

NSX-T Data Center インストール ガイド

変更日 : 2021 年 8 月 12 日
VMware NSX-T Data Center 2.5

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

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

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

Copyright © 2020 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

NSX-T Data Center インストール ガイド 8

1 NSX-T Data Center の概要 9

用語の説明 10

NSX Manager の概要 13

2 NSX-T Data Center インストールのワークフロー 16

vSphere の NSX-T Data Center ワークフロー 16

KVM の NSX-T Data Center インストール ワークフロー 17

ベア メタル サーバの NSX-T Data Center 構成ワークフロー 18

3 インストールの準備 19

システム要件 19

NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件 19

NSX Edge 仮想マシンのシステム要件 23

NSX Edge ベア メタル要件 24

ベア メタル サーバ システムの要件 27

ベア メタル Linux コンテナの要件 27

ポートとプロトコル 28

NSX Manager が使用する TCP および UDP ポート 28

NSX Edge が使用する TCP および UDP ポート 30

ESXi、KVM ホスト、ベアメタル サーバで使用する TCP および UDP ポート 31

4 NSX Manager のインストール 33

デフォルトの管理者パスワードの有効期限の変更 37

5 NSX-T Data Center の vSphere へのインストール 39

NSX Manager および利用可能なアプライアンスのインストール 39

コマンドライン OVF ツールを使用した ESXi への NSX Manager のインストール 43

起動時に GRUB メニューを表示するための NSX-T Data Center の設定 48

新しく作成された NSX Manager にログインする 49

コンピュータ マネージャの追加 49

クラスタを構成する NSX Manager ノードをユーザー インターフェイスから展開 52

クラスタの仮想 IP (VIP) アドレスの設定 58

NSX-T アプライアンスでのスナップショットの無効化 59

6 KVM への NSX-T Data Center のインストール 61

KVM のセットアップ 61

KVM CLI を使用したゲスト仮想マシンの管理	64
KVM への NSX Manager のインストール	65
新しく作成された NSX Manager にログインする	69
KVM ホストへのサードパーティ製パッケージのインストール	69
RHEL KVM ホストの Open vSwitch のバージョンを確認する	71
SUSE KVM ホストの Open vSwitch バージョンの確認	72
クラスタを構成する NSX Manager ノードを CLI を使用して展開	73

7 ベア メタル サーバが NSX-T Data Center を使用するように構成 75

ベア メタル サーバへのサードパーティ製パッケージのインストール	75
ベアメタル サーバ ワークロードのアプリケーション インターフェイスの作成	77

8 NSX Manager クラスタの要件 79

単一サイト、デュアル サイト、複数サイトに対する NSX Manager クラスタの要件	79
--	----

9 NSX Edge のインストール 83

NSX Edge のインストール要件	83
NSX Edge のネットワーク設定	85
NSX Edge のインストール方法	91
NSX Edge トランSPORT ノードの作成	93
NSX Edge クラスタの作成	97
vSphere の GUI を使用した ESXi への NSX Edge のインストール	98
コマンドライン OVF ツールを使用した ESXi への NSX Edge のインストール	102
ISO ファイルを使用した仮想アプライアンスとしての NSX Edge のインストール	106
ベア メタルへの NSX Edge のインストール	110
NSX Edge 用の PXE サーバの準備	110
ISO ファイルを使用した NSX Edge の自動インストール	115
ISO ファイルを使用した NSX Edge のインタラクティブ インストール	118
NSX Edge の管理プレーンへの追加	120
トランSPORT ノードとしての NSX Edge の設定	122

10 トランSPORT ゾーンとトランSPORT ノード 124

トランSPORT ゾーンの作成	124
トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成	126
拡張データ パス	128
プロファイルの設定	131
アップリンク プロファイルの作成	132
Network I/O Control プロファイルの設定	134
NSX Edge クラスタ プロファイルの追加	144
NSX Edge ブリッジ プロファイルの追加	144
トランSPORT ノード プロファイルの追加	145

VMkernel の N-VDS スイッチへの移行	149
VMkernel の移行エラー	154
スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成	157
管理対象ホストのトランスポート ノードの構成	165
リンク集約による ESXi ホスト トランスポート ノードの設定	170
トランスポート ノードの状態の確認	171
ESXi の VMkernel アダプタおよび物理アダプタの移行	173
NSX メンテナンス モード	174
N-VDS の可視表示	175
VLAN ID 範囲と MTU 設定の健全性チェック	176
双方向フォワーディング検出の状態の表示	179
NSX-T Data Center カーネル モジュールの手動インストール	180
ESXi ハイパーバイザーへの NSX-T Data Center カーネル モジュールの手動インストール	180
Ubuntu KVM ハイパーバイザーへの NSX-T Data Center ソフトウェア パッケージの手動インストール	183
RHEL および CentOS KVM ハイパーバイザーへの NSX-T Data Center ソフトウェア パッケージの手動インストール	185
SUSE KVM ハイパーバイザーへの NSX-T Data Center ソフトウェア パッケージの手動インストール	186
最小の vSphere クラスタ NSX-T の展開	187

11 NSX-T とホスト プロファイルの統合 199

Auto Deploy ステートレス クラスタ	199
ステートレス クラスタの Auto Deploy タスクの概要	199
前提条件とサポートされるバージョン	200
ステートレス ホスト用のカスタム イメージ プロファイルの作成	201
リファレンス ホストまたはターゲット ホストとカスタム イメージの関連付け	202
リファレンス ホストでのネットワークの構成	203
NSX-T でのトランスポート ノードとしてのリファレンス ホストの設定	204
ホスト プロファイルの抽出と確認	207
ステートレス クラスタとホスト プロファイルの関連付けの確認	208
ホストのカスタマイズの更新	208
ターゲット ホストでの自動展開のトリガ	210
ホスト プロファイルとトランスポート ノード プロファイルのトラブルシューティング	218
ステートフル サーバ	220
サポートされる NSX-T と ESXi のバージョン	221
ステートフル ターゲット クラスタの準備	221
ホスト プロファイルを適用する VMkernel の移行	222
ホスト プロファイルを適用しない VMkernel の移行	224

12 ホスト トランスポート ノードからの NSX-T Data Center のアンインストール 225

アンインストールのためのホスト ネットワーク マッピングの確認	225
---------------------------------	-----

vSphere クラスタからの NSX-T Data Center のアンインストール	227
vSphere クラスタ内のホストからの NSX-T Data Center のアンインストール	229
スタンドアローン ホストからの NSX-T Data Center のアンインストール	230

13 NSX Cloud コンポーネントのインストール 232

NSX Cloud のアーキテクチャとコンポーネント	232
NSX Cloud の展開の概要	234
NSX-T Data Center オンプレミス コンポーネントの展開	234
CSM のインストール	234
NSX Manager への CSM の追加	235
ポートとプロトコルへのアクセスの有効化	235
(オプション) プロキシ サーバの設定	236
(オプション) Cloud Service Manager の vIDM の設定	237
パブリック クラウド アカウントの追加	238
Microsoft Azure ネットワークとオンプレミス NSX-T Data Center 環境の接続	238
Amazon Web Services (AWS) ネットワークとオンプレミス NSX-T Data Center 環境の接続	245
NSX Public Cloud Gateway の展開	250
VNet での PCG の展開	253
VPC での PCG の展開	254
トランジット VPC または VNet へのリンク	257
自動作成された論理エンティティとクラウド ネイティブのセキュリティ グループ	258
(オプション) ワークロード仮想マシンへの NSX Tools のインストール	264
PCG の展開解除またはリンク解除	264
パブリック クラウドの nsx.network タグの削除	265
検疫ポリシーの無効化とフォールバック セキュリティ グループの指定	265
ユーザー作成の論理エンティティの削除	266
CSM からの [展開解除またはリンク解除]	266
PCG の展開解除のトラブルシューティング	267

14 NSX Intelligence のインストールと構成 268

NSX Intelligence のインストールと構成のワークフロー	269
NSX Intelligence のインストールの準備	269
NSX Intelligence のシステム要件	270
NSX Intelligence が使用する TCP および UDP ポート	271
NSX Intelligence インストーラ バンドルのダウンロードと解凍	272
NSX Intelligence アプライアンスのインストール	274
NSX Intelligence アプライアンスのインストールで発生した問題のトラブルシューティング	276
認証情報が無効か、指定したアカウントがロックされている	276
アプライアンスの展開に失敗した状態がクリアされない	277
NSX Intelligence アプライアンスのアンインストール	277

15 インストール問題のトラブルシューティング 279

ESXi ホスト上の bootbank の容量が不足しているためインストールが失敗する 279

NSX-T Data Center インストール ガイド

『NSX-T Data Center インストール ガイド』では、VMware NSX-T™ Data Center 製品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

この情報は、NSX-T Data Center 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。システム管理者としての経験があり、仮想マシン テクノロジーとネットワーク仮想化の概念に詳しい方を対象にしています。

技術ドキュメントの用語集

VMware は、新しい用語を集めた用語集を提供しています。VMware の技術ドキュメントで使用されている用語の定義については、<https://www.vmware.com/topics/glossary> を参照してください。

NSX-T Data Center の概要

1

サーバ仮想化ではプログラムによって、仮想マシンの作成および管理を行います。NSX-T Data Center のネットワーク仮想化は、同じような方法で、ソフトウェア ベースの仮想ネットワークの作成および管理を行います。

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同等の機能によって、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（スイッチング、ルーティング、アクセス コントロール、ファイアウォール、QoS 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。

NSX-T Data Center は、管理プレーン、制御プレーン、およびデータ プレーンの 3 つのプレーンを実装することで機能します。それぞれ独立し、相互に連携する 3 つのプレーンは、NSX Manager およびトランスポート ノードの 2 種類のノードに、プロセス、モジュール、およびエージェントのセットとして実装されます。

- すべてのノードで管理プレーン エージェントをホストします。
- NSX Manager ノードは、API サービスと、管理プレーンのクラスタ デーモンをホストします。
- NSX Controller ノードは、統合制御プレーンのクラスタ デーモンをホストします。
- トランスポート ノードは、ローカル制御プレーンのデーモンと転送エンジンをホストします。

NSX Manager は、ノードのクラスタに Policy Manager、管理、統合制御サービスをマージする 3 ノードによるクラスタリングをサポートします。NSX Manager クラスタリングでは、ユーザー インターフェイスと API による高可用性が提供されます。管理プレーン ノードと制御プレーン ノードのコンバージェンスにより、NSX-T Data Center 管理者による展開と管理が必要な仮想アプライアンスの数は削減されています。

NSX Manager アプライアンスは、異なる展開シナリオに対し、3 種類のサイズで使用可能です。ラボまたは POC（事前検証）展開環境向けには、Small アプライアンスを利用できます。さらに、最大 64 台のホストから成る Medium アプライアンスと、大規模な環境に展開するお客様向けの Large アプライアンスが利用可能です。[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件と構成の上限ツール](#)を参照してください。

この章には、次のトピックが含まれています。

- [用語の説明](#)
- [NSX Manager の概要](#)

用語の説明

このドキュメントとユーザー インターフェイスで使用されている NSX-T Data Center の一般的な用語について説明します。

コンピュータ マネージャ

コンピュータ マネージャは、ホストや仮想マシンなどのリソースを管理するアプリケーションです。例：vCenter Server。

制御プレーン

管理プレーンからの設定に基づいてランタイム状態を算出します。制御プレーンは、データ プレーン要素からもたらされたトポロジ情報を伝達し、ステートレス設定をフォワーディング エンジンにプッシュします。

データ プレーン

制御プレーンが設定したテーブルに基づいて、パケットのステートレスな転送または変換を行います。データ プレーンはトポロジ情報を制御プレーンに報告し、パケット レベルの統計情報を保持します。

外部ネットワーク

NSX-T Data Center の管理対象ではない物理ネットワークまたは VLAN です。NSX Edge を通じて、論理ネットワークまたはオーバーレイ ネットワークを外部ネットワークにリンクできます。例として、お客様のデータセンター内の物理ネットワークや、物理環境内の VLAN などが挙げられます。

論理ポート出力

仮想マシンまたは論理ネットワークから送信される送信ネットワーク トラフィックは、トラフィックが仮想ネットワークから出てデータセンターに入るため、出力方向と呼ばれます。

論理ポート入力

データセンターから出て仮想マシンに入る受信ネットワーク トラフィックは入力方向のトラフィックと呼ばれます。

論理ルーター

NSX-T Data Center のルーティング エンティティです。

論理ルーター ポート

論理スイッチ ポート、または物理ネットワークへのアップリンク ポートを関連付けることができる論理ネットワーク ポートです。

論理スイッチ

仮想マシン インターフェイスとゲートウェイ インターフェイスに仮想レイヤー 2 スイッチングを提供するエンティティです。論理スイッチは、物理レイヤー 2 スイッチに対応する論理スイッチをテナント ネットワークの管理者に提供し、管理者が複数の仮想マシンを共通のブロードキャスト ドメインに接続できるようにします。論理スイッチは、物理ハイパーバイザー インフラストラクチャから独立した、多数のハイパーバイザーにまたがる論理エンティティであり、物理的な配置場所仮想マシンを接続します。

マルチテナントのクラウドでは、各レイヤー 2 セグメントを相互に分離した状態で、多数の論理スイッチを同じハイパーバイザー ハードウェアに並べて配置できます。論理スイッチは論理ルーターを使用して接続でき、論理ルーターは外部物理ネットワークに接続したアップリンク ポートを提供できます。

論理スイッチ ポート

仮想マシン ネットワーク インターフェイスまたは論理ルーター インターフェイスへの接続を確立する、論理スイッチの接続ポイントです。論理スイッチ ポートは、適用されているスイッチング プロファイル、ポートの状態、リンクのステータスをレポートします。

管理プレーン

システムへの単一の API エントリ ポイントで、ユーザー設定の維持とユーザー クエリの処理、システム内の管理プレーン、制御プレーン、データ プレーンのすべてのノードの処理を行います。管理プレーンは、ユーザー設定のクエリ、変更、維持を行います。

NSX Edge クラスタ

高可用性の監視にプロトコルと同じ設定を持つ NSX Edge ノード アプライアンスの集合。

NSX Edge ノード

IP ルーティングと IP サービスの機能に処理能力を提供することを機能的目標とするコンポーネント。

NSX 管理対象の分散仮想スイッチまたは KVM Open vSwitch

NSX の管理対象の分散仮想スイッチ（以前はホスト スイッチと呼ばれていた N-VDS）または OVS は、共有 NSX Edge とコンピュート クラスタに使用されます。N-VDS は、オーバーレイ トラフィック構成では必須です。

N-VDS には標準と拡張データパスの 2 つのモードがあります。拡張データパスの N-VDS には、NFV (Network Functions Virtualization) ワークロードをサポートするパフォーマンス機能があります。

NSX Manager

API サービス、管理プレーン、エージェント サービスをホストするノードです。NSX Manager は、NSX-T Data Center インストール パッケージに含まれているアプライアンスです。NSX Manager または `nsx-cloud-service-manager` のロールでアプライアンスを展開できます。現在、アプライアンスが一度にサポートできるロール数は 1 つのみです。

NSX Manager クラスタ

高可用性を提供できる NSX Manager のクラスタです。

Open vSwitch (OVS)

XenServer、Xen、KVM、およびその他の Linux ベースのハイパーバイザーで仮想スイッチとして機能するオープン ソース ソフトウェア スイッチです。

オーバーレイ論理ネットワーク

仮想マシンで認識されるトポロジが物理ネットワークのトポロジから切り離されるように、レイヤー 3 内のレイヤー 2 を使用して実装された論理ネットワークです。

物理インターフェイス (pNIC)

ハイパーバイザーがインストールされている物理サーバ上のネットワーク インターフェイスです。

セグメント

仮想マシン インターフェイスとゲートウェイ インターフェイスに仮想レイヤー 2 スwitchングを提供するエンティティです。セグメントは、物理レイヤー 2 スwitchに対応する論理スイッチをテナント ネットワークの管理者に提供し、管理者が複数の仮想マシンを共通のブロードキャスト ドメインに接続できるようにします。セグメントは、物理ハイパーバイザー インフラストラクチャに依存せず、多数のハイパーバイザーにまたがる論理エンティティであり、物理的な場所を問わずに仮想マシンを接続します。セグメントは、論理スイッチとも呼ばれます。

マルチテナントのクラウドでは、各レイヤー 2 セグメントを相互に分離した状態で、多数のセグメントを同じハイパーバイザー ハードウェアに並べて配置できます。セグメントには、外部の物理ネットワークへの接続を提供できるゲートウェイを使用して接続できます。

Tier-0 ゲートウェイまたは Tier-0 論理ルーター

[ネットワークとセキュリティの詳細設定] タブで、Tier-0 ゲートウェイは Tier-0 論理ルーターと表示されます。物理ネットワークとのインターフェイスとして機能し、アクティブ/アクティブまたはアクティブ/スタンバイ構成のクラスタとして認識されます。Tier-0 ゲートウェイは BGP を実行し、物理ルーターとピアリングされます。アクティブ/スタンバイ モードでは、ゲートウェイがステートフル サービスを提供することもできます。

Tier-1 ゲートウェイまたは Tier-1 論理ルーター

[ネットワークとセキュリティの詳細設定] タブで、Tier-1 ゲートウェイは Tier-1 論理ルーターと表示されます。North バウンド接続用に 1 台の Tier-0 ゲートウェイと接続し、South バウンド接続用に 1 つ以上のオーバーレイ ネットワークと接続します。Tier-1 ゲートウェイは、ステートフル サービスを提供するアクティブ/スタンバイ クラスタにすることができます。

トランスポート ゾーン

論理スイッチの最大範囲を定義するトランスポート ノードの集合。トランスポート ゾーンは、同じようにプロビジョニングされた一連のハイパーバイザーと、これらのハイパーバイザー上の仮想マシンを接続する論理スイッチを表します。NSX-T Data Center の管理プレーンに登録され、NSX-T Data Center モジュールがインストールされているホストです。ハイパーバイザー ホストまたは NSX Edge を NSX-T Data Center のオーバーレイの一部にするためには、NSX-T Data Center のトランスポート ゾーンに追加する必要があります。

トランスポート ノード

NSX-T Data Center オーバーレイまたは NSX-T Data Center VLAN ネットワークに参加できるノード。KVM ホストの場合は、N-VDS を事前に設定できます。また、NSX Manager で設定を実行することも可能です。ESXi ホストの場合は、常に NSX Manager で N-VDS が設定されます。

アップリンク プロファイル

ハイパーバイザー ホストから NSX-T Data Center 論理スイッチまたは NSX Edge ノードからトップオブラック スwitchへのリンクのポリシーを定義します。アップリンク プロファイルでは、チーミング ポリシー、アクティブ/スタンバイ リンク、トランスポート VLAN ID、MTU 設定などを定義します。アップリンク プロ

ファイルに設定されたトランスポート VLAN がオーバーレイ トラフィックにのみタグ付けし、VLAN ID が TEП エンドポイントによって使用されます。

仮想マシン インターフェイス (vNIC)

仮想ゲスト OS と標準の vSwitch または vSphere Distributed Switch 間の接続を提供する、仮想マシンのネットワーク インターフェイスです。vNIC は論理ポートに接続できます。vNIC は、固有の ID (UUID) で識別できます。

仮想トンネル エンドポイント

各ハイパーバイザーには、仮想トンネル エンドポイント (VTEP) があります。これは、VLAN ヘッダー内の仮想マシン トラフィックをカプセル化したり、パケットを宛先 VTEP にルーティングしてさらに処理をしたりするのに使用されます。トラフィックは、物理ネットワークにアクセスする別のホストまたは NSX Edge ゲートウェイ上の別の VTEP にルーティングすることができます。

NSX Manager の概要

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

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

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

ポリシー インターフェイスと詳細設定インターフェイスの使用する条件

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

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

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


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

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

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

ポリシー インターフェイスの使用

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

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

ポリシー インターフェイスと詳細設定インターフェイスの場所

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

表 1-2. ポリシー インターフェイスと詳細設定インターフェイス

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

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

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

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

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

表 1-3. オブジェクト名

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

NSX-T Data Center インストールの ワークフロー

2

vSphere または KVM ホストに NSX-T Data Center をインストールできます。また、NSX-T Data Center を使用するベア メタル サーバを設定することもできます。

ハイパーバイザーまたはベア メタルをインストールまたは設定するには、ワークフローの推奨タスクを実行してください。

この章には、次のトピックが含まれています。

- [vSphere の NSX-T Data Center ワークフロー](#)
- [KVM の NSX-T Data Center インストール ワークフロー](#)
- [ベア メタル サーバの NSX-T Data Center 構成ワークフロー](#)

vSphere の NSX-T Data Center ワークフロー

チェックリストを使用して、vSphere ホストへのインストールの進行状況を追跡します。

推奨される手順は次のとおりです。

- 1 NSX Manager のインストール要件を確認します。[4 章 NSX Manager のインストール](#) を参照してください。
- 2 必要なポートおよびプロトコルを構成します。[ポートとプロトコル](#) を参照してください。
- 3 NSX Manager をインストールします。[NSX Manager および利用可能なアプライアンスのインストール](#) を参照してください。
- 4 新しく作成された NSX Manager にログインします。[新しく作成された NSX Manager にログインする](#) を参照してください。
- 5 コンピュート マネージャを設定します。[コンピュート マネージャの追加](#) を参照してください。
- 6 追加の NSX Manager ノードを展開して、クラスタを構成します。[クラスタを構成する NSX Manager ノードをユーザー インターフェイスから展開](#) を参照してください。
- 7 NSX Edge のインストール要件を確認します。[NSX Edge のインストール要件](#) を参照してください。
- 8 NSX Edge をインストールします。[vSphere の GUI を使用した ESXi への NSX Edge のインストール](#) を参照してください。
- 9 NSX Edge クラスタを作成します。[NSX Edge クラスタの作成](#) を参照してください。
- 10 トランスポート ゾーンを作成します。[トランスポート ゾーン](#) の作成 を参照してください。

- 11 ホスト トランスポート ノードを作成します。 [スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#)または[管理対象ホストのトランスポート ノードの構成](#)を参照してください。

各ホストで仮想スイッチが作成されます。管理プレーンからホストの証明書が制御プレーンに送信され、管理プレーンによって制御プレーンの情報がホストにプッシュされます。各ホストは、証明書を提示して SSL 経由で制御プレーンに接続します。制御プレーンは、管理プレーンから提供されたホスト証明書に基づいて証明書を検証します。検証が正常に完了すると、コントローラが接続を許可します。

インストール後

ホストがトランスポート ノードの場合、NSX Manager のユーザー インターフェイスまたは API を使用して、トランスポート ゾーン、論理スイッチ、論理ルーター、その他のネットワーク コンポーネントをいつでも作成できます。NSX Edge とホストを管理プレーンに追加するときに、NSX-T Data Center の論理エンティティと設定状態が自動的に NSX Edge とホストにプッシュされます。

詳細については、『NSX-T Data Center 管理ガイド』を参照してください。

KVM の NSX-T Data Center インストール ワークフロー

チェックリストを使用して、KVM ホストへのインストールの進行状況を追跡します。

推奨される手順は次のとおりです。

- 1 KVM 環境を準備します。 [KVM のセットアップ](#) を参照してください。
- 2 NSX Manager のインストール要件を確認します。 [4 章 NSX Manager のインストール](#) を参照してください。
- 3 必要なポートおよびプロトコルを構成します。 [ポートとプロトコル](#) を参照してください。
- 4 NSX Manager をインストールします。 [KVM への NSX Manager のインストール](#) を参照してください。
- 5 新しく作成された NSX Manager にログインします。 [新しく作成された NSX Manager にログインする](#) を参照してください。
- 6 KVM ホストにサードパーティ製パッケージを構成します。 [KVM ホストへのサードパーティ製パッケージのインストール](#) を参照してください。
- 7 追加の NSX Manager ノードを展開して、クラスタを構成します。 [クラスタを構成する NSX Manager ノードを CLI を使用して展開](#) を参照してください。
- 8 NSX Edge のインストール要件を確認します。 [NSX Edge のインストール要件](#) を参照してください。
- 9 NSX Edge をインストールします。 [ベア メタルへの NSX Edge のインストール](#) を参照してください。
- 10 NSX Edge クラスタを作成します。 [NSX Edge クラスタの作成](#) を参照してください。
- 11 トランスポート ゾーンを作成します。 [トランスポート ゾーンの作成](#) を参照してください。
- 12 ホスト トランスポート ノードを作成します。 [スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

