters

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

- 15 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。



BASH シェルを有効にする別の方法として、root としてログインし、[shell.set --enabled true] コマンドを実行します。

- 16 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\

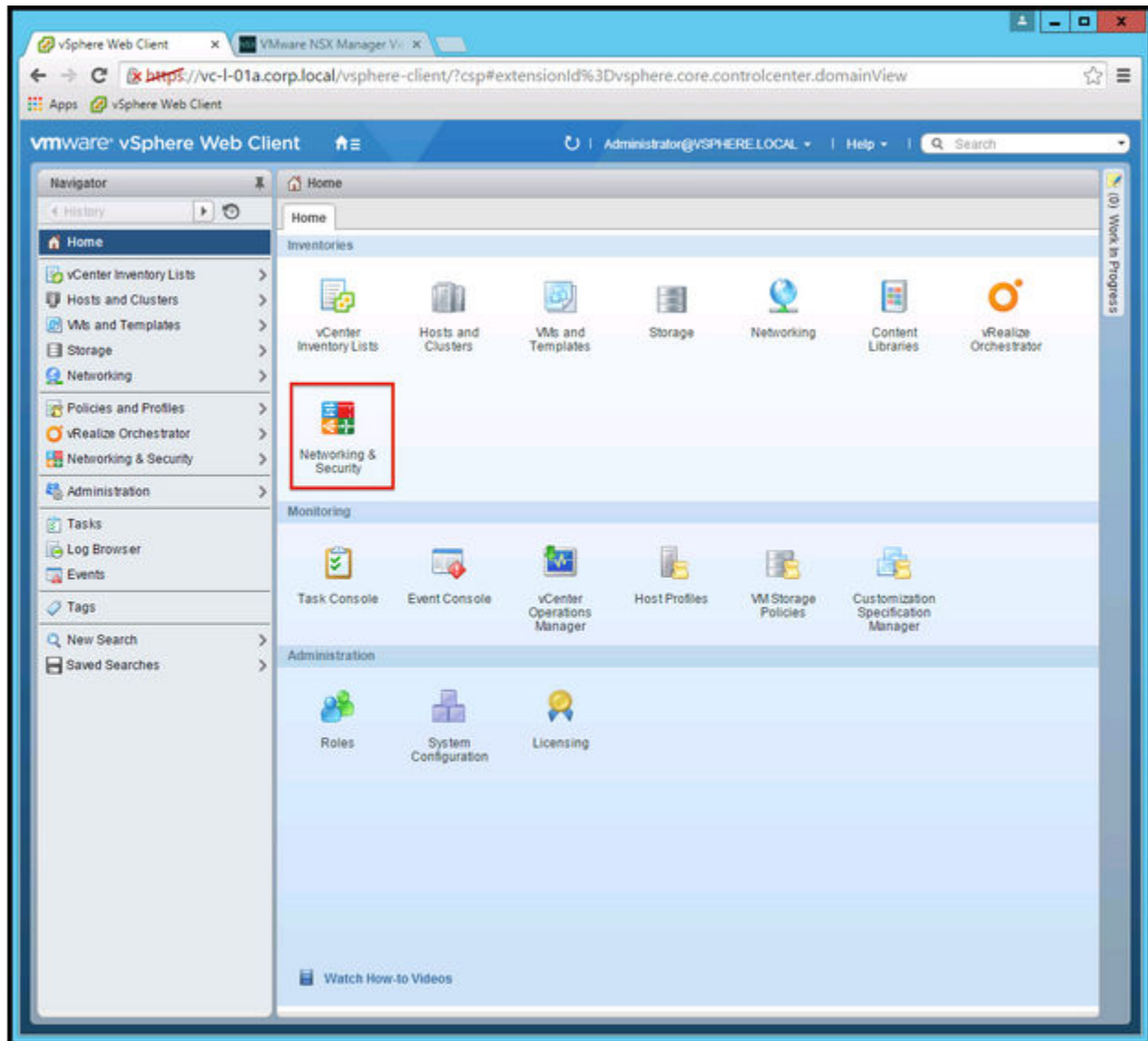
- Windows 2008/2012 – %ALLUSERSPROFILE%\VMware\vsphere Web Client\vc-packages\vsphere-client-serenity\
 - VMware vCenter Server Appliance – /var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
- vCenter Server 6.0.x
 - Windows 2008/2012 – C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\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

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] > [クライアント プラグイン (Administration > 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。