各ホストで仮想スイッチが作成されます。管理プレーンからホストの証明書が制御プレーンに送信され、管理プレーンによって制御プレーンの情報がホストにプッシュされます。各ホストは、証明書を提示して SSL 経由で制御プレーンに接続します。制御プレーンは、管理プレーンから提供されたホスト証明書に基づいて証明書を検証します。検証が正常に完了すると、コントローラが接続を許可します。

インストール後

ホストがトランスポート ノードの場合、NSX Manager のユーザー インターフェイスまたは API を使用して、トランスポート ゾーン、論理スイッチ、論理ルーター、その他のネットワーク コンポーネントをいつでも作成できます。NSX Edge とホストを管理プレーンに追加するときに、NSX-T Data Center の論理エンティティと設定状態が自動的に NSX Edge とホストにプッシュされます。

詳細については、『NSX-T Data Center 管理ガイド』を参照してください。

ベア メタル サーバの NSX-T Data Center 構成ワークフロー

NSX-T Data Center を使用するベア メタル サーバを構成する際は、チェックリストを使用して進行状況を追跡します。

推奨される手順は次のとおりです。

- 1 ベア メタルの要件を確認します。[ベア メタル サーバ システムの要件](#) を参照してください。
- 2 必要なポートおよびプロトコルを構成します。[ポートとプロトコル](#) を参照してください。
- 3 NSX Manager をインストールします。[KVM への NSX Manager のインストール](#) を参照してください。
- 4 ベア メタル サーバ上のサードパーティ製パッケージを構成します。[ベア メタル サーバへのサードパーティ製パッケージのインストール](#) を参照してください。
- 5 ホスト トランスポート ノードを作成します。[スタンドアロン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

各ホストで仮想スイッチが作成されます。管理プレーンからホストの証明書が制御プレーンに送信され、管理プレーンによって制御プレーンの情報がホストにプッシュされます。各ホストは、証明書を提示して SSL 経由で制御プレーンに接続します。制御プレーンは、管理プレーンから提供されたホスト証明書に基づいて証明書を検証します。検証が正常に完了すると、コントローラが接続を許可します。

- 6 ベア メタル サーバ ワークロードにアプリケーション インターフェイスを作成します。[ベアメタル サーバ ワークロードのアプリケーション インターフェイスの作成](#) を参照してください。

インストールの準備

3

NSX-T Data Center をインストールする前に、導入環境の準備が完了していることを確認します。

この章には、次のトピックが含まれています。

- システム要件
- ポートとプロトコル

システム要件

NSX-T Data Center をインストールする前に、環境が特定のハードウェアおよびリソース要件を満たしている必要があります。

NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件

NSX Manager または他の NSX-T Data Center アプライアンスをインストールする前に、環境がサポートされている要件を満たしていることを確認します。

ホスト トランスポート ノードでサポートされているハイパーバイザー

ハイパーバイザー	バージョン	CPU コア	メモリ
vSphere	サポート対象の vSphere バージョン	4	16 GB
CentOS Linux KVM	7.4、7.5、7.6	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.6、7.5 および 7.4	4	16 GB
SUSE Linux Enterprise Server KVM	12 sp3、12 sp4	4	16 GB
Ubuntu KVM	16.04、18.04.2 LTS	4	16 GB

表 3-1. NSX Manager でサポートされているホスト

サポートの説明	ハイパーバイザー
ESXi	サポート対象のホストについては、 VMware 製品互換性マトリクス を参照してください。
KVM	RHEL 7.4 および Ubuntu 18.04.2 LTS 注： NSX-T Data Center 2.5 以降では、バージョン 18.04.2 LTS を実行する Ubuntu ホストを 16.04 からアップグレードするか、新規にインストールします。

ESXi ホストに対しては、NSX-T Data Center は vSphere 6.7 U1 以降でホスト プロファイルおよび Auto Deploy 機能をサポートします。詳細については、『VMware ESXi のインストールとセットアップ』の「vSphere Auto Deploy について」を参照してください。

注意： RHEL と Ubuntu で yum update コマンドを実行すると、カーネルのバージョンが更新されることがあります。バージョンが 4.14.x 以前でないと、NSX-T Data Center との互換性はなくなります。yum update を実行する場合は、カーネルの自動更新を無効にします。また、yum install を実行した後、NSX-T Data Center が該当のカーネルのバージョンをサポートしていることを確認します。

ハイパーバイザー ホストのネットワーク要件

使用する NIC カードは、NSX-T Data Center が実行されている ESXi のバージョンと互換性がある必要があります。サポートされている NIC カードについては、[VMware 互換性ガイド](#) を参照してください。

ヒント： 互換性ガイドで互換性のあるカードをすばやく識別するには、次の基準を適用します。

- [I/O デバイス タイプ] で、**ネットワーク** を選択します。
- サポートされている GENEVE カプセル化を使用するには、[機能] で、GENEVE オプションを選択します。
- 拡張データ バスを使用するには、**N-VDS 拡張データ バス** を選択します。

拡張データ バスの NIC ドライバ

[My VMware](#) 画面からサポート対象の NIC ドライバをダウンロードします。

NIC カード	NIC ドライバ
Intel 82599	ixgben 1.1.0.26-10EM.670.0.0.7535516
Intel(R) Ethernet Controller X710 for 10GbE SFP+	i40en 1.2.0.0-10EM.670.0.0.8169922
Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	

NSX Manager 仮想マシンのリソース要件

シン仮想ディスクのサイズは 3.8 GB、シック仮想ディスクのサイズは 200 GB です。

アプライアンスのサイズ	メモリ	vCPU	ディスク容量	仮想マシンのハードウェア バージョン
NSX Manager 極小規模	8 GB	2	200 GB	10 以降
NSX Manager の小規模な仮想マシン	16 GB	4	200 GB	10 以降
NSX Manager の中規模の仮想マシン	24 GB	6	200 GB	10 以降
NSX Manager の大規模な仮想マシン	48 GB	12	200 GB	10 以降

注： NSX Manager では、これまで個別のアプライアンスを必要としていた複数のロールを提供しています。これには、ポリシー ロール、管理プレーン ロール、中央制御プレーン ロールが含まれます。中央制御プレーン ロールは、これまで NSX Controller アプライアンスによって提供されていました。

- 極小規模な仮想マシンのリソース サイズは、Cloud Service Manager アプライアンス (CSM) にのみ使用できます。必要に応じて、極小規模以上の仮想マシン サイズに CSM を展開します。詳細については、[NSX Cloud の展開の概要](#)を参照してください。
- NSX Manager の小規模な仮想マシンのアプライアンス サイズは、ラボおよび POC（事前検証）の環境に適しています。本番環境では使用しないでください。
- NSX Manager の中規模の仮想マシンのアプライアンス サイズは、一般的な本番環境に適しています。このアプライアンス サイズを使用して構成された NSX-T 管理クラスタは、最大 64 のハイパーバイザーをサポートできます。
- NSX Manager の大規模な仮想マシンのアプライアンス サイズは、大規模な環境に適しています。このアプライアンス サイズを使用して構成された NSX-T 管理クラスタは、64 を超えるハイパーバイザーをサポートできます。

NSX Manager の大規模な仮想マシンのアプライアンス サイズを使用して最大のスケーリングを行う場合は、<https://configmax.vmware.com/guest> にある VMware Configuration Maximums ツールに移動し、製品リストから NSX-T Data Center を選択します。

言語サポート

NSX Manager は、英語、ドイツ語、フランス語、日本語、簡体字中国語、韓国語、繁体字中国語、スペイン語にローカライズされています。

NSX Manager のブラウザのサポート

NSX Manager には次のブラウザを使用することをおすすめします。

ブラウザ	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 76	○	○	○
Mozilla Firefox 68	○	○	○

ブラウザ	Windows 10	Mac OS X 10.13、10.14	Ubuntu 18.04
Microsoft Edge 44	○		
Apple Safari 12		○	

注：

- Internet Explorer はサポートされていません。
- サポートされるブラウザの最小解像度は、1280 × 800 ピクセルです。
- 言語サポート：NSX Manager は、英語、ドイツ語、フランス語、日本語、簡体字中国語、韓国語、繁体字中国語、スペイン語にローカライズされています。NSX Manager のローカライズではブラウザの言語設定が使用されるため、設定が目的の言語と一致することを確認してください。NSX Manager インターフェイス自体に言語プリファレンスはありません。

ネットワーク遅延の要件

NSX Manager クラスターの NSX Manager 間のネットワークの最大遅延は 10 ミリ秒です。

NSX Manager とトランスポート ノード間のネットワークの最大遅延は 150 ミリ秒未満です。

ストレージ要件

- ディスク アクセスの最大遅延は 10 ミリ秒未満です。
- NSX Manager は共有ストレージに配置することをおすすめします。
- ストレージ障害の発生ですべての NSX Manager のファイル システムが読み取り専用モードにならないように、ストレージを高可用性にする必要があります。

最適な高可用性ストレージ ソリューションを設計する方法については、ご使用のストレージ テクノロジーのドキュメントを参照してください。

NSX Edge 仮想マシンのシステム要件

NSX Edge をインストールする前に、環境がサポートされている要件を満たしていることを確認します。

注： NSX Edge ノードのホストには、次の条件が適用されます。

- NSX Edge ノードは、Intel ベースのチップセットを搭載した ESXi ベースのホストでのみサポートされます。
それ以外の場合に vSphere EVC モードを使用すると、NSX Edge ノードが起動せず、コンソールにエラーメッセージが表示されることがあります。
- NSX Edge 仮想マシンのホストで vSphere EVC モードが有効になっている場合、CPU は Haswell 以降の世代にする必要があります。
- NSX Edge 仮想マシンでは、VMXNET3 vNIC のみがサポートされます。

NSX Cloud の注 NSX Cloud を使用している場合、NSX Public Cloud Gateway(PCG) は、サポートされているパブリッククラウドごとに1つのデフォルトサイズで展開されます。詳細については、[NSX Public Cloud Gateway の展開](#) を参照してください。

NSX Edge 仮想マシンのリソース要件

アプライアンスのサイズ	メモリ	vCPU	ディスク容量	仮想マシンのハードウェアバージョン	注：
NSX Edge (小規模)	4 GB	2	200 GB	11 以降 (vSphere 6.0 以降)	NSX Edge の小規模な仮想マシンのアプライアンスサイズは、ラボおよび POC (事前検証) の環境に適しています。 注： 小規模の NSX Edge 仮想マシンを展開すると、Tier-1 ゲートウェイで L7 ルールが認識されません。
NSX Edge (中規模)	8 GB	4	200 GB	11 以降 (vSphere 6.0 以降)	NSX Edge Medium アプライアンスサイズは、一般的な本番環境に適しています。
NSX Edge (大規模)	32 GB	8	200 GB	11 以降 (vSphere 6.0 以降)	NSX Edge Large アプライアンスサイズは、ロードバランシングを行う環境に適しています。『NSX-T Data Center 管理ガイド』の ロードバランサ リソースの拡張 を参照してください。

NSX Edge 仮想マシンの CPU 要件

DPDK をサポートするには、基盤となるプラットフォームが次の要件を満たしている必要があります。

- CPU に AES-NI 機能が必要です。
- CPU に 1 GB Huge Page のサポートが必要です。

ハードウェア	タイプ
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx (Westmere-EX 以降の世代の CPU) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge 以降の世代の CPU) ■ Intel Xeon Platinum (すべての世代) ■ Intel Xeon Gold (すべての世代) ■ Intel Xeon Silver (すべての世代) ■ Intel Xeon Bronze (すべての世代)

NSX Edge ベア メタル要件

NSX Edge ベア メタルを構成する前に、環境がサポートされている要件を満たしていることを確認します。

NSX Edge ベア メタルのメモリ、CPU およびディスクの要件

最小要件

メモリ	CPU コア	ディスク容量
32 GB	8	200 GB

推奨要件

メモリ	CPU コア	ディスク容量
256 GB	24	200 GB

NSX Edge ベア メタルの DPDK CPU 要件

DPDK をサポートするには、基盤となるプラットフォームが次の要件を満たしている必要があります。

- CPU に AES-NI 機能が必要です。
- CPU に 1 GB Huge Page のサポートが必要です。

ハードウェア	タイプ
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx (Westmere-EX 以降の世代の CPU) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge 以降の世代の CPU) ■ Intel Xeon Platinum (すべての世代) ■ Intel Xeon Gold (すべての世代) ■ Intel Xeon Silver (すべての世代) ■ Intel Xeon Bronze (すべての世代)

NSX Edge ベア メタルのハードウェア要件

以下の URL で、ベア メタル NSX Edge ハードウェアがリストに含まれていることを確認します：<https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server>。ハードウェアがリストにない場合、ストレージ、ビデオ アダプタ、またはマザーボード コンポーネントは NSX Edge アプライアンス上で動作しません。

NSX Edge ベア メタルの NIC 要件

NIC タイプ	説明	PCI デバイス ID	ファームウェアのバージョン
Mellanox ConnectX-4 EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4	0x1013	12.21.1000 以降
Mellanox ConnectX-4 Lx EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4LX	0x1015	14.21.1000 以降
Mellanox ConnectX-5	PCI_DEVICE_ID_MELLANOX_CONNECTX5	0x1017	16.21.1000 以降
Mellanox ConnectX-5 EX	PCI_DEVICE_ID_MELLANOX_CONNECTX5EX	0x1019	16.21.1000 以降
Intel XXV710	I40E_DEV_ID_25G_B	0x158A	6.0.1
	I40E_DEV_ID_25G_SFP28	0x158B	6.0.1

NIC タイプ	説明	PCI デバイス ID	ファームウェアのバージョン
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7	n/a
		0x1514	n/a
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1517	n/a
		0x10F8	n/a
	IXGBE_DEV_ID_82599_KR	0x000C	n/a
	IXGBE_DEV_ID_82599_CO	0x10F9	n/a
	MBO_BACKPLANE	0x10FB	n/a
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x11A9	n/a
		0x1F72	n/a
	IXGBE_DEV_ID_82599_CX4	0x17D0	n/a
		0x0470	n/a
	IXGBE_DEV_ID_82599_SF	0x1507	n/a
	P	0x154D	n/a
		0x154A	n/a
	IXGBE_SUBDEV_ID_82599_SFP	0x1558	n/a
		0x1557	n/a
	IXGBE_SUBDEV_ID_82599_RNDC	0x10FC	n/a
		0x151C	n/a
	IXGBE_SUBDEV_ID_82599_560FLR		
	IXGBE_SUBDEV_ID_82599_ECNA_DP		
	IXGBE_DEV_ID_82599_SF		
	P_EM		
	IXGBE_DEV_ID_82599_SF		
	P_SF2		
	IXGBE_DEV_ID_82599_SF		
	P_SF_QP		
	IXGBE_DEV_ID_82599_QS		
	FP_SF_QP		
	IXGBE_DEV_ID_82599EN_SFP		
	IXGBE_DEV_ID_82599_XA		
	UI_LOM		
	IXGBE_DEV_ID_82599_T3		
	_LOM		
Intel X540	IXGBE_DEV_ID_X540T	0x1528	n/a
	IXGBE_DEV_ID_X540T1	0x1560	n/a
Intel X550	IXGBE_DEV_ID_X550T	0x1563	n/a
	IXGBE_DEV_ID_X550T1	0x15D1	n/a
Intel X710	I40E_DEV_ID_SFP_X710	0x1572	6.0.1
	I40E_DEV_ID_KX_C	0x1581	6.0.1
	I40E_DEV_ID_10G_BASE_T	0x1586	6.0.1

NIC タイプ	説明	PCI デバイス ID	ファームウェアのバージョン
Intel XL710	I40E_DEV_ID_KX_B	0x1580	6.0.1
	I40E_DEV_ID_QSFP_A	0x1583	6.0.1
	I40E_DEV_ID_QSFP_B	0x1584	6.0.1
	I40E_DEV_ID_QSFP_C	0x1585	6.0.1
Cisco VIC 1300 シリーズ	Cisco UCS Virtual Interface Card 1300	0x0043	n/a

注： 上記のサポート対象の NIC については、使用するメディア アダプタとケーブルがベンダーのサポート対象メディア タイプであることを確認してください。ベンダーでサポートされていないメディア アダプタまたはケーブルを使用すると、予期しない動作が発生する可能性があります。たとえば、メディア アダプタが認識されず、起動できないことがあります。サポート対象のメディア アダプタとケーブルの詳細については、NIC ベンダーのドキュメントを参照してください。

ベア メタル サーバ システムの要件

ベア メタル サーバを構成する前に、サーバがサポート対象の要件を満たしていることを確認します。

重要： インストールを実行するユーザーは、一部の手順で `sudo` コマンド権限が必要になる場合があります。[ベア メタル サーバへのサードパーティ製パッケージのインストール](#) を参照してください。

ベア メタル サーバの要件

オペレーティング システム	バージョン	CPU コア	メモリ
CentOS Linux	7.4 (1708)	4	16 GB
	7.5		
Red Hat Enterprise Linux (RHEL)	7.6 (カーネル : 3.10.0-957)	4	16 GB
	7.5		
	7.4 (カーネル : 3.10.0-6**)		
SUSE Linux Enterprise Server	12 sp3, 12 sp4	4	16 GB
Ubuntu	16.04.2 LTS (カーネル : 4.4.0-*)	4	16 GB
	18.04		

注： NSX-T Data Center 2.5 以降では、バージョン 18.04.2 LTS を実行する Ubuntu ホストをバージョン 16.04 からアップグレードするか、新規にインストールします。

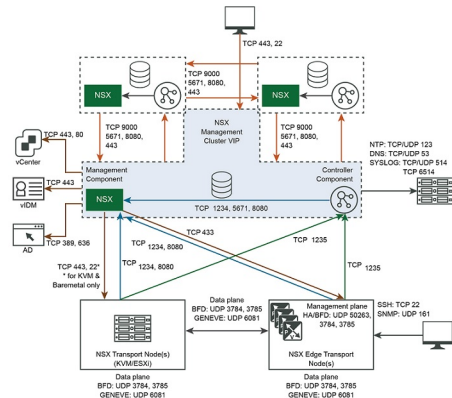
ベア メタル Linux コンテナの要件

ベア メタル Linux コンテナの要件については、『NSX Container Plugin for OpenShift - インストールおよび管理ガイド』を参照してください。

ポートとプロトコル

ポートとプロトコルにより、NSX-T Data Center でノード間の通信パスが使用可能になります。このパスはセキュリティで保護され、認証が行われます。また、資格情報の保管場所を使って相互認証が確立されます。

注： 物理およびホストの両方のハイパーバイザー ファイアウォールで、必要なポートとプロトコルが開いている必要があります。



デフォルトでは、すべての証明書が自己署名の証明書です。ノースバウンドのユーザー インターフェイス、API 証明書、プライベート キーは、CA 署名付きの証明書で置き換えることができます。

ループバックまたは UNIX ドメインのソケットを経由して通信する内部デーモンがあります。

- KVM : MPA、netcpa、nsx-agent、OVS
- ESXi : netcpa、ESX-DP（カーネル内）

注: NSX-T Data Center ノードにアクセスするには、これらのノードで SSH を有効にする必要があります。

NSX Cloud のメモ NSX Cloud を展開するために必要なポートのリストについては、[ポートとプロトコルへのアクセスの有効化](#) を参照してください。

NSX Manager が使用する TCP および UDP ポート

NSX Manager は、特定の TCP および UDP ポートを使用して、他のコンポーネントおよび製品と通信します。ファイアウォールで、これらのポートを開く必要があります。

API 呼び出しまたは CLI コマンドを使用して、ファイルを転送するためのカスタム ポート（デフォルトは 22）および Syslog データをエクスポートするためのカスタム ポート（デフォルトは 514 および 6514）を指定することができます。その場合は、ファイアウォールを適切に設定する必要があります。

表 3-2. NSX Manager が使用する TCP および UDP ポート

送信元	宛先	ポート	プロトコル	説明
NSX Manager、NSX Edge ノード、トランスポート ノード	NSX Manager	5671、1234、1235、443	TCP	NSX メッセージング
NSX Manager、NSX Edge ノード、トランスポート ノード、vCenter Server	NSX Manager	8080	TCP	インストールとアップグレードの HTTP リポジトリ
NSX Manager	NSX Manager	9000 5671、1234、443、8080	TCP	分散データストア
NSX Manager	DNS サーバ	53	TCP	DNS
NSX Manager	DNS サーバ	53	UDP	DNS
NSX Manager	管理 SCP サーバ	22	TCP	SSH (サポート バンドル、バックアップなどのアップロード)
NSX Manager	NTP サーバ	123	UDP	NTP
NSX Manager	SNMP サーバ	161、162	TCP	SNMP
NSX Manager	SNMP サーバ	161、162	UDP	SNMP
NSX Manager	Syslog サーバ	514	TCP	Syslog
NSX Manager	Syslog サーバ	514	UDP	Syslog
NSX Manager	Syslog サーバ	6514	TCP	Syslog
NSX Manager	Syslog サーバ	6514	UDP	Syslog
NSX Manager	中間およびルート CA サーバ	80	TCP	Syslog (TLS 経由でエクスポート) 注： 証明書失効リスト (CRL) の取得に使用される TCP ポートを確認するには、認証局の CRL 配布ポイント (CDP) URI を確認します。
NSX Manager	Traceroute の宛先	3343 - 33523	UDP	Traceroute
NSX Manager	vCenter Server	80	TCP	設定されている場合、NSX Manager からコンピュータ マネージャ (vCenter Server) への通信。

表 3-2. NSX Manager が使用する TCP および UDP ポート（続き）

送信元	宛先	ポート	プロトコル	説明
NSX Manager	vCenter Server	443	TCP	設定されている場合、NSX Manager からコンピュート マネージャ (vCenter Server) への通信。
NTP サーバ	NSX Manager	123	UDP	NTP
管理クライアント	NSX Manager	22	TCP	SSH（デフォルトでは無効）
管理クライアント	NSX Manager	443	TCP	NSX API サーバ
SNMP サーバ	NSX Manager	161	UDP	SNMP

NSX Edge が使用する TCP および UDP ポート

NSX Edge は、特定の TCP および UDP ポートを使用して、他のコンポーネントおよび製品と通信します。ファイアウォールで、これらのポートを開く必要があります。

API 呼び出しまたは CLI コマンドを使用して、ファイルを転送するためのカスタム ポート（デフォルトは 22）および Syslog データをエクスポートするためのカスタム ポート（デフォルトは 514 および 6514）を指定することができます。その場合は、ファイアウォールを適切に設定する必要があります。

表 3-3. NSX Edge が使用する TCP および UDP ポート

送信元	宛先	ポート	プロトコル	説明
管理クライアント	NSX Edge ノード	22	TCP	SSH（デフォルトでは無効）
NSX Agent	NSX Edge ノード	5555	TCP	NSX クラウド：インスタンス上のエージェントが NSX Cloud Gateway と通信します。
NSX Edge ノード	DNS サーバ	53	UDP	DNS
NSX Edge ノード	管理 SCP または SSH サーバ	22	TCP	SSH
NSX Edge ノード	NSX Manager	1235	TCP	下位の制御プレーン (LCP) から中央制御プレーン (CCP) への通信
NSX Edge ノード	NSX Edge ノード	1167	TCP	DHCP バックエンド
NSX Edge ノード	NSX Edge ノード	2480	TCP	Nestdb
NSX Edge ノード	NSX Edge ノード	6666	TCP	NSX クラウド：NSX Edge ローカル通信。
NSX Edge ノード	NSX Edge ノード	50263	UDP	高可用性
NSX Edge ノード	NSX Manager	443	TCP	HTTPS
NSX Edge ノード	NSX Manager	1234	TCP	NSX Manager への NSX メッセージ チャンネル

表 3-3. NSX Edge が使用する TCP および UDP ポート (続き)

送信元	宛先	ポート	プロトコル	説明
NSX Edge ノード	NSX Manager	8080	TCP	NAPI、NSX-T Data Center のアップグレード
NSX Edge ノード	NTP サーバ	123	UDP	NTP
NSX Edge ノード	OpenStack Nova API サーバ	3000 - 9000	TCP	メタデータ プロキシ
NSX Edge ノード	SNMP サーバ	161、162	TCP	SNMP
NSX Edge ノード	SNMP サーバ	161、162	UDP	SNMP
NSX Edge ノード	Syslog サーバ	514	TCP	Syslog
NSX Edge ノード	Syslog サーバ	514	UDP	Syslog
NSX Edge ノード	Syslog サーバ	6514	TCP	Syslog
NSX Edge ノード	Syslog サーバ	6514	UDP	Syslog
NSX Edge ノード	中間およびルート CA サーバ	80	TCP	Syslog (TLS 経由でエクスポート) 注: 証明書失効リスト (CRL) の取得に使用される TCP ポートを確認するには、認証局の CRL 配布ポイント (CDP) URI を確認します。
NSX Edge ノード	Traceroute の宛先	33434 - 33523	UDP	Traceroute
NSX Edge ノード、トランスポート ノード	NSX Edge ノード	3784、3785	UDP	データ内のトランスポート ノード TEP IP アドレス間の BFD。
NTP サーバ	NSX Edge ノード	123	UDP	NTP
SNMP サーバ	NSX Edge ノード	161	UDP	SNMP

ESXi、KVM ホスト、ベアメタル サーバで使用する TCP および UDP ポート

ESXi、KVM ホスト、ベアメタル サーバをトランスポート ノードとして使用する場合、特定の TCP および UDP ポートを開いておく必要があります。

表 3-4. ESXi および KVM ホストによって使用される TCP および UDP ポート

送信元	宛先	ポート	プロトコル	説明
ESXi ホスト	NSX Manager	1235	TCP	ローカルの制御プレーン (LCP) から中央制御プレーン (CCP) への通信
ESXi ホスト	NSX Manager	1234	TCP	NSX Manager への NSX メッセージ チャンネル NSX Manager との AMQP 通信チャンネル

表 3-4. ESXi および KVM ホストによって使用される TCP および UDP ポート（続き）

送信元	宛先	ポート	プロトコル	説明
ESXi ホスト	NSX Manager	8080	TCP	HTTP リポジトリのインストールおよびアップグレード
ESXi および KVM ホスト	NSX Manager	443	TCP	管理とプロビジョニング接続
ESXi および KVM ホスト	NSX Manager	443	TCP	HTTP リポジトリのインストールおよびアップグレード
GENEVE Termination End Point (TEP)	GENEVE Termination End Point (TEP)	6081	UDP	トランスポート ネットワーク
KVM ホスト	NSX Manager	1234	TCP	NSX Manager への NSX メッセージ チャネル NSX Manager との AMQP 通信チャネル
ベアメタル サーバ ホスト	NSX Manager	5671、 1235、 1234、 8080	TCP	NSX Manager との AMQP 通信チャネル
KVM ホスト	NSX Manager	1235	TCP	ローカルの制御プレーン (LCP) から中央制御プレーン (CCP) への通信
KVM ホスト	NSX Manager	8080	TCP	HTTP リポジトリのインストールおよびアップグレード
NSX Manager	ESXi ホスト	443	TCP	管理とプロビジョニング接続
NSX Manager	KVM ホスト	443	TCP	管理とプロビジョニング接続
ホスト	Syslog サーバ	514	TCP	Syslog (ホストの Syslog ドキュメントを参照)
ホスト	Syslog サーバ	514	UDP	Syslog (ホストの Syslog ドキュメントを参照)
ホスト	Syslog サーバ	6514	TCP	Syslog (ホストの Syslog ドキュメントを参照)
ホスト	Syslog サーバ	6514	UDP	Syslog (ホストの Syslog ドキュメントを参照)
ホスト	中間およびルート CA サーバ	80	TCP	Syslog (TLS 経由でエクスポート) 注： 証明書失効リスト (CRL) の取得に使用される TCP ポートを確認するには、認証局の CRL 配布ポイント (CDP) URI を確認します。
NSX-T Data Center トランスポート ノード	NSX-T Data Center トランスポート ノード	3784、 3785	UDP	TEP インターフェイスを使用するデータベースにおける TEPS 間の BFD セッション

NSX Manager のインストール

4

NSX Manager には、論理スイッチ、論理ルーター、ファイアウォールなどの NSX-T Data Center コンポーネントを作成、設定、監視する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 があります。

NSX Manager はシステム ビューを提供するものであり、NSX-T Data Center の管理コンポーネントです。

高可用性の場合、NSX-T Data Center は 3 つの NSX Manager の管理クラスタをサポートします。本番環境では、管理クラスタの展開をお勧めします。POC（事前検証）環境では、単一の NSX Manager を展開できます。

vSphere 環境では、次の機能が NSX Manager でサポートされています。

- vCenter Server で vMotion 機能を使用して、ホストおよびクラスタ間で NSX Manager のライブ移行を実行できます。
- vCenter Server で Storage vMotion 機能を使用して、ホストおよびクラスタ間で NSX Manager のライブ移行を実行できます。
- vCenter Server で Distributed Resource Scheduler 機能を使用して、ホストおよびクラスタ間で NSX Manager を再調整できます。
- vCenter Server で非アフィニティ機能を使用して、ホストおよびクラスタ間で NSX Manager を管理できます。

NSX Manager の展開、プラットフォームおよびインストール要件

次の表では、NSX Manager の展開、プラットフォーム、インストールの要件について詳しく説明します。

要件	説明
サポートされる展開方法	<ul style="list-style-type: none">■ OVA/OVF■ QCOW2
サポート対象のプラットフォーム	NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件 を参照してください。 ESXi では、共有ストレージに NSX Manager アプライアンスをインストールすることが推奨されます。
IP アドレス	NSX Manager には固定 IP アドレスが必要です。インストール後に IP アドレスを変更することはできません。

要件	説明
NSX-T Data Center アプライアンスのパスワード	<ul style="list-style-type: none"> ■ 12 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の大文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 5 文字以上の異なる文字 ■ 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。 <ul style="list-style-type: none"> ■ <code>retry=3</code> : 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。 ■ <code>minlen=12</code> : 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。 ■ <code>difok=0</code> : 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。<code>difok</code> に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。 ■ <code>lcredit=1</code> : 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の <code>minlen</code> 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>ucredit=1</code> : 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の <code>minlen</code> 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>dcredit=1</code> : 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の <code>minlen</code> 値に合わせるため、それぞれの数字が +1 とカウントされます。 ■ <code>ocredit=1</code> : 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の <code>minlen</code> 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>enforce_for_root</code> : <code>root</code> ユーザーに設定されるパスワード。 <p>注： Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、<code>man</code> ページを参照してください。</p> <p>たとえば、単純で体系的なパスワードの使用は避けます。たとえば、VMware123! 123、VMware12345 などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、VMware123! 45、VMware1! 2345、VMware@1az23x などです。</p>
ホスト名	<p>NSX Manager をインストールするときに、アンダースコアなどの無効な文字や、ドット (.) などの特殊文字を含まないホスト名を指定します。ホスト名に無効な文字や特殊文字が含まれていると、展開後にホスト名が nsx-manager に設定されます。</p> <p>ホスト名の制限の詳細については、https://tools.ietf.org/html/rfc952 および https://tools.ietf.org/html/rfc1123 を参照してください。</p>
VMware Tools	<p>ESXi で実行される NSX Manager 仮想マシンには、VMware Tools がインストールされています。VMware Tools を削除またはアップグレードしないでください。</p>

要件	説明
システム	<ul style="list-style-type: none"> ■ システム要件を満たしていることを確認します。システム要件を参照してください。 ■ 必要なポートが開いていることを確認します。ポートとプロトコルを参照してください。 ■ ESXi ホストでデータストアが構成されていて、アクセスできることを確認します。 ■ 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 アドレスを確認します。 ■ まだ作成していない場合は、宛先の仮想マシン ポート グループ ネットワークを作成します。NSX-T Data Center アプライアンスを管理仮想マシン ネットワークに配置します。 <p>複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。</p> <ul style="list-style-type: none"> ■ NSX Manager IPv4 IP アドレス スキームを使用します。
OVF の権限	<p>ESXi ホストに OVF テンプレートを展開するために必要な権限があることを確認します。</p> <p>OVF テンプレートを展開できる管理ツール (vCenter Server、vSphere Client など) が必要です。手動で設定するには、OVF 展開ツールで設定オプションがサポートされている必要があります。OVF ツールは、4.0 以降のバージョンを使用する必要があります。</p>
クライアント プラグイン	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。

注： NSX Manager のフレッシュ インストールや再起動時、また初回のログイン時にプロンプトで **admin** のパスワードを変更した後は、NSX Manager の起動に数分かかる場合があります。

NSX Manager のインストール シナリオ

重要： vSphere Client またはコマンド ラインのいずれかを使用して OVA または OVF ファイルから NSX Manager をインストールすると、仮想マシンがパワーオン状態になるまで、ユーザー名、パスワードなどの OVA/OVF プロパティ値が検証されません。ただし、[固定 IP アドレス] フィールドは、NSX Manager のインストールに必要なフィールドです。

- **admin** または **audit** ユーザーのユーザー名を指定する場合には、一意の名前を使用する必要があります。同じ名前を指定すると、名前が無視され、デフォルトの名前 (**admin** または **audit**) が使用されます。
- **admin** ユーザーのパスワードが要件を満たしていない場合には、SSH またはコンソール経由で **admin** ユーザーとして NSX Manager にログインする必要があります。ログイン パスワードは **default** です。プロンプトが表示され、パスワードの変更が指示されます。
- **audit** ユーザーのパスワードが要件を満たしていない場合、ユーザー アカウントは無効になります。アカウントを有効にするには、**admin** ユーザーとして SSH またはコンソール経由で NSX Manager にログインし、**set user audit** コマンドを実行して **audit** ユーザーのパスワードを設定します (現在のパスワードは空の文字列です)。

- **root** ユーザーのパスワード要件を満たしていない場合には、**root** として SSH またはコンソール経由で NSX Manager にログインする必要があります。ログイン パスワードは **vmware** です。プロンプトが表示され、パスワードの変更が指示されます。

注意： **root** ユーザー認証情報を使用してログインしている際に NSX-T Data Center に変更を加えると、システム障害が発生し、ネットワークに影響する可能性があります。**root** ユーザー認証情報を使用して変更を加えるのは、VMware のサポート チームから指示があった場合のみにすることをお勧めします。

注： アプライアンス上のコア サービスは、要件を満たすパスワードが設定されるまで起動しません。

NSX Manager を OVA ファイルから展開した後は、仮想マシンをパワーオフして vCenter Server から OVA 設定を変更し、仮想マシンの IP アドレス設定を変更することはできません。

DNS サーバからアクセスする場合の NSX Manager の構成

デフォルトでは、トランスポート ノードは IP アドレスに基づいて NSX Manager にアクセスします。この処理は、NSX Manager の DNS 名に基づいて行うこともできます。

NSX Manager で FQDN の使用 (DNS) を有効にすると、トランスポートノードに影響を与えずに、Manager の IP アドレスを変更できます。

FQDN の使用を有効にするには、NSX Manager の FQDN を公開します。

注： 複数サイトの Lite と NSX Cloud の場合、NSX Manager で FQDN 使用 (DNS) を有効にする必要があります。他の展開タイプではオプションです。『NSX-T Data Center 管理ガイド』の「NSX-T Data Center の複数サイトの展開」とこのガイドの [13 章 NSX Cloud コンポーネントのインストール](#) を参照してください。

NSX Manager の FQDN の公開

NSX-T Data Center コア コンポーネントと CSM をインストールした後、FQDN を使用して NAT を有効にするには、DNS サーバのマネージャ ノードに正引き参照と逆引き参照のエントリを設定する必要があります。

重要： NSX Manager の FQDN に正引き参照と逆引き参照の両方のエントリを設定し、短い TTL (たとえば 600 秒) を設定することを推奨します。

また、NSX-T API を使用して NSX Manager の FQDN を公開できるようにする必要があります。

要求の例：PUT `https://<nsx-mgr>/api/v1/configs/management`

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

応答の例：

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

詳細については、『NSX-T Data Center API ガイド』を参照してください。

注： FQDN を公開した後、次のセクションの説明に従ってトランスポート ノードによるアクセスを検証します。

トランスポート ノードによる FQDN を介したアクセスの検証

NSX Manager の FQDN を公開した後、トランスポート ノードが NSX Manager に正常にアクセスしていることを確認します。

SSH を使用して、ハイパーバイザーまたは Edge ノードなどのトランスポート ノードにログインし、`get controllers` CLI コマンドを実行します。

応答の例：

Controller IP FQDN	Port	SSL	Status	Is Physical Master	Session State	Controller
192.168.60.5 nsxmgr.corp.com	1235	enabled	connected	true	up	

この章には、次のトピックが含まれています。

■ デフォルトの管理者パスワードの有効期限の変更

デフォルトの管理者パスワードの有効期限の変更

デフォルトでは、NSX Manager および NSX Edge アプライアンスの管理者パスワードは、90 日後に期限切れになります。この有効期限は、最初のインストールと構成を行った後でリセットできます。

パスワードが期限切れになると、ログインしてコンポーネントを管理できなくなります。また、管理者パスワードを必要とするタスクまたは API 呼び出しがすべて失敗します。パスワードの有効期限が切れている場合は、ナレッジベースの記事 KB70691、[NSX-T admin password expired](#) を参照してください。

手順

- 1 セキュアなプログラムを使用して、NSX CLI コンソールに接続します。
- 2 有効期限をリセットします。

有効期限は 1 ～ 9,999 日の間で設定できます。

```
nsxcli> set user admin password-expiration <1 - 9999>
```

注： API コマンドを使用して管理者パスワードの有効期間を設定することもできます。

- 3** （オプション） パスワードの有効期限を無効にすると、パスワードが期限切れになることはありません。

```
nsxcli> clear user audit password-expiration
```

NSX-T Data Center の vSphere へのインストール

5

NSX-T Data Center コンポーネント、NSX Manager および NSX Edge は、ユーザー インターフェイスまたは CLI を使用してインストールできます。

vSphere のサポートされているバージョンがあることを確認します。[vSphere のサポート](#)を参照してください。

この章には、次のトピックが含まれています。

- [NSX Manager および利用可能なアプライアンスのインストール](#)
- [クラスタの仮想 IP \(VIP\) アドレスの設定](#)
- [NSX-T アプライアンスでのスナップショットの無効化](#)

NSX Manager および利用可能なアプライアンスのインストール

vSphere Client を使用して NSX Manager または Cloud Service Manager を仮想アプライアンスとして展開できます。

Cloud Service Manager は、NSX-T Data Center コンポーネントを使用する仮想アプライアンスで、パブリック クラウドへのコンポーネントの組み込みを行います。

前提条件

- システム要件を満たしていることを確認します。[システム要件](#)を参照してください。
- 必要なポートが開いていることを確認します。[ポートとプロトコル](#)を参照してください。
- ESXi ホストでデータストアが構成されていて、アクセスできることを確認します。
- 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 アドレスを確認します。
- まだ作成していない場合は、宛先の仮想マシン ポート グループ ネットワークを作成します。NSX-T Data Center アプライアンスを管理仮想マシン ネットワークに配置します。

複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。

- NSX Manager IPv4 IP アドレス スキームを使用します。

手順

- 1 VMware ダウンロード ポータルで NSX-T Data Center OVA 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 ファイルをダウンロードします。
- 2 右クリックして [OVF テンプレートの展開] を選択し、インストール ウィザードを開始します。
- 3 OVA のダウンロード URL を入力するか、OVA ファイルに移動して、[次へ] をクリックします。
- 4 NSX Manager 仮想マシンの名前と場所を入力して、[次へ] をクリックします。
ここに入力する名前が vSphere と vCenter Server インベントリに表示されます。
- 5 NSX Manager アプライアンスのコンピューティング リソースを選択して、[次へ] をクリックします。
 - ◆ vCenter Server によって管理される ESXi ホストにインストールする場合は、NSX Manager アプライアンスを展開するホストを選択します。
 - ◆ スタンドアローンの ESXi ホストにインストールする場合は、NSX Manager アプライアンスを展開するホストを選択します。
- 6 OVF テンプレートの詳細を確認して、[次へ] をクリックします。
- 7 展開の構成サイズを指定して、[次へ] をクリックします。
ウィザードの右側にある説明パネルに、選択した構成の詳細が表示されます。
- 8 構成とディスク ファイルのストレージを指定します。
 - a 仮想ディスク フォーマットを選択します。
 - b 仮想マシン ストレージ ポリシーを選択します。
 - c NSX Manager アプライアンスのファイルを格納するデータストアを指定します。
 - d [次へ] をクリックします。
- 9 各ソース ネットワークのターゲット ネットワークを選択します。
- 10 NSX Manager のポート グループまたはインストール先ネットワークを選択します。
- 11 IP 割り当ての設定を行います。
 - a IP 割り当ての場合は、**固定 - 手動** を指定します。
 - b IP プロトコルの場合は、**IPv4** を選択します。
- 12 [次へ] をクリックします。
次の手順は、OVF テンプレートの展開ウィザードの [テンプレートのカスタマイズ] セクションにあります。
- 13 [アプリケーション] セクションで、NSX Manager のシステム ルート、CLI 管理者、監査パスワードを入力します。**root** と **admin** の認証情報は必須フィールドです。
パスワード強度の基準に準拠したパスワードを使用する必要があります。
 - 12 文字以上
 - 1 文字以上の小文字

- 1 文字以上の大文字
- 1 文字以上の数字
- 1 文字以上の特殊文字
- 5 文字以上の異なる文字
- 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。
 - `retry=3` : 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。
 - `minlen=12` : 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。
 - `difok=0` : 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。`difok` に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。
 - `lcredit=1` : 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `ucredit=1` : 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `dcredit=1` : 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の `minlen` 値に合わせるため、それぞれの数字が +1 とカウントされます。
 - `ocredit=1` : 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `enforce_for_root` : `root` ユーザーに設定されるパスワード。

注： Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、`man` ページを参照してください。

たとえば、単純で体系的なパスワードの使用は避けます。たとえば、**VMware123! 123**、**VMware12345** などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、**VMware123! 45**、**VMware1! 2345**、**VMware@1az23x** などです。

- 14 [オプション パラメータ] セクションで、パスワード フィールドは空白のままにします。これは、vCenter Server へのアクセス権を持つユーザーによって VMC ロールのパスワードを悪用するリスクを回避するためです。NSX-T Data Center の VMC を展開する場合、このフィールドは、クラウド管理者ロールとクラウド監査ロールのパスワードを設定するために内部で使用されます。
- 15 [ネットワーク プロパティ] セクションで、NSX Manager のホスト名を入力します。

注： ホスト名は、有効なドメイン名にする必要があります。ドットで区切られたホスト名（ドメイン/サブドメイン）の各部分は、英字で始まっている必要があります。

16 アプライアンスの [ロール名] を選択します。デフォルトのロールは [NSX Manager] です。

- NSX Manager アプライアンスをインストールするには、[NSX Manager] ロールを選択します。
- NSX Cloud 展開で Cloud Service Manager (CSM) アプライアンスをインストールするには、[nsx-cloud-service-manager] ロールを選択します。

詳細については、[NSX Cloud の展開の概要](#)を参照してください。

17 (必須フィールド) デフォルト ゲートウェイ、管理ネットワークの IPv4、管理ネットワークのネットマスクを入力します。

重要： 固定 IP アドレスを入力せずに管理ネットワークの IPv4 フィールドを空白にすると、アプライアンスの展開中に IP アドレスが NSX Manager に割り当てられません。パワーオン時に NSX Manager にアクセスすることはできません。回避策として、NSX Manager アプライアンスを再デプロイします。

18 [DNS] セクションで、DNS サーバ リストとドメイン検索リストを入力します。

19 [サービス設定] セクションで、NTP サーバ リストを入力します。

必要に応じて、SSH サービスを有効にして、root の SSH ログインを許可することができます。(推奨されません。)

20 すべてのカスタム OVF テンプレートの仕様が正確であることを確認し、[終了] をクリックしてインストールを開始します。

インストールには 7 ～ 8 分かかる場合があります。

21 最適なパフォーマンスを維持するため、アプライアンス用のメモリを予約します。

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、予約を設定します。[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#) を参照してください。

22 vSphere Client から仮想マシン コンソールを開いて、ノードの起動プロセスを追跡します。

23 ノードが起動した後、admin として CLI にログインし、get interface eth0 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。

24 get services コマンドを入力して、すべてのデフォルトのサービスが実行されていることを確認します。

デフォルトでは、次のサービスは必要なく、自動的に開始されません。

- liagent
- migration-coordinator：このサービスは、Migration Coordinator の実行時にのみ使用されます。このサービスを開始する前に、NSX-T Data Center Migration Coordinator ガイドを参照してください。
- snmp：SNMP の起動の詳細については、NSX-T Data Center 管理ガイドの「簡易ネットワーク管理プロトコル」を参照してください。
- nsx-message-bus：このサービスは NSX-T Data Center 3.0 では使用されていません。

25 NSX Manager または グローバル マネージャ ノードに必要な接続があることを確認します。

次のタスクを実行できることを確認します。

- 別のマシンからノードに ping を実行します。
- ノードは、デフォルト ゲートウェイに ping を実行できます。
- ノードは、管理インターフェイスを使用して、同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- ノードは、DNS サーバと NTP サーバに ping を実行できます。
- SSH を有効にした場合は、SSH を使用してノードに接続できることを確認します。

接続が確立されていない場合は、仮想アプライアンスのネットワーク アダプタが適切なネットワークまたは VLAN に配置されていることを確認します。

次のステップ

サポートされている Web ブラウザで NSX Manager にログインします。新しく作成された NSX Manager にログインするを参照してください。

コマンドライン OVF ツールを使用した ESXi への NSX Manager のインストール

NSX Manager のインストールを自動的に行うか、CLIで行う場合は、コマンドライン ユーティリティの VMware OVF ツールを使用します。

デフォルトでは、`nsx_isSSHEnabled` と `nsx_allowSSHRootLogin` はいずれもセキュリティ上の理由により無効になっています。無効になっている場合、NSX Manager のコマンドラインへの SSH 接続やログインはできません。`nsx_isSSHEnabled` を有効にして、`nsx_allowSSHRootLogin` を有効にしなかった場合、NSX Manager に SSH で接続することはできますが、`root` でログインすることはできません。

前提条件

- システム要件を満たしていることを確認します。システム要件を参照してください。
- 必要なポートが開いていることを確認します。ポートとプロトコルを参照してください。
- ESXi ホストでデータストアが構成されていて、アクセスできることを確認します。
- 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 アドレスを確認します。
- まだ作成していない場合は、宛先の仮想マシン ポート グループ ネットワークを作成します。NSX-T Data Center アプライアンスを管理仮想マシン ネットワークに配置します。

複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。

- NSX Manager IPv4 IP アドレス スキームを使用します。

手順

- 1 適切なオプションを使用して ovftool コマンドを実行します。

このプロセスは、ホストがスタンドアローンか、vCenter Server によって管理されているかによって異なります。

- スタンドアローン ホストの場合：
 - Windows の例：

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--deploymentOption=medium \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_cli_audit_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51
```

注： 上の Windows のコード ブロックでは、コマンドラインの継続を表すためにバックスラッシュ (\) を使用しています。実際に使用する場合は、バックスラッシュを省略し、コマンド全体を 1 行で入力します。

注： 上記の例では、10.168.110.51 が NSX Manager の展開先ホスト マシンの IP アドレスです。

注： 上記の例では、--deploymentOption がデフォルト サイズの Medium に設定されています。サポートされているその他のサイズについては、[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#)を参照してください。

■ Linux の例 :

```

mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@mgresxhost01

```

結果は次のようになります。

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates

```

```
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

■ vCenter Server によって管理されているホストの場合：

■ Windows の例：

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--deploymentOption=medium \
--X:injectOvfEnv \
--X:logFile=ovftool.log \
  --allowExtraConfig \
--datastore=ds1 \
--network="management" \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51
```

注： 上の Windows のコード ブロックでは、コマンドラインの継続を表すためにバックスラッシュ (\) を使用しています。実際に使用する場合は、バックスラッシュを省略し、コマンド全体を 1 行で入力します。

注： 上記の例では、--deploymentOption がデフォルト サイズの Medium に設定されています。サポートされているその他のサイズについては、[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#)を参照してください。

■ Linux の例：

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
```

```

mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

vadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vadmin:$vcpass@$vcip/?ip=$mgresxhost01

```

結果は次のようになります。

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/

```

```
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

- 2 OVF ツールをプローブ モードで実行して、ソースのコンテンツを表示することもできます。OVA および OVF パッケージは、サポートされているその他のソース タイプのリストから探すことができます。プローブ モードで返された情報を使用して、展開を構成できます。

```
$> \ovftool --allowExtraConfig <OVA path or URL>
```

ここで、--allowExtraConfig は、Cloud Service Manager (CSM) でサポートされているアプライアンス タイプです。

- 3 最適なパフォーマンスを維持するため、アプライアンス用のメモリを予約します。

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、予約を設定します。[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#) を参照してください。

- 4 vSphere Client から仮想マシン コンソールを開いて、ノードの起動プロセスを追跡します。
- 5 ノードが起動した後、admin として CLI にログインし、get interface eth0 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。
- 6 NSX Manager または グローバル マネージャ ノードに必要な接続があることを確認します。

次のタスクを実行できることを確認します。

- 別のマシンからノードに ping を実行します。
- ノードは、デフォルト ゲートウェイに ping を実行できます。
- ノードは、管理インターフェイスを使用して、同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- ノードは、DNS サーバと NTP サーバに ping を実行できます。
- SSH を有効にした場合は、SSH を使用してノードに接続できることを確認します。

接続が確立されていない場合は、仮想アプライアンスのネットワーク アダプタが適切なネットワークまたは VLAN に配置されていることを確認します。

次のステップ

サポートされている Web ブラウザで NSX Manager にログインします。[新しく作成された NSX Manager にログインする](#) を参照してください。

起動時に GRUB メニューを表示するための NSX-T Data Center の設定

NSX-T Data Center アプライアンスの root パスワードをリセットするには、起動時に GRUB メニューを表示するように NSX-T Data Center アプライアンスを設定する必要があります。

重要： アプライアンスを展開してから、この設定を行わなかった場合、root、admin または audit パスワードを忘れたときにリセットできなくなります。

手順

- 1 仮想マシンに root としてログインします。
- 2 `/etc/default/grub` ファイルで、`GRUB_HIDDEN_TIMEOUT` パラメータの値を変更します。

```
GRUB_HIDDEN_TIMEOUT=2
```

- 3 (オプション) `/etc/grub.d/40_custom` ファイルで、GRUB パスワードを変更します。

デフォルトのパスワードは、`VMware1` です。

- 4 GRUB 設定を更新します。

```
update-grub
```

新しく作成された NSX Manager にログインする

NSX Manager をインストールした後は、ユーザー インターフェイスを使用して、その他のインストール タスクを実行できます。

NSX Manager をインストールしたら、NSX-T Data Center のカスタマー エクスペリエンス向上プログラム (CEIP) に参加できます。プログラムへの参加または参加を後で中止する方法については、『NSX-T Data Center 管理ガイド』の NSX のカスタマー エクスペリエンス向上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 がインストールされていることを確認します。[NSX Manager および利用可能なアプライアンスのインストール](#) を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
エンド ユーザー使用許諾契約書 (EULA) が表示されます。
- 2 エンド ユーザー使用許諾契約書 (EULA) を読んで同意します。
- 3 VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加するかどうかを選択します。
- 4 [保存] をクリックします。

コンピュート マネージャの追加

コンピュート マネージャは、vCenter Server のように、ホストや仮想マシンなどのリソースを管理するアプリケーションです。

NSX-T Data Center は、コンピュート マネージャをポーリングし、vCenter Server からクラスタ情報を収集します。

vCenter Server コンピュート マネージャを追加する場合は、vCenter Server ユーザーの認証情報を指定する必要があります。vCenter Server 管理者認証情報を指定することも、NSX-T Data Center 専用のロールとユーザーを作成して、このユーザーの認証情報を指定することもできます。このロールには、次の vCenter Server 権限が必要です。

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Host.Configuration.NetworkConfiguration
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

vCenter Server ロールと権限の詳細については、vSphere Security のドキュメントを参照してください。

前提条件

- サポート対象の vSphere バージョンを使用していることを確認します。[サポート対象の vSphere バージョン](#) を参照してください。
- IPv6 および IPv4 は vCenter Server と通信します。
- 推奨される数のコンピュート マネージャを使用していることを確認します。<https://configmax.vmware.com/home> を参照してください。

注： NSX-T Data Center では、同じ vCenter Server を複数の NSX Manager に登録できません。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [コンピュート マネージャ] - [追加] を選択します。

3 コンピュート マネージャの詳細を設定します。

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

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

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

4 進行状況アイコンが [処理中] から [未登録] に変わった場合は、次の手順を実行してエラーを解決します。

- a エラー メッセージを選択し、[解決] をクリックします。次のようなエラー メッセージが表示される可能性があります：

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

- b vCenter Server 認証情報を入力し、[解決] をクリックします。

すでに登録がされている場合には置き換えられます。

結果

vCenter Server にコンピュート マネージャを登録し、接続状態が「稼動中」と表示されるまでしばらく時間がかかります。

コンピュート マネージャの名前をクリックすると、詳細の表示、コンピュート マネージャの編集、コンピュート マネージャに適用するタグの管理を行うことができます。

vCenter Server が正常に登録されたら、コンピュート マネージャを削除する前に、NSX Manager 仮想マシンをパワーオフして削除しないでください。削除の順序が異なると、新しい NSX Manager を展開するときに、同じ vCenter Server を再度登録できなくなります。vCenter Server が別の NSX Manager に登録されているというエラーが表示されます。

注： vCenter Server (VC) コンピュート マネージャが正常に追加された後に、次のいずれかのアクションが正常に実行された場合、vCenter Server を削除することはできません。

- NSX サービス挿入を使用して、vCenter Server 内のホストまたはクラスタにサービス仮想マシンを展開する。
- NSX Manager UI を使用して、ホストまたは vCenter Server のクラスタに NSX Edge、NSX Intelligence 仮想マシンまたは NSX Manager ノードを展開する。

これらのアクションのいずれかでエラーが発生した場合（インストールの失敗など）、上記のいずれかの操作が正常に実行されていなければ、vCenter Server を削除できます。

次の場合にも vCenter Server を削除できます。

- すべてのトランスポート ノードの準備が解除された。
- すべてのサービス仮想マシン、NSX Intelligence 仮想マシン、すべての NSX Edge 仮想マシン、NSX Manager ノードの展開が解除された。

この制限は、NSX-T Data Center 2.5.x の新規インストールだけでなく、アップグレードにも適用されます。

クラスタを構成する NSX Manager ノードをユーザー インターフェイスから展開

複数の NSX Manager ノードを展開して高可用性と信頼性を確保することができます。

新しいノードの展開後、これらのノードはクラスタを構成する NSX Manager ノードに接続します。クラスタ化する NSX Manager ノードの推奨数は 3 です。

注： ユーザー インターフェイスを使用した複数の NSX Manager ノードの展開は、vCenter Server の管理対象である ESXi ホストでのみサポートされます。

最初に展開された NSX Manager ノードのすべてのリポジトリの詳細とパスワードが、クラスタ内に新しく展開されたノードと同期されます。

前提条件

- NSX Manager ノードがインストールされていることを確認します。[NSX Manager および利用可能なアプライアンスのインストール](#) を参照してください。
- コンピュート マネージャが設定されていることを確認します。[コンピュート マネージャの追加](#) を参照してください。
- システム要件を満たしていることを確認します。[システム要件](#) を参照してください。
- 必要なポートが開いていることを確認します。[ポートとプロトコル](#) を参照してください。
- ESXi ホストでデータストアが構成されていて、アクセスできることを確認します。

- 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 アドレスを確認します。
- まだ作成していない場合は、宛先の仮想マシン ポート グループ ネットワークを作成します。NSX-T Data Center アプライアンスを管理仮想マシン ネットワークに配置します。

複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [アプライアンス] - [概要] - [ノードの追加] を選択します。
- 3 NSX Manager の共通属性の詳細を入力します。

オプション	説明
コンピュート マネージャ	登録されているリソースのコンピュート マネージャが表示されます。
SSH の有効化	新しい NSX Manager ノードへの SSH ログインの許可をボタンで切り替えます。
root アクセスの有効化	新しい NSX Manager ノードへの root アクセスの許可をボタンで切り替えます。

オプション	説明
CLI ユーザー名とパスワードの確認	<p>新しいノードの CLI パスワードとパスワードの確認を設定します。</p> <p>パスワード強度の基準に準拠したパスワードを使用する必要があります。</p> <ul style="list-style-type: none"> ■ 12 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の大文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 5 文字以上の異なる文字 ■ 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。 <ul style="list-style-type: none"> ■ <code>retry=3</code> : 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。 ■ <code>minlen=12</code> : 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。 ■ <code>difok=0</code> : 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。difok に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。 ■ <code>lcredit=1</code> : 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>ucredit=1</code> : 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>dcredit=1</code> : 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の minlen 値に合わせるため、それぞれの数字が +1 とカウントされます。 ■ <code>ocredit=1</code> : 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>enforce_for_root</code> : root ユーザーに設定されるパスワード。 <p>注： Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、man ページを参照してください。</p> <p>たとえば、単純で体系的なパスワードの使用は避けます。たとえば、VMware123!、123、VMware12345 などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、VMware123!、45、VMware1!、2345、VMware@1az23x などです。</p> <p>CLI ユーザー名は <code>admin</code> に設定されています。</p>

オプション	説明
root パスワードとパスワードの確認	<p>新しいノードの root パスワードとパスワードの確認を設定します。</p> <p>パスワード強度の基準に準拠したパスワードを使用する必要があります。</p> <ul style="list-style-type: none"> ■ 12 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の大文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 5 文字以上の異なる文字 ■ 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。 <ul style="list-style-type: none"> ■ <code>retry=3</code> : 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。 ■ <code>minlen=12</code> : 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。 ■ <code>difok=0</code> : 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。difok に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。 ■ <code>lcredit=1</code> : 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>ucredit=1</code> : 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>dcredit=1</code> : 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の minlen 値に合わせるため、それぞれの数字が +1 とカウントされます。 ■ <code>ocredit=1</code> : 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>enforce_for_root</code> : root ユーザーに設定されるパスワード。 <p>注： Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、man ページを参照してください。</p> <p>たとえば、単純で体系的なパスワードの使用は避けます。たとえば、VMware123! 123、VMware12345 などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、VMware123! 45、VMware1! 2345、VMware@1az23x などです。</p>
DNS サーバ	vCenter Server で使用可能な DNS サーバの IP アドレスを入力します。
NTP サーバ	NTP サーバの IP アドレスを入力します。

4 NSX Manager ノードの詳細を入力します。

オプション	説明
名前	NSX Manager ノードの名前を入力します。
クラスタ	ドロップダウン メニューから、ノードが参加するクラスタを指定します。
リソース プールまたはホスト	ドロップダウン メニューから、ノードにリソース プールまたはホストのいずれかを割り当てます。
データストア	ドロップダウン メニューから、ノードのファイルのデータストアを選択します。
ネットワーク	ドロップダウン メニューからネットワークを割り当てます。
管理 IP アドレス/ネットマスク	IP アドレスとネットマスクを入力します。
管理ゲートウェイ	ゲートウェイの IP アドレスを入力します。

5 (オプション) [ノードの作成] をクリックして別のノードを構成します。

手順 3 ～ 4 を繰り返します。

6 [終了] をクリックします。

新しいノードが展開されます。展開のプロセスは、[システム] - [アプライアンス] - [概要] 画面または vCenter Server で追跡することができます。

7 展開、クラスタの構成、およびリポジトリの同期が完了するまで 10 ～ 15 分かかるため、待機します。

最初に展開された NSX Manager ノードのすべてのリポジトリの詳細とパスワードが、クラスタ内に新しく展開されたノードと同期されます。

注： 新しいノードの展開中に最初のノードが再起動すると、クラスタへの新しいノードの登録が失敗し、新しいノードのサムネイルに Failed to Register というメッセージが表示されることがあります。クラスタに手動でノードを再展開するには、新しいノードのサムネイルに移動し、垂直方向の省略記号を選択して、[再実行] をクリックします。

8 ノードが起動した後、admin として CLI にログインし、get interface eth0 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。

9 get services コマンドを入力して、すべてのデフォルトのサービスが実行されていることを確認します。

デフォルトでは、次のサービスは必要なく、自動的に開始されません。

- liagent
- migration-coordinator：このサービスは、Migration Coordinator の実行時にのみ使用されます。このサービスを開始する前に、NSX-T Data Center Migration Coordinator ガイドを参照してください。
- snmp：SNMP の起動の詳細については、NSX-T Data Center 管理ガイドの「簡易ネットワーク管理プロトコル」を参照してください。
- nsx-message-bus：このサービスは NSX-T Data Center 3.0 では使用されていません。

- 最初に展開された NSX Manager ノードにログインし、`get cluster status` コマンドを入力してノードが正常にクラスタに追加されていることを確認します。
- NSX Manager または グローバル マネージャ ノードに必要な接続があることを確認します。

次のタスクを実行できることを確認します。

- 別のマシンからノードに ping を実行します。
- ノードは、デフォルト ゲートウェイに ping を実行できます。
- ノードは、管理インターフェイスを使用して、同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- ノードは、DNS サーバと NTP サーバに ping を実行できます。
- SSH を有効にした場合は、SSH を使用してノードに接続できることを確認します。

接続が確立されていない場合は、仮想アプライアンスのネットワーク アダプタが適切なネットワークまたは VLAN に配置されていることを確認します。

次のステップ

NSX Edge を設定します。[vSphere の GUI を使用した ESXi への NSX Edge のインストール](#) を参照してください。

クラスタを構成する NSX Manager ノードを CLI を使用して展開

CLI を使用してクラスタを構成する NSX Manager を参加させると、クラスタ内のすべての NSX Manager ノードが相互に通信できるようになります。

前提条件

NSX-T Data Center コンポーネントのインストールが完了している必要があります。

手順

- 最初に展開した NSX Manager ノードへの SSH セッションを開きます。
- 管理者の認証情報を使用してログインします。
- NSX Manager ノードで `get certificate api thumbprint` コマンドを実行します。
コマンド出力は、この NSX Manager に固有の一連の数値です。
- `get cluster config` コマンドを実行して最初に展開した NSX Manager クラスタ ID を取得します。
- NSX Manager ノードをクラスタに追加します。

注： 参加コマンドは、新しく展開した NSX Manager ノードに実行する必要があります。

このとき、次の NSX Manager 情報を指定します。

- 参加させるノードのホスト名または IP アドレス
- Cluster ID
- ユーザー名

- パスワード
- 証明書サムプリント

CLI コマンドまたは API 呼び出しを使用できます。

- CLI コマンド

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username>
password <NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
```

- API 呼び出し POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster

参加とクラスタの安定化プロセスには、10 ～ 15 分かかります。

6 3 台目の NSX Manager ノードをクラスタに追加します。

手順 5 を繰り返します。

7 ホストで `get cluster status` コマンドを実行してクラスタの状態を確認します。

8 (NSX Manager UI) [システム] - [アプライアンス] - [概要] の順に選択し、クラスタの接続を確認します。

次のステップ

トランスポート ゾーンを作成します。 [スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

クラスタの仮想 IP (VIP) アドレスの設定

NSX Manager ノードにフォルト トレランスと高可用性を提供するには、NSX-T クラスタのメンバーに仮想 IP アドレス (VIP) を割り当てます。

クラスタの NSX Manager は HTTPS グループの一部になり、API 要求と UI 要求を処理します。クラスタのリーダー ノードは、API 要求と UI 要求を処理するため、クラスタの仮想 IP アドレス セットの所有権を引き継ぎます。クライアントからの API 要求と UI 要求はリーダー ノードに送信されます。

注： 仮想 IP アドレスを割り当てるときは、クラスタ内のすべての NSX Manager 仮想マシンを同じサブネットに設定する必要があります。

仮想 IP アドレスを所有するリーダー ノードが使用不能になった場合、NSX-T が新しいリーダーを選択します。新しいリーダーが仮想 IP アドレスを所有します。Gratuitous ARP パケットを送信し、新しい仮想 IP アドレスと MAC アドレスのマッピングをアドバタイズします。新しいリーダー ノードが選択されると、新しい API 要求と UI 要求が新しいリーダー ノードに送信されます。

クラスタの新しいリーダー ノードへの仮想 IP アドレスのフェイルオーバーが機能するまでに数分かかる場合があります。前のリーダー ノードが使用不能になったことが原因で新しいリーダー ノードに仮想 IP アドレスがフェイルオーバーする場合、API 要求が新しいリーダー ノードに送信されるように、認証情報の再認証を行います。

注： VIP はロード バランサとして機能するように設計されていません。このため、[システム] - [ユーザー] - [設定] で vIDM [外部ロード バランサ統合] を有効にしている場合、VIP を使用することはできません。vIDM から外部ロード バランサを使用する場合は、VIP を設定しないでください。詳細については、『NSX-T Data Center 管理ガイド』の [VMware Identity Manager Integration の設定](#) を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] > [概要] の順に移動します。
- 3 [仮想 IP アドレス] フィールドで、[編集] をクリックします。
- 4 クラスタの仮想 IP アドレスを入力します。仮想 IP アドレスが他の管理ノードと同じサブネットに属していることを確認します。
- 5 [保存] をクリックします。
- 6 HTTPS グループのクラスタ状態と API リーダーを確認するには、NSX Manager コンソールまたは SSH 経由で NSX Manager CLI コマンド `get cluster status verbose` を入力します。

次に出力の例を示します。太字の部分がリーダーです。

```
Group Type: HTTPS
Group Status: STABLE

Members:
  UUID                                FQDN                                IP
STATUS
  cdb93642-ccba-fdf4-8819-90bf018cd727  nsx-manager                        192.196.197.84
UP
  51a13642-929b-8dfc-3455-109e6cc2a7ae  nsx-manager                        192.196.198.156
UP
  d0de3642-d03f-c909-9cca-312fd22e486b  nsx-manager                        192.196.198.54
UP

Leaders:
  SERVICE                                LEADER
LEASE VERSION
  api                                cdb93642-ccba-fdf4-8819-90bf018cd727  8
```

- 7 仮想 IP アドレスのトラブルシューティングを行うには、NSX Manager CLI で `/var/log/proxy/reverse-proxy.log` にあるリバース プロキシ ログと `/var/log/cbm/cbm.log` にあるクラスタ マネージャ ログを確認します。

結果

NSX-T への API 要求は、リーダー ノードが所有するクラスタの仮想 IP アドレスにリダイレクトされます。その後、リーダー ノードがアプライアンスの他のコンポーネントに要求を転送します。

NSX-T アプライアンスでのスナップショットの無効化

仮想マシンとして、スナップショットを作成して保存するように NSX Manager と NSX Edge が設定されている場合があります。ただし、NSX-T アプライアンスのクローンとスナップショットはサポートされていないため、誤動作や他の問題が発生する可能性があります。このため、NSX-T アプライアンス仮想マシンでスナップショットを無効にすることを強くおすすめします。

各 NSX-T アプライアンス仮想マシンで次の手順を実行します。

手順

- 1 vSphere Client でアプライアンス仮想マシンを探します。
- 2 仮想マシンをパワーオフします。
- 3 仮想マシンを右クリックして、[設定の編集] を選択します。
- 4 [仮想マシン オプション] タブをクリックし、[詳細] を展開します。
- 5 [設定パラメータ] フィールドで、[設定の編集...] をクリックします。
- 6 [設定パラメータ] ウィンドウで、[設定パラメータの追加] をクリックします。
- 7 次のように入力します。
 - 名前に **snapshot.MaxSnapshots** を入力します。
 - 値に **-0** を入力します。
- 8 [[OK]] をクリックして変更内容を保存します。
- 9 仮想マシンを再度パワーオンします。

KVM への NSX-T Data Center のインストール

6

NSX-T Data Center では、KVM をホスト トランスポート ノードと NSX Manager のホストの、2 つの方法でサポートしています。

KVM のサポートされているバージョンがあることを確認します。[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#) を参照してください。

この章には、次のトピックが含まれています。

- KVM のセットアップ
- KVM CLI を使用したゲスト仮想マシンの管理
- KVM への NSX Manager のインストール
- 新しく作成された NSX Manager にログインする
- KVM ホストへのサードパーティ製パッケージのインストール
- RHEL KVM ホストの Open vSwitch のバージョンを確認する
- SUSE KVM ホストの Open vSwitch バージョンの確認
- クラスタを構成する NSX Manager ノードを CLI を使用して展開

KVM のセットアップ

KVM をトランスポート ノードまたは NSX Manager ゲスト仮想マシンのホストとして使用する場合で、KVM のセットアップが完了していない場合は、次の手順を実行します。

注： Geneve カプセル化プロトコルは UDP ポート 6081 を使用します。KVM ホストのファイアウォールで、このポートへのアクセスを許可する必要があります。

手順

- 1 (RHEL のみ) /etc/yum.conf ファイルを開きます。
- 2 「exclude」行を検索します。
- 3 「"kernel* redhat-release*"」行を追加し、サポートされていない RHEL のアップグレードが回避されるように YUM を構成します。

```
exclude=[existing list] kernel* redhat-release*
```

特定の互換性要件を持つ NSX-T Data Center コンテナ プラグインを実行することがある場合は、コンテナ関連のモジュールも除外します。

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-*
docker-*
```

サポートされている RHEL のバージョンは 7.4 および 7.5 です。

4 KVM とブリッジ ユーティリティをインストールします。

Linux ディストリビューション	コマンド
Ubuntu	<pre>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge- utils virtinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL または CentOS Linux	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>
SUSE Linux Enterprise Server	YaSt を起動し、[Virtualization (仮想化)] - [Install Hypervisor and Tools (ハイパーバイザーとツールのインストール)] の順に選択します。 YaSt では、ネットワーク ブリッジを自動的に有効にして設定できます。

5 NSX Manager が KVM ホストに NSX ソフトウェア パッケージを自動的にインストールできるように、アップリンク/データ インターフェイスのネットワーク構成を準備します。

KVM ホストには複数のネットワーク インターフェイスを定義できます。NSX-T でアップリンク インターフェイス (データ インターフェイス) として提供するネットワーク インターフェイスの場合は、ネットワーク構成ファイルを正しく設定することが重要です。NSX-T は、これらのネットワーク構成ファイルを参照し、NSX-T 固有のネットワーク デバイスを作成します。Ubuntu の場合、`/etc/network/interfaces` ファイルにデータを使用します。RHEL、CentOS、SUSE の場合は、`/etc/sysconfig/network-scripts/ifcfg-$uplinkdevice` ファイルを使用します。

次の例で、インターフェイス「ens32」がアップリンク デバイス (データ インターフェイス) です。このインターフェイスでは、導入環境に応じて DHCP または固定 IP アドレス設定を使用します。

注： インターフェイス名は環境によって異なる場合があります。

重要： Ubuntu の場合、すべてのネットワーク構成を `/etc/network/interfaces` で指定する必要があります。`/etc/network/ifcfg-eth1` など、ネットワーク構成ファイルを個別に作成しないでください。トランスポート ノードが作成できなくなる可能性があります。

Linux ディストリビューション	ネットワーク構成
Ubuntu	<p data-bbox="405 260 922 281">/etc/network/interfaces を次のように編集します。</p> <pre data-bbox="421 310 716 438"> auto eth0 iface eth0 inet manual auto ens32 iface ens32 inet manual </pre>
RHEL または CentOS Linux	<p data-bbox="405 487 1241 508">/etc/sysconfig/network-scripts/ifcfg-ens32 ファイルを次のように編集します。</p> <pre data-bbox="421 537 703 747"> DEVICE="ens32" TYPE="Ethernet" NAME="ens32" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" </pre>
SUSE Linux Enterprise Server	<p data-bbox="405 793 1369 890">SLES ホストがすでに存在する場合は、そのホストでデータ インターフェイスが設定済みかどうか確認します。構成済みの SLES ホストがない場合は、管理とデータ インターフェイスのリファレンス構成を参照してください。次のように、/etc/sysconfig/network/ifcfg-ens32 ファイルを編集します。</p> <pre data-bbox="421 928 639 1083"> DEVICE="ens32" NAME="ens32" UUID="<UUID>" BOOTPROTO="none" LLADDR="<HWADDR>" STARTMODE="yes" </pre>

- 6 コマンド `systemctl restart network` でネットワーク サービスを再開するか、Linux サーバを再起動してネットワークの変更を有効にします。
- 7 KVM ホストをトランスポート ノードとして設定すると、NSX-T により、ブリッジ インターフェイス `nsx-vtep0.0` が自動的に作成されます。

Ubuntu の場合、/etc/network/interfaces ファイルに次のようなエントリが追加されます。

```

iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up

```

RHEL の場合、ホスト NSX Agent (nsxa) によって `ifcfg-nsx-vtep0.0` という構成ファイルが作成され、次のようなエントリが追加されます。

```

DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>

```

```
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

SUSE の場合:

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=255.255.255.0
IPADDR=192.168.13.119
MACADDR=ae:9d:b7:ca:20:4a
MTU=1600
USERCTL=no
STARTMODE=auto
```

- 8 サイズベースのポリシーではなく、時間ベースのポリシーとして、Syslog ローターション ポリシーを構成します。サイズベースの Syslog ローターション ポリシーでは、生成されるログ ファイルのサイズが非常に大きくなる場合があります。

KVM CLI を使用したゲスト仮想マシンの管理

NSX Manager は、KVM 仮想マシンとしてインストールできます。また、KVM を NSX-T Data Center トランスポート ノードのハイパーバイザーとして使用することもできます。

KVM のゲスト仮想マシンの管理は、このガイドの対象範囲外です。ここでは簡単な KVM CLI コマンドを紹介します。

KVM CLI でゲスト仮想マシンを管理するには、`virsh` コマンドを使用します。一般的な `virsh` コマンドをいくつか示します。詳細については、KVM のドキュメントを参照してください。

```
# List running
virsh list

# List all
virsh list --all

# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```


Linux CLI では、`ifconfig` コマンドが、ゲスト仮想マシン用に作成されたインターフェイスを表す `vnetX` インターフェイスを表示します。ゲスト仮想マシンを追加すると、`vnetX` インターフェイスが追加されます。

```
ifconfig
...

[vnet0]      Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
            inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
            TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:500
            RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

KVM への NSX Manager のインストール

NSX Manager は、KVM ホストに仮想アプライアンスとしてインストールできます。

QCOW2 のインストール手順では、`guestfish` という Linux のコマンドライン ツールを使用して、仮想マシンの設定を QCOW2 ファイルに書き込みます。

前提条件

- KVM が構成されていること。[KVM のセットアップ](#) を参照してください。
- QCOW2 イメージを KVM ホストに展開する権限。
- インストール後にログインできるように、`guestinfo` のパスワードがパスワードの強度の要件に準拠していることを確認します。[4 章 NSX Manager のインストール](#) を参照してください。
- NSX Manager のリソース要件について理解しておく必要があります。[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#) を参照してください。
- Ubuntu OS のインストールを計画している場合は、KVM ホストに NSX Manager をインストールする前に Ubuntu バージョン 18.04 をインストールすることをおすすめします。

手順

- 1 `[nsx-unified-appliance] - [exports] - [kvm]` フォルダから NSX Manager QCOW2 イメージをダウンロードします。
- 2 `scp` によるファイル転送または同期を使用して NSX Manager が実行されている KVM マシンにコピーします。
- 3 (Ubuntu のみ) 現在ログインしているユーザーを `libvirtd` ユーザーとして追加します。

```
adduser $USER libvirtd
```

- 4 QCOW2 イメージを保存したディレクトリに `guestinfo.xml` というファイルを作成し、NSX Manager 仮想マシンのプロパティを入力します。

プロパティ	説明
<ul style="list-style-type: none"> ■ <code>nsx_cli_passwd_0</code> ■ <code>nsx_cli_audit_passwd_0</code> ■ <code>nsx_passwd_0</code> 	<p>パスワード強度の基準に準拠したパスワードを使用する必要があります。</p> <ul style="list-style-type: none"> ■ 12 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の大文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 5 文字以上の異なる文字 ■ 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。 <ul style="list-style-type: none"> ■ <code>retry=3</code>: 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。 ■ <code>minlen=12</code>: 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。 ■ <code>difok=0</code>: 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。difok に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。 ■ <code>lcredit=1</code>: 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>ucredit=1</code>: 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>dcredit=1</code>: 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の minlen 値に合わせるため、それぞれの数字が +1 とカウントされます。 ■ <code>ocredit=1</code>: 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の minlen 値に合わせるため、それぞれの文字が +1 とカウントされます。 ■ <code>enforce_for_root</code>: root ユーザーに設定されるパスワード。 <p>注: Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、man ページを参照してください。</p> <p>たとえば、単純で体系的なパスワードの使用は避けます。たとえば、VMware123! 123、VMware12345 などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、VMware123! 45、VMware1! 2345、VMware@1az23x などです。</p>
<code>nsx_hostname</code>	NSX Manager のホスト名を入力します。ホスト名は、有効なドメイン名にする必要があります。ドットで区切られたホスト名（ドメイン/サブドメイン）の各部分は、英字で始まっている必要があります。

プロパティ	説明
nsx_role	<ul style="list-style-type: none"> ■ <i>nsx-manager</i>: 必須。このロール名は NSX Manager アプライアンスをインストールします。 ■ <i>nsx-cloud-service-manager</i>: オプション。NSX Manager をインストールした後、このロール名を使用して NSX Cloud の Cloud Service Manager アプライアンスをインストールします。
nsx_isSSHEnabled	このプロパティを有効または無効にすることができます。有効になっている場合は、SSH を使用して NSX Manager にログインできます。
nsx_allowSSHRootLogin	このプロパティを有効または無効にすることができます。有効になっている場合は、root ユーザーとして SSH を使用して NSX Manager にログインできます。このプロパティを使用できるようにするには、 <i>nsx_isSSHEnabled</i> を有効にする必要があります。
<ul style="list-style-type: none"> ■ nsx_dns1_0 ■ nsx_ntp_0 ■ nsx_domain_0 ■ nsx_gateway_0 ■ nsx_netmask_0 ■ nsx_ip_0 	デフォルト ゲートウェイの IP アドレス、管理ネットワークの IPv4、管理ネットワークのネットマスク、DNS、NTP の IP アドレスを入力します。

次はその例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0"/>
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
  </PropertySection>
</Environment>
```

注： この例では、*nsx_isSSHEnabled* と *nsx_allowSSHRootLogin* がいずれも有効になっています。無効になっている場合、NSX Manager のコマンドラインへの SSH 接続やログインはできません。

nsx_isSSHEnabled を有効にして、*nsx_allowSSHRootLogin* を有効にしなかった場合、NSX Manager に SSH で接続することはできますが、root でログインすることはできません。

- 5 guestfish を使用して guestinfo.xml ファイルを QCOW2 イメージに書き込みます。

注： guestinfo の情報を QCOW2 イメージに書き込んだ後、情報を上書きすることはできません。

```
sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /
config/guestinfo
```

- 6 virt-install コマンドで QCOW2 イメージを展開します。

仮想 CPU と RAM の値は、大規模な仮想マシンに適しています。ネットワーク名とポートグループ名は環境によって異なります。モデルは virtio にする必要があります。

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole \
--cpu mode=host-passthrough,cache.mode=passthrough

Starting install...
Domain installation still in progress. Waiting for installation to complete.
```

- 7 NSX Manager が展開されていることを確認します。

```
virsh list --all

Id      Name                State
-----
18      nsx-manager1        running
```

- 8 NSX Manager コンソールを開いてログインします。

```
virsh console 18
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login: admin
Password:
```

- 9 ノードが起動した後、admin として CLI にログインし、get interface eth0 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。

- 10 get services を実行してサービスが実行されていることを確認します。

- 11 NSX Manager または グローバル マネージャ ノードに必要な接続があることを確認します。

次のタスクを実行できることを確認します。

- 別のマシンからノードに ping を実行します。

- ノードは、デフォルト ゲートウェイに ping を実行できます。
- ノードは、管理インターフェイスを使用して、同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- ノードは、DNS サーバと NTP サーバに ping を実行できます。
- SSH を有効にした場合は、SSH を使用してノードに接続できることを確認します。

接続が確立されていない場合は、仮想アプライアンスのネットワーク アダプタが適切なネットワークまたは VLAN に配置されていることを確認します。

12 KVM コンソールを終了します。

```
control-]
```

13 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。

新しく作成された NSX Manager にログインする

NSX Manager をインストールした後は、ユーザー インターフェイスを使用して、その他のインストール タスクを実行できます。

NSX Manager をインストールしたら、NSX-T Data Center のカスタマー エクスペリエンス向上プログラム (CEIP) に参加できます。プログラムへの参加または参加を後で中止する方法については、『NSX-T Data Center 管理ガイド』の NSX のカスタマー エクスペリエンス向上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 がインストールされていることを確認します。[NSX Manager および利用可能なアプライアンスのインストール](#) を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
エンド ユーザー使用許諾契約書 (EULA) が表示されます。
- 2 エンド ユーザー使用許諾契約書 (EULA) を読んで同意します。
- 3 VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加するかどうかを選択します。
- 4 [保存] をクリックします。

KVM ホストへのサードパーティ製パッケージのインストール

KVM ホストをファブリック ノードにする準備を整えるには、いくつかのサードパーティ製パッケージをインストールする必要があります。

前提条件

- (RHEL と CentOS Linux) サードパーティ製のパッケージをインストールする前に、次のコマンドを実行して仮想化パッケージをインストールします。

```
yum groupinstall "Virtualization Hypervisor"
yum groupinstall "Virtualization Client"
yum groupinstall "Virtualization Platform"
yum groupinstall "Virtualization Tools"
```

パッケージをインストールできない場合は、新しいインストール環境にコマンド `yum install glibc.i686 nspr` を使用して手動でインストールできます。

- (Ubuntu) サードパーティ製のパッケージをインストールする前に、次のコマンドを実行して仮想化パッケージをインストールします。

```
apt install -y \
qemu-kvm \
libvirt-bin \
virtinst \
virt-manager \
virt-viewer \
ubuntu-vm-builder \
bridge-utils
```

- (SUSE Linux Enterprise Server) サードパーティ製のパッケージをインストールする前に、次のコマンドを実行して仮想化パッケージをインストールします。

```
libcap-progs
```

手順

- ◆ Ubuntu 18.04.2 LTS では、`apt-get install <package_name>` を実行して、以下のサードパーティ製パッケージを手動でインストールします。

```
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
dkms
libc6-dev
libelf-dev
```

- ◆ RHEL と CentOS Linux では、`yum install <package_name>` を実行してサードパーティ製パッケージを手動でインストールします。

すでに RHEL または CentOS に登録されているホストを手動で準備する場合は、ホストにサードパーティ製パッケージをインストールする必要はありません。

RHEL 7.6、7.5、および 7.4 CentOS Linux 7.5 および 7.4

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
net-tools
```

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
```

- ◆ SUSE では、`zypper install <package_name>` を実行してサードパーティ製パッケージを手動でインストールします。

SUSE Linux Enterprise Server 12.0

```
python-simplejson
python-PyYAML
python-netaddr
lsb-release
```

RHEL KVM ホストの Open vSwitch のバージョンを確認する

RHEL ホストに OVS パッケージがない場合は、このトピックをスキップしてください。RHEL ホストに OVS パッケージがすでに存在する場合は、既存の OVS パッケージを削除して、NSX-T でサポートされている OVS パッケージをインストールするか、既存の OVS パッケージを NSX-T でサポートされているパッケージにアップグレードする必要があります。

Open vSwitch のサポート対象のバージョンは 2.9.1.8614397-1 です。

手順

- 1 ホストにインストールされている Open vSwitch の現在のバージョンを確認します。

```
ovs-vswitchd --version
```

重要: 既存の Open vSwitch パッケージが最新バージョンまたはそれ以前のバージョンの場合、既存の Open vSwitch パッケージをサポート対象のバージョンに置き換える必要があります。

- 2 次の Open vSwitch パッケージを削除します。
 - `kmod-openvswitch` または `openvswitch-kmod`
 - `openvswitch`
 - `openvswitch-selinux-policy`
- 3 または、NSX-T Data Center に必要な Open vSwitch パッケージにアップグレードします。
 - a 管理者としてホストにログインします。
 - b `nsx-lcp` ファイルをダウンロードし、`/tmp` ディレクトリにコピーします。

- c パッケージを解凍します。

```
tar -zxvf nsx-lcp-<release>-rhel75_x86_64.tar.gz
```

- d パッケージ ディレクトリに移動します。

```
cd nsx-lcp-rhel75_x86_64/
```

- e Open vSwitch の既存のバージョンをサポート対象のバージョンに置き換えます。

- 新しいバージョンの Open vSwitch が使用されている場合は、`--nodeps` コマンドを使用します。

```
rpm -Uvh openvswitch*.rpm --nodeps
```

- 以前のバージョンの Open vSwitch が使用されている場合は、`--force` コマンドを使用します。

```
rpm -Uvh openvswitch*.rpm --nodeps --force
```

SUSE KVM ホストの Open vSwitch バージョンの確認

SUSE ホストに OVS パッケージがない場合は、このトピックをスキップしてください。SUSE ホストに OVS パッケージが存在する場合は、既存の OVS パッケージを削除して、NSX-T でサポートされている OVS パッケージをインストールするか、既存の OVS パッケージを NSX-T でサポートされているパッケージにアップグレードする必要があります。

Open vSwitch のサポート対象のバージョンは 2.9.1.8614397-1 です。

手順

- 1 ホストにインストールされている Open vSwitch の現在のバージョンを確認します。

```
ovs-vswitchd --version
```

重要: 既存の Open vSwitch パッケージが最新バージョンまたはそれ以前のバージョンの場合、既存の Open vSwitch パッケージをサポート対象のバージョンに置き換える必要があります。

- 2 次の Open vSwitch パッケージを削除します。

- `kmod-openvswitch` または `openvswitch-kmod`
- `openvswitch`
- `openvswitch-selinux-policy`

- 3 または、NSX-T Data Center に必要な Open vSwitch パッケージにアップグレードします。

- a 管理者としてホストにログインします。
- b `nsx-lcp` ファイルをダウンロードし、`/tmp` ディレクトリにコピーします。
- c パッケージを解凍します。

```
nsx-lcp-3.0.0.0.0.14335404-linux64-sles12sp3.tar.gz
```


- d パッケージ ディレクトリに移動します。

```
nsx-lcp-linux64-sles12sp3/
```

- e Open vSwitch の既存のバージョンをサポート対象のバージョンに置き換えます。

- 新しいバージョンの Open vSwitch が使用されている場合は、`--nodeps` コマンドを使用します。

```
rpm -Uvh openvswitch*.rpm --nodeps
```

- 以前のバージョンの Open vSwitch が使用されている場合は、`--force` コマンドを使用します。

```
rpm -Uvh openvswitch*.rpm --nodeps --force
```

クラスタを構成する NSX Manager ノードを CLI を使用して展開

CLI を使用してクラスタを構成する NSX Manager を参加させると、クラスタ内のすべての NSX Manager ノードが相互に通信できるようになります。

前提条件

NSX-T Data Center コンポーネントのインストールが完了している必要があります。

手順

- 1 最初に展開した NSX Manager ノードへの SSH セッションを開きます。
- 2 管理者の認証情報を使用してログインします。
- 3 NSX Manager ノードで `get certificate api thumbprint` コマンドを実行します。
コマンド出力は、この NSX Manager に固有の一連の数値です。
- 4 `get cluster config` コマンドを実行して最初に展開した NSX Manager クラスタ ID を取得します。
- 5 NSX Manager ノードをクラスタに追加します。

注： 参加コマンドは、新しく展開した NSX Manager ノードに実行する必要があります。

このとき、次の NSX Manager 情報を指定します。

- 参加させるノードのホスト名または IP アドレス
- Cluster ID
- ユーザー名
- パスワード
- 証明書サムプリント

CLI コマンドまたは API 呼び出しを使用できます。

- CLI コマンド

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username>
password <NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
```

- API 呼び出し `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

参加とクラスタの安定化プロセスには、10 ～ 15 分かかることがあります。

- 6 3 台目の NSX Manager ノードをクラスタに追加します。

手順 5 を繰り返します。

- 7 ホストで `get cluster status` コマンドを実行してクラスタの状態を確認します。

- 8 (NSX Manager UI) [システム] - [アプライアンス] - [概要] の順に選択し、クラスタの接続を確認します。

次のステップ

トランスポート ゾーンを作成します。 [スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

ベア メタル サーバが NSX-T Data Center を使用するように構成

7

ベア メタル サーバ上で NSX-T Data Center を使用するには、サポートされているサードパーティ製パッケージをインストールする必要があります。

NSX-T Data Center では、ベア メタル サーバをホスト トランスポート ノードと NSX Manager のホストの、2 つの方法でサポートしています。

ベア メタル サーバのサポートされているバージョンがあることを確認します。[ベア メタル サーバ システムの要件](#)を参照してください。

注： NSX Edge が仮想マシンのフォーム ファクタにあり、VLAN ベースの論理スイッチに展開された NSX DHCP サービスを使用する場合は、NSX Edge が展開されているベアメタル ホストで偽造転送オプションを [承諾] に設定する必要があります。vSphere 製品ドキュメントで「偽造転送」を参照してください。

この章には、次のトピックが含まれています。

- [ベア メタル サーバへのサードパーティ製パッケージのインストール](#)
- [ベアメタル サーバ ワークロードのアプリケーション インターフェイスの作成](#)

ベア メタル サーバへのサードパーティ製パッケージのインストール

ベア メタル サーバをファブリック ノードにする準備を整えるには、いくつかのサードパーティ製パッケージをインストールする必要があります。

前提条件

- インストールを実行するユーザーに次のアクションの実行に必要な管理権限を持っていることを確認します。この中には、`sudo` 権限を必要とするものもあります。
 - バンドルをダウンロードして解凍します。
 - `dpkg` または `rpm` コマンドを実行して、NSX コンポーネントをインストールまたはアンインストールします。
 - `nsxcli` コマンドを実行して、`join management plane` コマンドを実行します。
- 仮想化パッケージがインストールされていることを確認します。
 - Redhat または CentOS : `yum install libvirt-libs`
 - Ubuntu : `apt-get install libvirt0`

- SUSE : `zypper install libvirt-libs`

手順

- ◆ Ubuntu の場合、`apt-get install <package_name>` を実行してサードパーティ製パッケージをインストールします。

Ubuntu 18.04.2	Ubuntu 16.04
<pre>tracertoute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0 libelf-dev</pre>	<pre>libunwind8 libgflags2v5 libgoogle-perftools4 tracertoute python-mako python-simplejson python-unittest2 python-yaml python-netaddr python-openssl libboost-file-system1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0 libelf-dev</pre>

- ◆ RHEL または CentOS の場合、`yum install` を実行してサードパーティ製パッケージをインストールします。

RHEL 7.4、7.5、および 7.6	CentOS 7.4、7.5、および 7.6
tcpdump	tcpdump
boostfilesystem	boostfilesystem
PyYAML	PyYAML
boostiostreams	boostiostreams
boostchrono	boostchrono
python-mako	python-mako
python-netaddr	python-netaddr
python-six	python-six
gperftools-libs	gperftools-libs
libunwind	libunwind
libelf-dev	libelf-dev
snappy	snappy
boost-date-time	boost-date-time
c-ares	c-ares
redhat-lsb-core	redhat-lsb-core
wget	wget
net-tools	net-tools
yum-utils	yum-utils
lsof	lsof
python-gevent	python-gevent
libev	libev
python-greenlet	python-greenlet
libvirt-libs	libvirt-libs

- ◆ SUSE では、`zypper install <package_name>` を実行してサードパーティ製パッケージを手動でインストールします。

```
net-tools
tcpdump
python-simplejson
python-netaddr
python-PyYAML
python-six
libunwind
wget
lsof
libcap-progs
libvirt-libs
```

ベアメタル サーバ ワークロードのアプリケーション インターフェイスの作成

ベアメタル サーバ ワークロードのアプリケーション インターフェイスを作成または移行する前に、NSX-T Data Center を設定し、Linux サードパーティ パッケージをインストールする必要があります。

NSX-T Data Center は、Linux OS のインターフェイス ボンディングをサポートしていません。ベアメタル サーバのトランスポート ノードには、Open vSwitch (OVS) のボンディングを使用する必要があります。ナレッジベースの記事 KB67835、[Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T](#) を参照してください。

手順

- 1 必要なサードパーティ パッケージをインストールします。

[ベア メタル サーバへのサードパーティ製パッケージのインストール](#) を参照してください。

- 2 TCP および UDP ポートを設定します。

[ESXi、KVM ホスト、ベアメタル サーバで使用される TCP および UDP ポート](#) を参照してください。

- 3 ベア メタル サーバを NSX-T Data Center ファブリックに追加し、トランスポート ノードを作成します。

[スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

- 4 Ansible Playbook を使用してアプリケーション インターフェイスを作成します。

<https://github.com/vmware/bare-metal-server-integration-with-nsxt> を参照してください。

NSX Manager クラスタの要件

8

次のサブセクションでは、NSX Manager クラスタの要件と特定のサイト展開の推奨事項について説明します。また、NSX Manager ノードを実行しているホストで障害が発生したときに迅速にリカバリできるように、NSX-T Data Center で vSphere HA を使用する方法についても説明します。

この章には、次のトピックが含まれています。

- 単一サイト、デュアル サイト、複数サイトに対する NSX Manager クラスタの要件

単一サイト、デュアル サイト、複数サイトに対する NSX Manager クラスタの要件

NSX Manager クラスタの構成は、環境が単一サイト、デュアル サイト、複数サイトのいずれかによって異なります。

NSX-T Data Center で vSphere HA を使用すると、NSX Manager ノードを実行しているホストで障害が発生したときに、迅速にリカバリできます。

注： vSphere 製品ドキュメントで「vSphere HA クラスタの作成と使用」を参照してください。

クラスタ要件

- 本番環境では、管理プレーンと制御プレーンの停止を回避するため、NSX Manager クラスタに 3 つのメンバーが必要です。

クラスタ メンバーはそれぞれ固有のハイパーバイザー ホストに配置する必要があります。合計で 3 台の物理ハイパーバイザー ホストが必要です。1 台の物理ハイパーバイザー ホストの障害が NSX 制御プレーンに影響を及ぼさないようにするため、この設定が必要になります。3 つのすべてのクラスタ メンバーが異なるホストで実行されるように、非アフィニティ ルールの適用をおすすめします。

本番環境では通常、3 ノードの NSX Manager クラスタが稼動しています。ただし、一時的に NSX Manager ノードを追加して、IP アドレスを変更することができます。

重要： NSX-T Data Center 2.4 では、NSX Manager に NSX 中央制御プレーンのプロセスが含まれています。これは、NSX の処理に重要なサービスです。NSX Manager が完全に失われた場合、またはクラスタが 3 つの NSX Manager から 1 つの NSX Manager に減少した場合、環境のトポロジを変更できません。また、NSX に依存するマシンの vMotion は失敗します。

- 本番環境のワークロードを処理しないラボや事前検証 (POC) 環境の場合は、リソースを節約するため、単一の NSX Manager を実行することもできます。NSX Manager ノードは、ESXi または KVM のいずれかに展開できます。ただし、ESXi と KVM の両方にマネージャを展開することはできません。

単一サイトの要件と推奨事項

次の推奨事項は、単一サイトの NSX-T Data Center 環境に適用されます。

- 単一ホストの障害で複数のマネージャに影響を及ぼさないように、NSX Manager を異なるホストに配置することをおすすめします。
- NSX Manager 間の最大遅延は 10 ミリ秒です。
- NSX Manager は、異なる vSphere クラスタに配置することも、共通の vSphere クラスタに配置することもできます。
- NSX Manager は、異なる管理サブネットまたは共有管理サブネットに配置することをおすすめします。vSphere HA を使用する場合は、共有管理サブネットの使用をおすすめします。これにより、vSphere によってリカバリされる NSX Manager の IP アドレスが維持されます。
- また、NSX Manager を共有ストレージに配置することをおすすめします。vSphere HA を使用する場合は、そのソリューションの要件を確認してください。

また、NSX-T で vSphere HA を使用すると、NSX Manager が実行されているホストで障害が発生したときに、失われた NSX Manager をリカバリできます。

シナリオの例：

- 1 つの vSphere クラスタに、3 つの NSX Manager がすべて展開されています。
- vSphere クラスタは 4 台以上のホストから構成されます。
 - Host-01 に nsxmgr-01 を展開
 - Host-02 に nsxmgr-02 を展開
 - Host-03 に nsxmgr-03 を展開
 - Host-04 には、NSX Manager が展開されていません。
- vSphere HA は、失われた NSX Manager（たとえば、nsxmgr-01）を任意のホスト（たとえば、Host-01）から Host-04 にリカバリするように設定されています。

NSX Manager が実行されているホストが失われると、vSphere は失われた NSX Manager を Host-04 にリカバリします。

デュアル サイトの要件と推奨事項

次の推奨事項は、デュアル サイト（サイト A/サイト B）の NSX-T Data Center 環境に適用されます。

- デュアル サイトのシナリオでは、vSphere HA なしで NSX Manager を展開することは推奨されません。このシナリオでは、1 つのサイトに 2 つの NSX Manager を展開する必要があり、このサイトを失うと、NSX-T Data Center の運用に支障をきたします。

- vSphere HA を使用するデュアル サイトのシナリオで NSX Manager を展開する場合は、次の点に注意してください。
 - 1 つの拡張された vSphere クラスタに、NSX Manager のすべてのホストが含まれます。
 - 3 つの NSX Manager がすべて共通管理サブネット/VLAN に展開され、失われた NSX Manager のリカバリ時に IP アドレスが維持されます。
 - サイト間の遅延については、ストレージ製品の要件を参照してください。

シナリオの例：

- 1 つの vSphere クラスタに、3 つの NSX Manager がすべて展開されています。
- vSphere クラスタは 6 台以上のホストで構成され、サイト A とサイト B はそれぞれ 3 台のホストで構成されます。
- 3 つの NSX Manager はそれぞれ別のホストに展開され、リカバリされた NSX Manager の配置でホストが追加されます。

サイト A：

- Host-01 に nsxmgr-01 を展開
- Host-02 に nsxmgr-02 を展開
- Host-03 に nsxmgr-03 を展開

サイト B：

- Host-04 には、NSX Manager が展開されていません。
- Host-05 には、NSX Manager が展開されていません。
- Host-06 には、NSX Manager が展開されていません。
- vSphere HA は、失われた NSX Manager（たとえば、nsxmgr-01）をサイト A の任意のホスト（たとえば、Host-01）からサイト B のいずれかのホストにリカバリするように設定されています。

サイト A で障害が発生すると、vSphere HA はすべての NSX Manager をサイト B のホストにリカバリします。

重要： NSX Manager が同じ共通ホストにリカバリされないように、非アフィニティ ルールを適切に構成する必要があります。

複数（3 つ以上）のサイトの要件と推奨事項

次の推奨事項は、複数サイト（サイト A/サイト B/サイト C）の NSX-T Data Center 環境に適用されます。

3 つ以上のサイトがあるシナリオでは、NSX Manager HA の有無に関わらず vSphere を展開できます。

vSphere HA なしで展開する場合：

- サイトごとに別の管理サブネットまたは VLAN を使用することをおすすめします。
- NSX Manager 間の最大遅延は 10 ミリ秒です。

シナリオの例（3 つのサイト）：

- 3 つの vSphere クラスター（サイトごとに 1 つずつ）。
- NSX Manager を実行しているサイトごとに 1 つ以上のホスト：
 - Host-01 に nsxmgr-01 を展開
 - Host-02 に nsxmgr-02 を展開
 - Host-03 に nsxmgr-03 を展開

障害のシナリオ：

- 単一サイトの障害：他のサイトの残り 2 つの NSX Manager が処理を継続します。NSX-T Data Center は状態が低下していますが、まだ動作しています。3 つ目の NSX Manager を手動で展開し、失われたクラスターメンバーを置き換えることをおすすめします。
- 2 つのサイトの障害：クォーラムが失われるため、NSX-T Data Center の処理に影響を及ぼします。

CPU 速度、ディスク パフォーマンス、その他の展開要因など、環境の条件によっては、NSX Manager のリカバリに 20 分ほどかかる場合があります。

NSX Edge のインストール

9

NSX-T ユーザー インターフェイス、vSphere Web Client またはコマンドライン OVF ツールを使用して、ESXi に NSX Edge をインストールします。

この章には、次のトピックが含まれています。

- NSX Edge のインストール要件
- NSX Edge のネットワーク設定
- NSX Edge のインストール方法
- NSX Edge トランスポート ノードの作成
- NSX Edge クラスタの作成
- vSphere の GUI を使用した ESXi への NSX Edge のインストール
- ベア メタルへの NSX Edge のインストール
- NSX Edge の管理プレーンへの追加
- トランスポート ノードとしての NSX Edge の設定

NSX Edge のインストール要件

NSX Edge は、ルーティング サービスと NSX-T Data Center 環境の外部にあるネットワーク NSX Edge との接続を提供します。ネットワーク アドレス変換 (NAT) や VPN などのステートフル サービスで Tier-0 ルーターまたは Tier-1 ルーターを展開する場合は、NSX Edge が必要です。

注： 1 台の NSX Edge ノードで使用できる Tier-0 ルーターは 1 つだけです。ただし、1 台の NSX Edge ノードに複数の Tier-1 論理ルーターをホストできます。同じクラスタ内でサイズが異なる NSX Edge 仮想マシンを組み合わせることができますが、これは推奨されません。

表 9-1. NSX Edge の展開、プラットフォームおよびインストール要件

要件	説明
サポートされる展開方法	<ul style="list-style-type: none">■ OVA/OVF■ PXE を使用した ISO■ PXE を使用しない ISO
サポート対象のプラットフォーム	NSX Edge は、ESXi またはベア メタルでのみサポートされます。 NSX Edge は KVM ではサポートされていません。

表 9-1. NSX Edge の展開、プラットフォームおよびインストール要件（続き）

要件	説明
PXE インストール	root ユーザーと admin ユーザーのパスワード文字列は、sha-512 アルゴリズムで暗号化する必要があります。
NSX-T Data Center アプライアンスのパスワード	<ul style="list-style-type: none"> ■ 12 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の大文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 5 文字以上の異なる文字 ■ 辞書に登録されている単語が使われていない ■ パリンドローム（回文）になっていない ■ 使用できるモノトニックな文字シーケンスは 4 つ以下です。
ホスト名	NSX Edge をインストールするときに、アンダースコアなどの無効な文字を含まないホスト名を指定します。ホスト名に無効な文字が含まれていると、展開後にホスト名が localhost に設定されます。ホスト名の制限の詳細については、 https://tools.ietf.org/html/rfc952 および https://tools.ietf.org/html/rfc1123 を参照してください。
VMware Tools	ESXi で実行される NSX Edge 仮想マシンには、VMware Tools がインストールされています。VMware Tools を削除またはアップグレードしないでください。
システム	システム要件を満たしていることを確認します。 NSX Edge 仮想マシンのシステム要件 を参照してください。
ポート	必要なポートが開いていることを確認します。 ポートとプロトコル を参照してください。
IP アドレス	<p>複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。</p> <p>NSX Edge IPv4 または IPv6 IP アドレス設定スキームを計画します。</p>
OVF テンプレート	<ul style="list-style-type: none"> ■ ESXi ホストに OVF テンプレートを展開するために必要な権限があることを確認します。 ■ ホスト名にアンダースコアが含まれていないことを確認します。含まれている場合、ホスト名が localhost に設定されます。 ■ OVF テンプレートを展開できる管理ツールが必要です（vCenter Server や vSphere Client など）。 <p>手動で構成するには、OVF 展開ツールで構成オプションがサポートされている必要があります。</p> <ul style="list-style-type: none"> ■ 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。
NTP サーバ	Edge クラスタ内のすべての NSX Edge 仮想マシンまたはベアメタル Edge で同じ NTP サーバを設定する必要があります。

Intel ベースのチップセット

NSX Edge ノードは、Intel ベースのチップセットを搭載した ESXi ベースのホストでのみサポートされます。それ以外の場合に vSphere EVC モードを使用すると、Edge ノードが起動せず、コンソールにエラー メッセージが表示されることがあります。

vSphere ビジネス継続性機能の NSX Edge サポート

NSX-T Data Center 2.5.1 から、NSX Edge ノードで vMotion、DRS および vSphere HA がサポートされます。

NSX Edge のインストール シナリオ

重要： vSphere Web Client またはコマンド ラインのいずれかを使用して OVA または OVF ファイルから NSX Edge をインストールすると、仮想マシンがパワーオン状態になるまで、ユーザー名、パスワード、IP アドレスなどの OVA/OVF プロパティ値が検証されません。

- **admin** または **audit** ユーザーのユーザー名を指定する場合には、一意の名前を使用する必要があります。同じ名前を指定すると、名前が無視され、デフォルトの名前 (**admin** または **audit**) が使用されます。
- **admin** ユーザーのパスワードが要件を満たしていない場合には、SSH またはコンソール経由で **admin** ユーザーとして NSX Edge にログインする必要があります。ログイン パスワードは **default** です。プロンプトが表示され、パスワードの変更が指示されます。
- **audit** ユーザーのパスワードが要件を満たしていない場合、ユーザー アカウントは無効になります。アカウントを有効にするには、**admin** ユーザーとして SSH またはコンソール経由で NSX Edge にログインし、**set user audit** コマンドを実行して **audit** ユーザーのパスワードを設定します（現在のパスワードは空の文字列です）。
- **root** ユーザーのパスワード要件を満たしていない場合には、**root** として SSH またはコンソール経由で NSX Edge にログインする必要があります。ログイン パスワードは **vmware** です。プロンプトが表示され、パスワードの変更が指示されます。

注意： **root** ユーザー認証情報を使用してログインしている際に NSX-T Data Center に変更を加えると、システム障害が発生し、ネットワークに影響する可能性があります。**root** ユーザー認証情報を使用して変更を加えるのは、VMware のサポート チームから指示があった場合のみにすることをお勧めします。

注： 要件を満たすパスワードが設定されるまで、コア サービスはアプライアンスで起動しません。

NSX Edge を OVA ファイルから展開した後は、仮想マシンをパワーオフして vCenter Server から OVA 設定を変更し、仮想マシンの IP アドレス設定を変更することはできません。

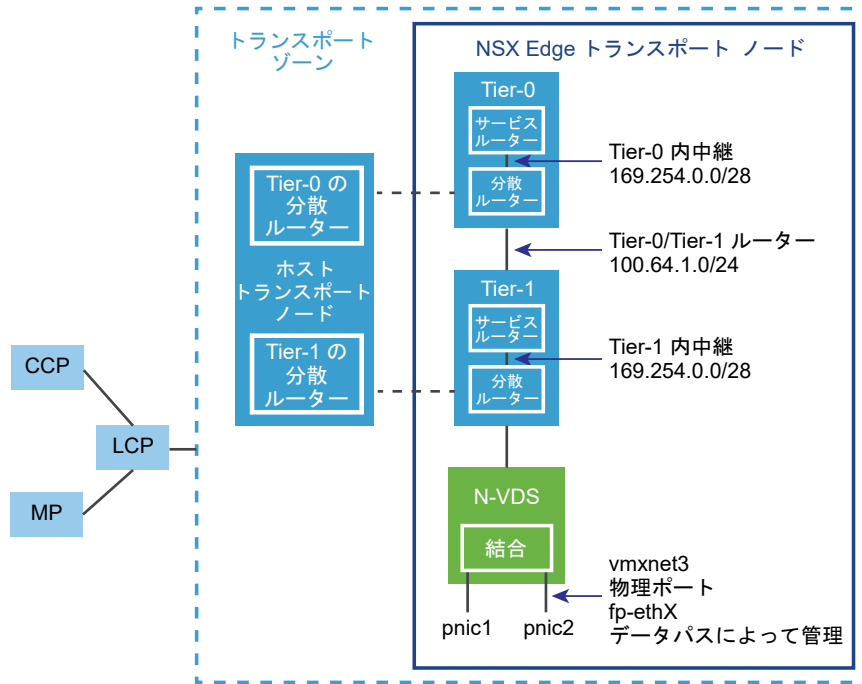
NSX Edge のネットワーク設定

NSX Edge は、ISO、OVA/OVF、または PXE を起動してインストールできます。いずれのインストール方法でも、NSX Edge をインストールする前にホスト ネットワークの準備ができていることを確認します。

トランスポート ゾーンにおける NSX Edge の概要図

NSX-T Data Center の概要図には、トランスポート ゾーンに 2 台のトランスポート ノードがあります。1 台のトランスポート ノードはホストです。もう 1 台は NSX Edge です。

図 9-1. NSX Edge の概要



展開直後の NSX Edge は、空のコンテナと考えることができます。論理ルーターを作成するまで、NSX Edge は何も行いません。NSX Edge は、Tier-0 と Tier-1 の論理ルーターの処理をバックアップします。各論理ルーターにはサービス ルーター (SR) と分散ルーター (DR) が含まれます。ルーターの分散とは、同じトランスポート ゾーンに属するすべてのトランスポート ノードにルーターを複製することです。この図では、ホスト トランスポート ノードに、Tier-0 および Tier-1 と同じ分散ルーターが含まれています。サービス ルーターは、NAT などのサービスを実行するように論理ルーターを設定する場合に必要です。Tier-0 の論理ルーターにはすべてサービス ルーターがあります。Tier-1 のルーターには、設計上の検討事項に基づいて必要な場合にサービス ルーターを設定できます。

デフォルトでは、サービス ルーターと分散ルーター間のリンクは 169.254.0.0/28 サブネットを使用します。これらのルーター内の中継リンクは、Tier-0 または Tier-1 の論理ルーターの展開時に自動的に作成されます。環境内で 169.254.0.0/28 サブネットが使用中ではない限り、リンクを設定あるいは変更する必要はありません。Tier-1 の論理ルーターでは、この論理ルーターの作成時に NSX Edge クラスタを選択した場合にのみ SR があります。

Tier-0 から Tier-1 の接続に割り当てられるデフォルトのアドレス空間は 100.64.0.0/10 です。Tier-0 から Tier-1 の各ピア接続には、100.64.0.0/10 アドレス空間内で /31 サブネットが提供されます。このリンクは、Tier-1 ルーターを作成し、Tier-0 ルーターに接続するときに自動的に作成されます。環境内で 100.64.0.0/10 サブネットが使用中ではない限り、このリンクのインターフェイスを設定または変更する必要はありません。

NSX-T Data Center 環境には、それぞれ管理プレーン クラスタ (MP) と制御プレーン クラスタ (CCP) があります。管理プレーン クラスタと制御プレーン クラスタは、各トランスポート ゾーンのローカル制御プレーン (LCP) に設定をプッシュします。ホストまたは NSX Edge が管理プレーンに加わると、管理プレーン エージェント (MPA) がホストまたは NSX Edge と接続を確立し、ホストまたは NSX Edge が NSX-T Data Center のファブリック ノードになります。その後、ファブリック ノードがトランスポート ノードとして追加されると、ホストまたは NSX Edge との LCP 接続が確立されます。

この図は、高可用性を提供するために結合された 2 つの物理 NIC (pNIC1 と pNIC2) の例を示しています。物理 NIC はデータベースで管理されます。これらは、外部ネットワークへの VLAN アップリンクとして、または内部の NSX-T Data Center で管理された仮想マシン ネットワークへのトンネル エンドポイントとして機能します。

ベスト プラクティスは、仮想マシンとして展開されている各 NSX Edge に 2 つ以上の物理リンクを割り当てることです。任意で、同じ pNIC のポート グループを、異なる VLAN ID を使用して重複させることができます。最初に見つかったネットワーク リンクが管理に使用されます。たとえば、NSX Edge 仮想マシンでは、vnic1 が最初に見つかったリンクだとします。ベア メタル インストールでは、eth0 または em0 が最初に見つかる場合があります。残りのリンクは、アップリンクやトンネルに使用されます。たとえば、1 つは、NSX-T Data Center によって管理されている仮想マシンのトンネル エンドポイントとして使用できます。もう 1 つは NSX Edge から外部 ToR へのアップリンクに使用できます。

管理者として CLI にログインし、コマンド `get interfaces` および `get physical-ports` を実行することによって、NSX Edge の物理リンク情報を表示できます。API では、`GET fabric/nodes/<edge-node-id>/network/interfaces` API 呼び出しを使用できます。物理リンクの詳細については、次のセクションを参照してください。

NSX Edge を仮想マシン アプライアンスとしてインストールするか、ベア メタルにインストールするかにかかわらず、ネットワーク設定には複数のオプションがあります。

トランスポート ゾーンと N-VDS

NSX Edge のネットワークを理解するには、トランスポート ゾーンと N-VDS についての知識が必要です。トランスポート ゾーンは NSX-T Data Center におけるレイヤー 2 ネットワークの到達範囲を制御します。N-VDS は、トランスポート ノードに作成されるソフトウェア スイッチです。N-VDS は、論理ルーターのアップリンクとダウンリンクを物理 NIC にバインドします。NSX Edge が属するトランスポート ゾーンごとに、NSX Edge に個別の N-VDS がインストールされます。

トランスポート ゾーンには次の 2 種類があります。

- トランスポート ノード間の内部 NSX-T Data Center トンネル用のオーバーレイ
- NSX-T Data Center 外部のアップリンク用 VLAN

NSX Edge はゼロ個の VLAN トランスポート ゾーンまたは多数のトランスポート ゾーンに属することができます。VLAN トランスポート ゾーンが 0 個の場合も、NSX Edge でアップリンクを使用できます。NSX Edge のアップリンクは、オーバーレイ トランスポート ゾーン用にインストールされている N-VDS を使用できるためです。各 NSX Edge に N-VDS を 1 つだけ設定する場合は、このようにできます。別の設計オプションとして、NSX Edge をアップリンクごとに 1 つずつ、複数の VLAN トランスポート ゾーンに加えることができます。

最も一般的な設計オプションは、3 つのトランスポート ゾーンです。1 つのオーバーレイと、冗長アップリンク用に 2 つの VLAN トランスポート ゾーンを設定します。

トランスポート ネットワークでオーバーレイ トラフィックに同じ VLAN ID を使用し、VLAN トラフィック (VLAN アップリンクなど) に別の VLAN ID を使用するには、2 つの異なる N-VDS (VLAN 用とオーバーレイ 用) に ID を設定します。

仮想アプライアンス/仮想マシンの NSX Edge ネットワーク

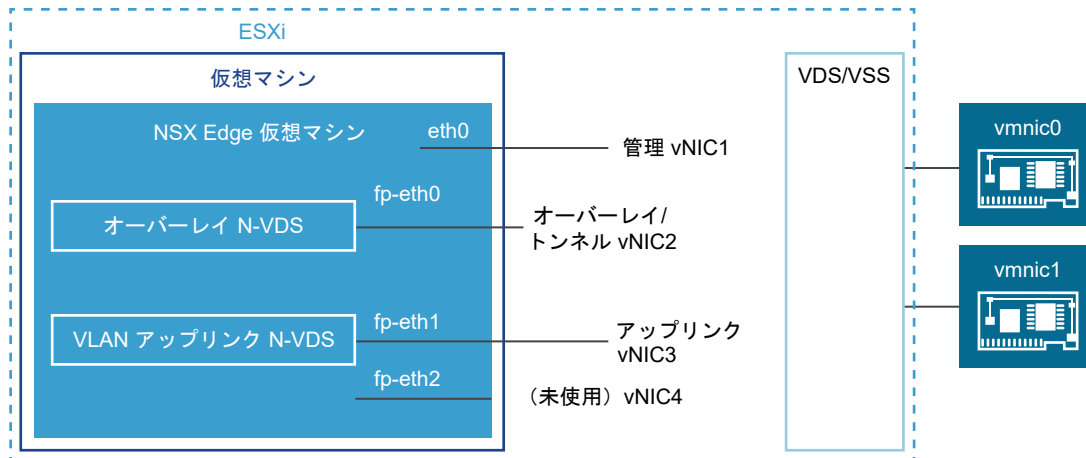
NSX Edge を仮想アプライアンスまたは仮想マシンとしてインストールすると、fp-ethX という内部インターフェイスが作成されます。ここで X は 0、1、2、3 です。これらのインターフェイスは、トップオブブラック (ToR) スイッチへのアップリンク用と、NSX-T Data Center のオーバーレイ トンネル用に割り当てられます。

NSX Edge のトランスポート ノードを作成するときに、アップリンクとオーバーレイ トンネルに関連付ける fp-ethX インターフェイスを選択できます。fp-ethX インターフェイスの使用方法は任意に決められます。

vSphere Distributed Switch または vSphere Standard スイッチで、NSX Edge に 2 つ以上の vmnics を割り当てる必要があります。1 つは NSX Edge の管理用で、もう 1 つはアップリンクやトンネル用です。

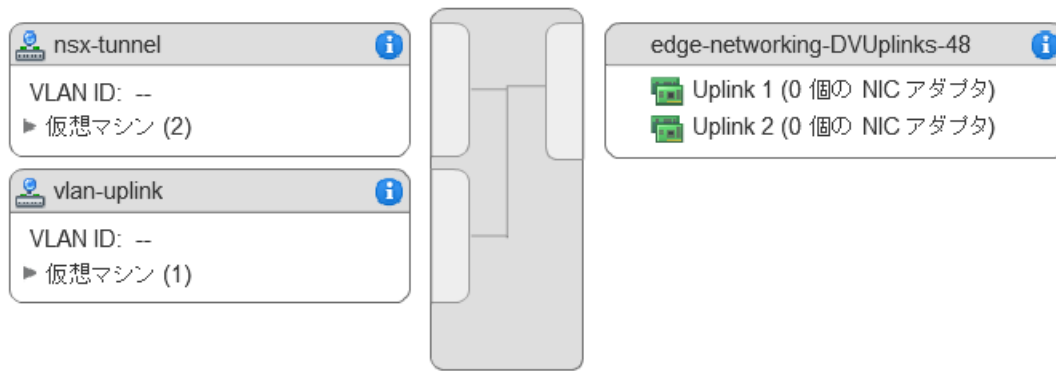
次の物理トポロジ例では、fp-eth0 を NSX-T Data Center のオーバーレイ トンネルに使用しています。fp-eth1 は VLAN アップリンクに使用しています。fp-eth2 と fp-eth3 は使用されていません。vNIC1 は、管理ネットワークに割り当てられます。

図 9-2. NSX Edge 仮想マシン ネットワークのリンク設定の例



この例に示す NSX Edge は 2 つのトランスポート ゾーンに属しています (オーバーレイ 1 つと VLAN 1 つ)。このため、トンネル用とアップリンク トラフィック用に 2 つの N-VDS があります。

このスクリーン ショットは、仮想マシンのポート グループ、nsx-tunnel と vlan-uplink を示しています。



展開時には、仮想マシンのポート グループで設定されている名前と一致するネットワーク名を指定する必要があります。たとえば、NSX Edge の展開に ovftool を使用している場合に、この例の仮想マシン ポート グループと一致させるには、ネットワークの ovftool 設定を次のように行うことができます。

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

この例では、仮想マシンのポート グループ名、Mgmt、nsx-tunnel、vlan-uplink を使用しています。仮想マシンのポート グループには任意の名前を使用できます。

NSX Edge でトンネルとアップリンク用に設定する仮想マシン ポート グループを、VMkernel ポートや、特定の IP アドレスに関連付ける必要はありません。これらは、レイヤー 2 でのみ使用されるためです。環境で DHCP を使用して管理インターフェイスにアドレスを提供する場合は、管理ネットワークに割り当てられている NIC が 1 つだけであることを確認します。

VLAN とトンネルのポート グループはトランク ポートとして設定されています。これは必須です。たとえば、標準の vSwitch では、トランク ポートを次のように設定します。[ホスト] - [設定] - [ネットワーク] - [ネットワークの追加] - [仮想マシン] - [VLAN ID すべて (4095)]。

アプライアンス ベースまたは仮想マシンの NSX Edge を使用する場合は、標準の vSwitch または vSphere Distributed Switch を使用できます。

準備が完了した NSX-T Data Center ホストに NSX Edge 仮想マシンをインストールして、トランスポート ノードとして設定することができます。展開には 2 つのタイプがあります。

- NSX Edge 仮想マシンを展開するには、VSS/VDS がホスト上の個別の pNIC を使用する VSS/VDS ポート グループを使用します。ホスト トランスポート ノードは、ホストにインストールされた N-VDS に対して独立した pNIC を使用します。ホスト トランスポート ノードの N-VDS は、VSS または VDS と共存します。いずれも、独立した pNIC を使用します。ホスト TEP (Tunnel End Point) および NSX Edge TEP は同じサブネットに配置することも、異なるサブネットに配置することもできます。
- NSX Edge 仮想マシンを展開するには、ホスト トランスポート ノードの N-VDS 上の VLAN によってバックアップされている論理スイッチを使用します。ホスト TEP および NSX Edge TEP は異なるサブネットに配置する必要があります。

また、複数の NSX Edge アプライアンス/仮想マシンを 1 台のホストにインストールし、同じ管理、VLAN、トンネル エンドポイントのポート グループを、インストールされているすべての NSX Edge に使用できます。

基盤となる物理リンクが稼動し、仮想マシンのポート グループ設定が完了したら、NSX Edge をインストールできます。

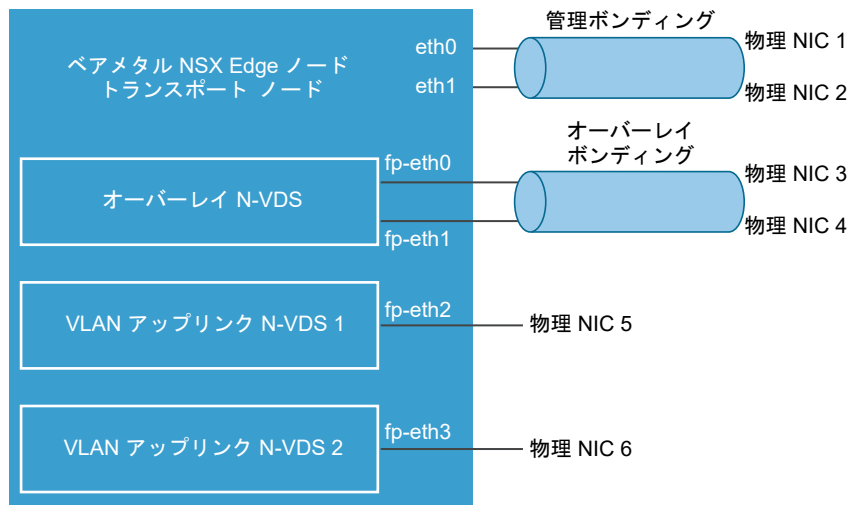
ベア メタルの NSX Edge ネットワーク

ベアメタルの NSX Edge には、fp-ethX という内部インターフェイスが含まれます。この X は、0、1、2、3、4 と続きます。作成される fp-ethX インターフェイス数は、ベア メタルの NSX Edge にある物理 NIC の数によって異なります。これらのインターフェイスの 4 つまでは、トップオブブラック (ToR) スイッチへのアップリンクや、NSX-T Data Center のオーバーレイ トンネルに割り当てることができます。

NSX Edge のトランスポート ノードを作成するときに、アップリンクとオーバーレイ トンネルに関連付ける fp-ethX インターフェイスを選択できます。

fp-ethX インターフェイスの使用方法は任意に決められます。次の物理トポロジ例では、fp-eth0 と fp-eth1 が結合され、NSX-T Data Center のオーバーレイ トンネルに使用されています。fp-eth2 と fp-eth3 は、ToR への冗長 VLAN アップリンクとして使用されています。

図 9-3. ベア メタルの NSX Edge ネットワークのリンク設定の一例



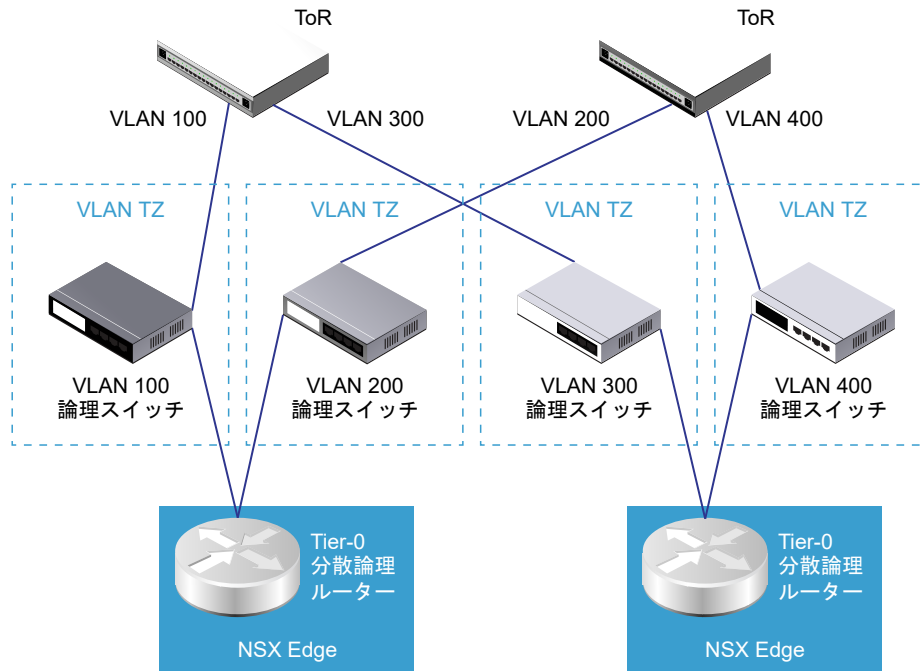
NSX Edge のアップリンクの冗長性

NSX Edge のアップリンクの冗長性によって、2 つの VLAN 等コスト マルチパス (ECMP) アップリンクを NSX Edge から外部 ToR のネットワーク接続に使用できます。

ECMP VLAN アップリンクが 2 つあるときは、高可用性と完全なメッシュ接続用に ToR スイッチも 2 つ用意する必要があります。VLAN 論理スイッチには、それぞれ対応する VLAN ID があります。

NSX Edge を VLAN のトランスポート ゾーンに追加すると、新しい N-VDS がインストールされます。たとえば、図に示すように 4 つの VLAN トランスポート ゾーンに NSX Edge ノードを追加すると、NSX Edge に 4 つの N-VDS がインストールされます。

図 9-4. NSX Edge から ToR への ECMP VLAN 設定の一例



注： vSphere Distributed Switch (vDS) が含まれ、N-VDS が含まれない ESXi ホスト上で展開されている Edge 仮想マシンの場合は、次の操作が必要です。

- 偽装転送を有効にして DHCP を機能させます。
- Edge 仮想マシンが不明なユニキャスト パケットを受信できるようにするため、無作為検出モードを有効にします。これは、MAC アドレスの学習がデフォルトで無効になっているためです。MAC アドレスの学習がデフォルトで有効になっている vDS 6.6 以降では、これは必要ありません。

NSX Edge のインストール方法

NSX Manager ユーザー インターフェイス (推奨)、vSphere Web Client または vSphere コマンドライン OVF ツールを使用して、ESXi ホストに NSX Edge をインストールします。

NSX Edge のインストール方法

インストール方法	方法
NSX Manager (NSX Edge 仮想マシン アプライアンスのみをインストールする場合の推奨方法)	<ul style="list-style-type: none"> ■ NSX Edge ネットワークの要件を満たしていることを確認します。NSX Edge のインストール要件 を参照してください。 ■ NSX Edge トランスポート ノードを作成します。NSX Edge トランスポート ノードの作成 を参照してください。 ■ NSX Edge クラスタを作成します。NSX Edge クラスタの作成 を参照してください。
vSphere Web Client または vSphere コマンドライン OVF ツール	<ul style="list-style-type: none"> ■ NSX Edge ネットワークの要件を満たしていることを確認します。NSX Edge のインストール要件 を参照してください。 ■ vSphere Web Client または vSphere コマンドライン OVF ツールを選択して、NSX Edge をインストールします。 <ul style="list-style-type: none"> ■ (Web Client) ESXi に NSX Edge をインストールします。vSphere の GUI を使用した ESXi への NSX Edge のインストール を参照してください。 ■ (コマンドライン OVF ツール) ESXi に NSX Edge をインストールします。コマンドライン OVF ツールを使用した ESXi への NSX Manager のインストール を参照してください。 ■ NSX Edge を管理プレーンに追加します。NSX Edge の管理プレーンへの追加 を参照してください。 ■ トランスポート ノードとして NSX Edge を構成します。トランスポート ノードとしての NSX Edge の設定 を参照してください。 ■ NSX Edge クラスタを作成します。NSX Edge クラスタの作成 を参照してください。
(ベアメタル サーバ) ISO (ISO ファイルによる自動またはインタラクティブ モード) または NSX Edge 仮想マシン アプライアンスとして使用	<p>ベアメタル サーバで NSX Edge の自動インストールを設定するか、PXE を使用して仮想マシン アプライアンスとして NSX Edge をインストールできます。PXE ブートのインストール手順は NSX Manager でサポートされません。</p> <ul style="list-style-type: none"> ■ NSX Edge ネットワークの要件を満たしていることを確認します。NSX Edge のインストール要件 を参照してください。 ■ PXE サーバを準備します。NSX Edge 用の PXE サーバの準備 を参照してください。サポートされているインストール方法のいずれかを選択します。 <ul style="list-style-type: none"> ■ (自動インストール) ISO ファイルを使用してベアメタルに NSX Edge をインストールします。ISO ファイルを使用した NSX Edge の自動インストール を参照してください。 ■ (自動インストール) ISO ファイルを使用して、NSX Edge を仮想アプライアンスとしてインストールします。ISO ファイルを使用した仮想アプライアンスとしての NSX Edge のインストール を参照してください。 ■ (手動インストール) ISO ファイルを使用して、NSX Edge を手動でインストールします。ISO ファイルを使用した NSX Edge のインタラクティブ インストール を参照してください。 ■ NSX Edge を管理プレーンに追加します。NSX Edge の管理プレーンへの追加 を参照してください。 ■ トランスポート ノードとして NSX Edge を構成します。トランスポート ノードとしての NSX Edge の設定 を参照してください。 ■ NSX Edge クラスタを作成します。NSX Edge クラスタの作成 を参照してください。

NSX Edge トランスポート ノードの作成

NSX Edge 仮想マシンを NSX-T Data Center ファブリックに追加して、NSX Edge トランスポート ノード仮想マシンとして設定することができます。

NSX Edge ノードは、ローカルの制御プレーン デーモンと、NSX-T データ プレーンを実装する転送エンジンを実行するトランスポート ノードです。NSX-T 分散仮想スイッチ（NSX 分散仮想スイッチ、N-VDS ともいいます）のインスタンスを実行します。Edge ノードは、ハイパーバイザーに配布できない集中管理のネットワーク サービスを実行する専用のサービス アプライアンスです。これらは、ベアメタル アプライアンスまたは仮想マシンのフォーム ファクタとしてインスタンス化されます。これらは、1 つ以上のクラスタにグループ化され、容量のプールを表します。

NSX Edge は、1 つのオーバーレイ トランスポート ゾーンおよび複数の VLAN トランスポート ゾーンに属することができます。NSX Edge は 1 つ以上の VLAN トランスポート ゾーンに属して、アップリンク アクセスを提供します。

注： テンプレート仮想マシンを使用してトランスポート ノードを作成する場合は、ホストの `/etc/vmware/nsx/` に証明書がないことを確認してください。証明書がすでに存在する場合、netcpa エージェントは証明書を作成しません。

前提条件

- トランスポート ゾーンが設定されている必要があります。[トランスポート ザーンの作成](#) を参照してください。
- コンピュート マネージャが設定されていることを確認します。[コンピュート マネージャの追加](#) を参照してください。
- アップリンク プロファイルが設定されている必要があります。設定されていない場合は、NSX Edge ノード用のデフォルトのアップリンク プロファイルを使用できます。[アップリンク プロファイルの作成](#) を参照してください。
- IP アドレス プールが設定されているか、ネットワーク環境内の IP プールを使用できる必要があります。[トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成](#) を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [Edge トランスポート ノード] - [Edge 仮想マシンの追加] を選択します。
- 3 NSX Edge の名前を入力します。
- 4 vCenter Server のホスト名または FQDN を入力します。
- 5 最適なパフォーマンスを維持するため、NSX Edge アプライアンス用のメモリを予約します。

NSX Edge 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、予約を設定します。[NSX Edge 仮想マシンのシステム要件](#) を参照してください。

6 CLI と NSX Edge の root パスワードを指定します。

パスワード強度の基準に準拠したパスワードを使用する必要があります。

- 12 文字以上
- 1 文字以上の小文字
- 1 文字以上の大文字
- 1 文字以上の数字
- 1 文字以上の特殊文字
- 5 文字以上の異なる文字
- 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。
 - `retry=3` : 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。
 - `minlen=12` : 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。
 - `difok=0` : 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。`difok` に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。
 - `lcredit=1` : 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `ucredit=1` : 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `dcredit=1` : 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の `minlen` 値に合わせるため、それぞれの数字が +1 とカウントされます。
 - `ocredit=1` : 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `enforce_for_root` : root ユーザーに設定されるパスワード。

注： Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、man ページを参照してください。

たとえば、単純で体系的なパスワードの使用は避けます。たとえば、**VMware123! 123**、**VMware12345** などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、**VMware123! 45**、**VMware1! 2345**、**VMware@1az23x** などです。

7 NSX Edge の詳細を入力します。

オプション	説明
コンピュー ト マネージャ	ドロップダウン メニューからコンピュー ト マネージャを選択します。 コンピュー ト マネージャは、管理プレーンに登録されている vCenter Server です。
クラス タ	ドロップダウン メニューから、NSX Edge が参加するクラス タを指定します。
リソース プールまたはホス ト	ドロップダウン メニューから NSX Edge にリソース プールまたは特定のホス トを割り当てます。
データ ス ト ア	ドロップダウン メニューから NSX Edge ファイルのデータ ス ト アを選択します。

8 NSX Edge インターフェイスの詳細を入力します。

オプション	説明
IP の割り当て	NSX Manager または NSX Controller との通信に必要な NSX Edge ノードに割り当てられた IP アドレスです。 [DHCP] または [固定] IP アドレスを選択します。 [固定] を選択した場合は、次の値を入力します。 ■ 管理 IP : NSX Edge の IP アドレスを CIDR 表記で入力します。 ■ デフォルト ゲートウェイ : NSX Edge のゲートウェイ IP アドレスを入力します。
管理インターフェイス	ドロップダウン メニューから管理ネットワーク インターフェイスを選択します。このインターフェイスは、NSX Manager から到達可能か、NSX Manager および NSX Controller と同じ管理インターフェイスに含まれている必要があります。 NSX Edge 管理インターフェイスは、NSX Manager 管理インターフェイスと通信を確立します。

9 このトランスポート ノードが属するトランスポート ゾーンを選択します。

NSX Edge トランスポート ノードは 2 つ以上のトランスポート ゾーン（NSX-T Data Center 接続用のオーバーレイとアップリンク接続用の VLAN）に属します。

注： 次の前提条件を満たしている場合、NSX Edge ノードは複数のオーバーレイ トンネル（マルチ TEP）をサポートします。

- TEP 構成が 1 つの N-VDS でのみ設定されている。
- すべての TEP が、オーバーレイ トラフィックに同じトランスポート VLAN を使用している。
- すべての TEP IP が同じサブネットに存在し、同じデフォルト ゲートウェイを使用している。

10 N-VDS の情報を入力します。

オプション	説明
Edge スイッチ名	ドロップダウン メニューから VLAN スイッチまたはオーバーレイ スイッチを選択します。
アップリンク プロファイル	ドロップダウン メニューからアップリンク プロファイルを選択します。 使用可能なアップリンクは、選択したアップリンク プロファイルでの設定によって異なります。

オプション	説明
IP の割り当て	<p>この IP アドレスは、構成済みの NSX Edge スイッチに割り当てられます。これは、オーバーレイまたは VLAN ネットワーク上のパケットのルーティングに使用されます。</p> <p>オーバーレイ N-VDS に [IP プールを使用] または [固定 IP アドレスのリストを使用] を選択します。</p> <ul style="list-style-type: none"> ■ [固定 IP のリストを使用] を選択した場合は、次の値を指定します。 <ul style="list-style-type: none"> ■ 固定 IP リスト: NSX Edge スイッチで使用される IP アドレスをコンマ区切りのリストで入力します。 ■ ゲートウェイ: デフォルトのゲートウェイ IP アドレスを入力します。これは、オーバーレイ ネットワーク内の NSX Edge トランスポート ノード間でパケットをルーティングするために使用されます。 ■ サブネット マスク: 構成済みのゲートウェイのサブネット マスクを入力します。 ■ IP 割り当てに [IP プールを使用] を選択した場合は、IP プール名を指定します。
DPDK Fastpath インターフェイス/仮想 NIC	<p>アップリンク インターフェイスのデータ パス インターフェイス名を選択します。</p> <p>注: Edge ノードに適用されたアップリンク プロファイルが、名前付きチーミング ポリシーを使用している場合は、次の条件を満たしていることを確認します。</p> <ul style="list-style-type: none"> ■ デフォルトのチーミング ポリシーのすべてのアップリンクが、名前付きチーミング ポリシーを使用する論理スイッチを介してトラフィックが転送されるように、Edge 仮想マシンの物理ネットワーク インターフェイスにマッピングされている必要があります。

注:

- LLDP プロファイルは、NSX Edge 仮想マシン アプライアンスでサポートされていません。
- NSX Manager またはベアメタル サーバを使用して NSX Edge がインストールされている場合、アップリンク インターフェイスは [DPDK Fastpath インターフェイス] として表示されます。
- vCenter Server を使用して NSX Edge が手動でインストールされている場合、アップリンク インターフェイスは [仮想 NIC] として表示されます。

11 [トランスポート ノード] ページで接続ステータスを表示します。

NSX Edge をトランスポート ノードとして追加した後、接続状態は 10 ～ 12 分後に [稼動中] に変わります。

12 (オプション) GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API 呼び出しを使用して、トランスポート ノードを確認します。**13** (オプション) 状態の情報を確認するには、GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 呼び出しを使用します。**14** vCenter Server を使用して NSX Edge ノードを新しいホストに移行した後、NSX Manager ユーザー インターフェイスに NSX Edge の古い設定情報 (コンピュート、データストア、ネットワーク、SSH、NTP、DNS、検索ドメイン) が表示されることがあります。新しいホストで NSX Edge の最新の設定情報を取得するには、API コマンドを実行します。

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

次のステップ

NSX Edge ノードを NSX Edge クラスタに追加します。 [NSX Edge クラスタの作成](#) を参照してください。

NSX Edge クラスタの作成

NSX Edge のマルチノード クラスタがあると、1 つ以上の NSX Edge が常に使用可能になります。

NAT やロード バランサなどのステートフル サービスを使用して Tier-0 論理ルーターまたは Tier-1 ルーターを作成するには、それを NSX Edge クラスタに関連付ける必要があります。そのため、NSX Edge が 1 つしかない場合でも、NSX Edge クラスタに属する必要があります。

1 台の NSX Edge トランスポート ノードは 1 つの NSX Edge クラスタにのみ追加できます。

1 つの NSX Edge クラスタを使用して複数の論理ルーターをバックアップできます。

NSX Edge クラスタを作成した後、これを編集して NSX Edge を追加できます。

前提条件

- 1 台以上の NSX Edge ノードを追加します。
- NSX Edge ノードをクラスタに参加させる前に、このノードが安定していること、および、すべてのサービスが実行中で、すべてのグループが安定した状態になっていることを確認します。
- NSX Edge を管理プレーンに追加します。
- NSX Edge をトランスポート ノードとして追加します。
- オプションで、高可用性 (HA) 用の NSX Edge クラスタ プロファイルを作成します。デフォルトの NSX Edge クラスタ プロファイルを使用することもできます。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [Edge クラスタ] - [追加] を選択します。
- 3 NSX Edge クラスタ名を入力します。
- 4 ドロップダウン メニューから NSX Edge クラスタ プロファイルを選択します。
- 5 仮想マシンがオンプレミスに展開されている場合は、[メンバー タイプ] ドロップダウン メニューで **Edge ノード** を選択します。仮想マシンがパブリック クラウドに展開されている場合は、**Public Cloud Gateway** を選択します。
- 6 [使用可能] 列から NSX Edge を選択し、右矢印をクリックして [選択済み] 列に移動します。

次のステップ

これで、論理ネットワーク トポロジを構築してサービスを設定できるようになります。『NSX-T Data Center 管理ガイド』を参照してください。

vSphere の GUI を使用した ESXi への NSX Edge のインストール

vSphere Web Client または vSphere Client を使用すると、インタラクティブ モードで NSX Edge を ESXi にインストールできます。

注： NSX-T Data Center 2.5.1 以降では、NSX Edge 仮想マシンは vMotion をサポートします。

前提条件

NSX Edge のインストール要件で NSX Edge のネットワーク要件を参照してください。

手順

- 1 VMware ダウンロード ポータルで NSX Edge アプライアンス OVA 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 vSphere Client で、NSX Edge アプライアンスをインストールするホストを選択します。
- 3 右クリックして [OVF テンプレートの展開] を選択し、インストール ウィザードを開始します。
- 4 OVA のダウンロード URL を入力するか、保存した OVA ファイルに移動します。
- 5 NSX Edge 仮想マシンの名前を入力します。
ここに入力する名前がインベントリに表示されます。
- 6 NSX Edge アプライアンスのコンピュート リソースを選択します。
- 7 最適なパフォーマンスを維持するため、NSX Edge アプライアンス用のメモリを予約します。
NSX Edge 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、予約を設定します。NSX Edge 仮想マシンのシステム要件を参照してください。
- 8 OVF テンプレートの詳細を確認します。
- 9 NSX Edge アプライアンスのファイルを格納するデータストアを選択します。
- 10 デフォルトのソースおよびターゲット ネットワーク インターフェイスを使用します。
他のネットワークについてもデフォルトのネットワーク ターゲットを使用し、NSX Edge の展開後にネットワーク構成を変更することもできます。
- 11 ドロップダウン メニューから IP アドレスの割り当てを選択します。
- 12 NSX Edge システムの root、CLI 管理者、監査者のパスワードを入力します。

注： [テンプレートのカスタマイズ] 画面で、All properties have valid values というメッセージは無視してください。このメッセージは、フィールドに値を入力する前でも表示されます。パラメータがすべてオプションのため、このメッセージが表示されます。どのフィールドにも値を入力していないので、検証は成功します。

パスワード強度の基準に準拠したパスワードを使用する必要があります。

- 12 文字以上
- 1 文字以上の小文字

- 1 文字以上の大文字
- 1 文字以上の数字
- 1 文字以上の特殊文字
- 5 文字以上の異なる文字
- 次の Linux PAM モジュールの引数によって、デフォルトのパスワード強度ルールが適用されます。
 - `retry=3` : 新しいパスワードの最大入力回数。この引数では、最大 3 回までの入力を許可しています。これを超えると、エラーが返されます。
 - `minlen=12` : 新しいパスワードに許容される最小サイズ。新しいパスワードの文字数だけでなく、それぞれの文字種（特殊、大文字、小文字、数字）ごとにクレジット (+1) が指定されます。
 - `difok=0` : 新しいパスワードで異なる必要がある最小バイト数。古いパスワードと新しいパスワードの類似性を示します。`difok` に 0 を割り当てると、古いパスワードと新しいパスワードで異なる文字列を使用する必要はありません。完全一致が許可されます。
 - `lcredit=1` : 新しいパスワードに小文字を使用する場合の最大クレジット。小文字が 1 文字以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `ucredit=1` : 新しいパスワードに大文字を使用する場合の最大クレジット。大文字が 1 文字以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `dcredit=1` : 新しいパスワードに数字が含まれる場合の最大クレジット。数字が 1 個以下の場合、現在の `minlen` 値に合わせるため、それぞれの数字が +1 とカウントされます。
 - `ocredit=1` : 新しいパスワードに特殊文字を使用する場合の最大クレジット。特殊文字が 1 個以下の場合、現在の `minlen` 値に合わせるため、それぞれの文字が +1 とカウントされます。
 - `enforce_for_root` : `root` ユーザーに設定されるパスワード。

注： Linux PAM モジュールでパスワードと辞書の単語を比較する方法については、`man` ページを参照してください。

たとえば、単純で体系的なパスワードの使用は避けます。たとえば、**VMware123! 123**、**VMware12345** などです。単純で体系的なパスワードは強度要件を満たしませんが、英字、特殊文字、数字を組み合わせたパスワードは強度要件を満たします。たとえば、**VMware123! 45**、**VMware1! 2345**、**VMware@1az23x** などです。

- 13 (オプション) 使用可能な NSX Manager があり、OVA の展開中に NSX Edge を管理プレーンに登録する場合は、[Manager IP]、[サムプリント]、[トークン] の各フィールドに値を入力します。

- a 親 NSX Manager ノードの IP アドレスとサムプリントを入力します。
- b API 呼び出し `POST https://<nsx-manager>/api/v1/aaa/registration-token` を実行し、NSX Manager トークンを取得します。

```
{
  "token": "4065a7c0-9658-4058-bb01-c149f20f238a",
  "roles": [
    "enterprise_admin"
  ],
  "user": "admin"
}
```

- c NSX Manager トークンを入力します。

注： [ノード UUID] フィールドは、システム内部でのみ使用されます。このフィールドは空白のままにします。

- 14 NSX Edge 仮想マシンのホスト名を入力します。

- 15 デフォルト ゲートウェイ、管理ネットワークの IPv4、管理ネットワークのネットマスク、DNS および NTP の IP アドレスを入力します。

注： VMC の設定は無視します。VMC 展開の値のみを入力します。

- 16 (オプション) コンソールから NSX Edge にアクセスする場合は、SSH を有効にしないでください。ただし、root で SSH ログインし、NSX Edge コマンドラインに CLI ログインを行う場合は、SSH オプションを有効にします。

デフォルトでは、セキュリティ上の理由から SSH アクセスは無効になっています。

- 17 すべてのカスタム OVA テンプレートの仕様が正確であることを確認し、[終了] をクリックしてインストールを開始します。

インストールには 7 ～ 8 分かかる場合があります。

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

コンソール ウィンドウが開かない場合は、ポップアップが許可されていることを確認してください。

- 19 NSX Edge が起動したら、管理者認証情報を使用して CLI にログインします。

注： NSX Edge の起動後、最初のログイン時に管理者認証情報を使用しなかった場合、データ プレーン サービスは NSX Edge で自動的に開始されません。

- 20 `get interface eth0` コマンド (VLAN なし) または `get interface eth0.<vlan_ID>` コマンド (VLAN あり) を実行し、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。

```
nsx-edge-1> [get interface eth0.100]

Interface: eth0.100
```

```
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

注： NSX で管理されていないホストで NSX Edge 仮想マシンを起動する場合は、データ NIC の物理ホストスイッチで MTU 設定が 1500 ではなく 1600 に設定されていることを確認します。

21 `get managers` コマンドを実行し、NSX Edge が登録されていることを確認します。

```
- 10.29.14.136 Standby
- 10.29.14.135 Standby
- 10.29.14.134 Connected
```

22 NSX Edge が管理プレーンに登録されていない場合は、[NSX Edge の管理プレーンへの追加](#)を参照してください。

23 NSX Edge アプライアンスで必要な接続が可能であることを確認します。

SSH を有効にした場合は、SSH を使用して NSX Edge に接続できることを確認します。

- NSX Edge に ping を実行できます。
- NSX Edge は、デフォルト ゲートウェイに ping を実行できます。
- NSX Edge は、NSX Edge と同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- NSX Edge は、DNS サーバと NTP サーバに ping を実行できます。

24 接続問題のトラブルシューティングを行います。

注： 接続が確立されていない場合は、仮想マシン ネットワーク アダプタが適切なネットワークまたは VLAN に置かれていることを確認します。

デフォルトでは、NSX Edge データパスは、管理 NIC (IP アドレスとデフォルト ルートを持つ NIC) を除くすべての仮想マシン NIC を要求します。管理インターフェイスとして NIC を誤って割り当てた場合は、次の手順に従って DHCP を使用し、正しい NIC に管理 IP アドレスを割り当てます。

- a CLI にログインして **stop service dataplane** コマンドを入力します。
- b **set interface interface dhcp plane mgmt** コマンドを入力します。
- c *interface* を DHCP ネットワークに置き、IP アドレスが *interface* に割り当てられるまで待ちます。
- d **start service dataplane** コマンドを入力します。

VLAN アップリンクとトンネル オーバーレイに使用するデータパス fp-ethX ポートが、NSX Edge 上で [get interfaces] コマンドと [get physical-port] コマンドに示されます。

次のステップ

トランスポート ノードとして NSX Edge を設定します。[トランスポート ノードとしての NSX Edge の設定](#) を参照してください。

コマンドライン OVF ツールを使用した ESXi への NSX Edge のインストール

NSX Edge のインストールを自動的に行う場合は、コマンドライン ユーティリティの VMware OVF Tool を使用します。

前提条件

- システム要件を満たしていることを確認します。 [システム要件](#)を参照してください。
- 必要なポートが開いていることを確認します。 [ポートとプロトコル](#) を参照してください。
- ESXi ホストでデータストアが構成されていて、アクセスできることを確認します。
- 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 アドレスを確認します。
- まだ作成していない場合は、宛先の仮想マシン ポート グループ ネットワークを作成します。NSX-T Data Center アプライアンスを管理仮想マシン ネットワークに配置します。

複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。

- NSX Manager IPv4 IP アドレス スキームを使用します。
- [NSX Edge のインストール要件](#)で NSX Edge のネットワーク要件を参照してください。
- ESXi ホストに OVF テンプレートを展開するために必要な権限があることを確認します。
- ホスト名にアンダースコアが含まれていないことを確認します。含まれている場合、ホスト名が *localhost* に設定されます。
- OVF Tool バージョン 4.3 以降。
- NSX Edge 仮想マシンの展開と管理プレーンへの追加に使用できるパラメータについて理解しておく必要があります。

フィールド名	OVF パラメータ	フィールド タイプ
システムの root パスワード	nsx_passwd_0	NSX Edge のインストールに必要。
CLI 管理者パスワード	nsx_cli_passwd_0	NSX Edge のインストールに必要。
CLI 監査パスワード	nsx_cli_audit_passwd_0	オプション
CLI 管理者ユーザー名	nsx_cli_username	オプション
CLI 監査ユーザー名	nsx_cli_audit_username	オプション
NSX Manager の IP	mpIp	NSX Edge 仮想マシンを NSX Manager に追加する場合に必要。
NSX Manager のトークン	mpToken	NSX Edge 仮想マシンを NSX Manager に追加する場合に必要。 トークンを取得するには、NSX Manager で POST https://<nsx-manager>/api/v1/aaa/registration-token を実行します。

フィールド名	OVF パラメータ	フィールド タイプ
NSX Manager のサムプリント	mpThumbprint	NSX Edge 仮想マシンを NSX Manager に追加する場合に必要。 サムプリントを取得するには、NSX Manager ノードで <code>get certificate api thumbprint</code> を実行します。
ノード ID	mpNodeId	内部でのみ使用。
ホスト名	nsx_hostname	オプション
デフォルト IPv4 ゲートウェイ	nsx_gateway_0	オプション
管理ネットワーク IP アドレス	nsx_ip_0	オプション
管理ネットワークのネットマスク	nsx_netmask_0	オプション
DNS サーバ	nsx_dns1_0	オプション
ドメイン検索サフィックス	nsx_domain_0	オプション
NTP サーバ	nsx_ntp_0	オプション
SSH サービスが有効かどうか	nsx_isSSHEnabled	オプション
root ログインで SSH が有効かどうか	nsx_allowSSHRootLogin	オプション

手順

- ◆ スタンドアロン ホストの場合、適切なパラメータを指定して `ovftool` コマンドを実行します。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
```

```
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- ◆ vCenter Server で管理されているホストの場合、適切なパラメータを指定して ovftool コマンドを実行します。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
```



```
--prop:mpThumbprint=<NSXManager-Thumbprint>
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- ◆ 最適なパフォーマンスを維持するため、アプライアンス用のメモリを予約します。
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、予約を設定します。[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#) を参照してください。
- ◆ NSX Edge のコンソールを開いて、ブート プロセスを追跡します。
- ◆ NSX Edge が起動したら、管理者認証情報を使用して CLI にログインします。
- ◆ `get interface eth0` コマンド (VLAN なし) または `get interface eth0.<vlan_ID>` コマンド (VLAN あり) を実行し、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。

```
nsx-edge-1> [get interface eth0.100]

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

注： NSX で管理されていないホストで NSX Edge 仮想マシンを起動する場合は、データ NIC の物理ホストスイッチで MTU 設定が 1500 ではなく 1600 に設定されていることを確認します。

- ◆ NSX Edge アプライアンスで必要な接続が可能であることを確認します。
SSH を有効にした場合は、SSH を使用して NSX Edge に接続できることを確認します。
 - NSX Edge に ping を実行できます。
 - NSX Edge は、デフォルト ゲートウェイに ping を実行できます。
 - NSX Edge は、NSX Edge と同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
 - NSX Edge は、DNS サーバと NTP サーバに ping を実行できます。

- ◆ 接続問題のトラブルシューティングを行います。

注： 接続が確立されていない場合は、仮想マシン ネットワーク アダプタが適切なネットワークまたは VLAN に置かれていることを確認します。

デフォルトでは、NSX Edge データパスは、管理 NIC (IP アドレスとデフォルト ルートを持つ NIC) を除くすべての仮想マシン NIC を要求します。管理インターフェイスとして NIC を誤って割り当てた場合は、次の手順に従って DHCP を使用し、正しい NIC に管理 IP アドレスを割り当てます。

- CLI にログインして **stop service dataplane** コマンドを入力します。
- set interface interface dhcp plane mgmt** コマンドを入力します。
- interface* を DHCP ネットワークに置き、IP アドレスが *interface* に割り当てられるまで待ちます。
- start service dataplane** コマンドを入力します。

VLAN アップリンクとトンネル オーバーレイに使用するデータパス fp-ethX ポートが、NSX Edge 上で [get interfaces] コマンドと [get physical-port] コマンドに示されます。

次のステップ

管理プレーンに NSX Edge を追加しなかった場合は、[NSX Edge の管理プレーンへの追加](#)を参照してください。

ISO ファイルを使用した仮想アプライアンスとしての NSX Edge のインストール

NSX Edge 仮想マシンは、ISO ファイルを使用して手動でインストールできます。

重要： NSX-T Data Center コンポーネント仮想マシンのインストールには VMware Tools が含まれます。NSX-T Data Center アプライアンスで VMware Tools を削除またはアップグレードすることはできません。

前提条件

- [NSX Edge のインストール要件](#)で NSX Edge のネットワーク要件を参照してください。

手順

- 1 MyVMware アカウント (myvmware.com) に移動し、[VMware NSX-T Data Center] - [ダウンロード] の順に移動します。
- 2 NSX Edge の ISO ファイルを見つけて、ダウンロードします。
- 3 vSphere Client で、ホスト データストアを選択します。
- 4 [ファイル] - [ファイルのアップロード] - [データストアへのファイルのアップロード] の順に選択し、ISO ファイルを探してアップロードします。

自己署名証明書を使用している場合は、ブラウザに IP アドレスを指定して、証明書に同意し、ISO ファイルを再びアップロードします。

- 5 vSphere Client インベントリで、ISO ファイルをアップロードしたホストを選択します。または、vSphere Client でも選択できます。

- 6 右クリックして [新規仮想マシン] を選択します。
- 7 NSX Edge アプライアンスのコンピュー ト リソースを選択します。
- 8 NSX Edge アプライアンスのファイルを格納するデータストアを選択します。
- 9 NSX Edge 仮想マシンのデフォルトの互換性を承認します。
- 10 NSX Edge 仮想マシンでサポートされている ESXi オペレーティング システムを選択します。
- 11 仮想ハードウェアを構成します。

- 新規ハード ディスク : 200 GB
- 新規ネットワーク : 仮想マシン ネットワーク
- 新規 CD/DVD ドライブ : データストア ISO ファイル

[接続] をクリックし、NSX Edge ISO ファイルを仮想マシンに割り当てる必要があります。

- 12 新しい NSX Edge 仮想マシンをパワーオンします。
- 13 ISO の起動時に、仮想マシン コンソールを開いて [自動インストール] を選択します。

Enter キーを押した後、開始するまでに 10 秒程かかる可能性があります。

インストール中に、管理インターフェイスの VLAN ID を入力するように求められます。ネットワーク インターフェイスの VLAN サブインターフェイスを作成する場合は、[はい] を選択して VLAN ID を入力します。パケットに VLAN タグ付けを設定しない場合は、[いいえ] を選択します。

パワーオン中に、仮想マシンが DHCP を介したネットワーク構成を要求します。環境内で DHCP を使用できない場合は、インストーラに IP アドレスの設定を求めるプロンプトが表示されます。

デフォルトでは、root のログイン パスワードは **vmware** で、admin のログイン パスワードは **default** です。

初回ログイン時にパスワードの変更を求められます。このパスワードの変更には、次に示すような厳密な複雑性ルールが適用されます。

- 12 文字以上
- 1 文字以上の小文字
- 1 文字以上の大文字
- 1 文字以上の数字
- 1 文字以上の特殊文字
- 5 文字以上の異なる文字
- 辞書に登録されている単語が使われていない
- パリンドローム（回文）になっていない
- 使用できるモノトニックな文字シーケンスは 4 つ以下です。

重要： 要件を満たすパスワードが設定されるまで、コア サービスはアプライアンスで起動しません。

- 14 最適なパフォーマンスを維持するため、NSX Edge アプライアンス用のメモリを予約します。

NSX Edge 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、予約を設定します。[NSX Edge 仮想マシンのシステム要件](#) を参照してください。

- 15 NSX Edge が起動したら、管理者認証情報を使用して CLI にログインします。

注： NSX Edge の起動後、最初のログイン時に管理者認証情報を使用しなかった場合、データプレーンサービスは NSX Edge で自動的に開始されません。

- 16 管理インターフェイスの設定方法は 3 つあります。

注： サーバが Mellanox NIC カードを使用している場合は、インバンド管理インターフェイスで Edge を設定しないでください。

- タグのないインターフェイス。このインターフェイスタイプは、アウトオブバンド管理インターフェイスを作成します。

```
(DHCP) set interface eth0 dhcp plane mgmt
```

```
(静的) set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt
```

- タグ付きインターフェイス。

```
set interface eth0 vlan <vlan_ID> plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(静的) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- インバンド インターフェイス。

```
set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(静的) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- 17 (オプション) SSH サービスを開始します。start service ssh を実行します。

- 18 get interface eth0 コマンド (VLAN なし) または get interface eth0.<vlan_ID> コマンド (VLAN あり) を実行し、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。

```
nsx-edge-1> [get interface eth0.100]
```

```
Interface: eth0.100
```

```
Address: 192.168.110.37/24
```

```
MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

注： NSX で管理されていないホストで NSX Edge 仮想マシンを起動する場合は、データ NIC の物理ホストスイッチで MTU 設定が 1500 ではなく 1600 に設定されていることを確認します。

- 19 (タグ付きインターフェイスとインバンド インターフェイス) 新しいインターフェイスを作成する前に、既存の VLAN 管理インターフェイスをクリアする必要があります。

```
Clear interface eth0.<vlan_ID>
```

新しいインターフェイスを設定するには、手順 15 を参照してください。

- 20 NSX Edge アプライアンスで必要な接続が可能であることを確認します。

SSH を有効にした場合は、SSH を使用して NSX Edge に接続できることを確認します。

- NSX Edge に ping を実行できます。
- NSX Edge は、デフォルト ゲートウェイに ping を実行できます。
- NSX Edge は、NSX Edge と同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- NSX Edge は、DNS サーバと NTP サーバに ping を実行できます。

- 21 接続問題のトラブルシューティングを行います。

注： 接続が確立されていない場合は、仮想マシン ネットワーク アダプタが適切なネットワークまたは VLAN に置かれていることを確認します。

デフォルトでは、NSX Edge データパスは、管理 NIC (IP アドレスとデフォルト ルートを持つ NIC) を除くすべての仮想マシン NIC を要求します。管理インターフェイスとして NIC を誤って割り当てた場合は、次の手順に従って DHCP を使用し、正しい NIC に管理 IP アドレスを割り当てます。

- a CLI にログインして **stop service dataplane** コマンドを入力します。
- b **set interface interface dhcp plane mgmt** コマンドを入力します。
- c *interface* を DHCP ネットワークに置き、IP アドレスが *interface* に割り当てられるまで待ちます。
- d **start service dataplane** コマンドを入力します。

VLAN アップリンクとトンネル オーバーレイに使用するデータパス fp-ethX ポートが、NSX Edge 上で [get interfaces] コマンドと [get physical-port] コマンドに示されます。

次のステップ

管理プレーンに NSX Edge を参加させなかった場合は、[NSX Edge の管理プレーンへの追加](#)を参照してください。

ベア メタルへの NSX Edge のインストール

PXE サーバを使用して、ベアメタル サーバの NSX Edge のインストールを自動化します。あるいは、ISO ファイルを使用して NSX Edge を仮想マシン アプライアンスとしてインストールするか、ベアメタル サーバにインストールします。

PXE ブートのインストールは、NSX Manager ではサポートされていません。IP アドレス、ゲートウェイ、ネットワーク マスク、NTP、DNS などのネットワークも設定できません。

前提条件

- NSX Edge ベアメタルサーバでバージョン 6.7u3 以前が実行されている場合は、vCenter Server で NSX Edge `virtualHW.version` を **14** 以降にアップグレードしないでください。デフォルトでは、`virtualHW.version` は **13** に設定されています。
- デフォルトでは、LAG 形成のためにイーサネット デバイスを集約する NSX Edge ベアメタル ボンディング デバイスは、ロード バランシング用に最適化されています。このため、ボンディング デバイスは、CPU がパケットを送信するローカル NUMA ノード上のネットワーク デバイスのみを使用します。ボンディングを形成しているデバイスが複数の NUMA ノードにまたがり、パケット処理に割り当てられている CPU が NUMA ノードのサブセットに属している場合、一部のデバイスのみがトラフィックを送信します。つまり、ボンディング デバイスから送信されるトラフィックのロード バランシングに一部のデバイスしか使用されないため、デフォルトの最適化を無効にすることはできません。

ただし、ボンディングのすべてのイーサネット デバイスを使用してトラフィックのロード バランシングを行う場合は、パケット処理用の CPU が接続している NUMA ノードにすべてのイーサネット デバイスを移動する必要があります。

注： フェイルオーバーとロード バランシングは排他的です。ローカル NUMA ノードに接続しているイーサネット デバイスが停止すると、そのトラフィックは他のデバイスに送信されます（NUMA のローカルにないデバイスに送信される場合もあります）。ロード バランシングの最適化は、フェイルオーバー機能に影響しません。

NSX Edge 用の PXE サーバの準備

PXE は DHCP、HTTP、TFTP の複数のコンポーネントから構成されます。この手順で、Ubuntu で PXE サーバのセットアップを実行します。

DHCP は、NSX Edge などの NSX-T Data Center コンポーネントに IP アドレス設定を動的に配信します。

PXE 環境の DHCP サーバでは、NSX Edge が IP アドレスを自動的に要求し、受け取ることができます。

TFTP はファイル転送プロトコルです。TFTP サーバは、ネットワーク上で常に PXE クライアントを待機しています。PXE サービスを要求するネットワーク PXE クライアントが検出されると、NSX-T Data Center コンポーネントの ISO ファイルと、preseed ファイルに含まれるインストール設定が提供されます。

前提条件

- 環境で PXE サーバが使用できる必要があります。PXE サーバは任意の Linux ディストリビューションに設定できます。PXE サーバには 2 つのインターフェイスが必要です。1 つは外部通信用で、もう 1 つは DHCP の IP アドレス サービスと TFTP サービス用です。

複数の管理ネットワークが存在する場合は、NSX-T Data Center アプライアンスから他のネットワークへのスタティック ルートを追加できます。

- 事前にシードされた構成ファイルの -- の後に、再起動後も存続するようにパラメータ `net.ifnames=0` および `biosdevname=0` が設定されていることを確認します。
- [NSX Edge のインストール要件](#)で NSX Edge のネットワーク要件を参照してください。

手順

- 1 (オプション) kickstart ファイルを使用して、Ubuntu サーバで新しい TFTP または DHCP サービスをセットアップします。

kickstart ファイルはテキスト ファイルで、最初の起動後にアプライアンスで実行する CLI コマンドが含まれます。

参照する PXE サーバに基づいて、kickstart ファイルに名前を付けます。次はその例です。

```
nsxcli.install
```

ファイルは、Web サーバの `/var/www/html/nsx-edge/nsxcli.install` などにコピーする必要があります。

kickstart ファイルに、CLI コマンドを追加できます。たとえば、管理インターフェイスの IP アドレスを構成するには、次のコマンドを使用します。

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

admin ユーザーのパスワードを変更するには、次のコマンドを使用します。

```
set user admin password <new_password> old-password <old-password>
```

preseed.cfg ファイルでパスワードを指定する場合は、kickstart ファイルでも同じパスワードを使用します。それ以外の場合は、デフォルトのパスワードである「default」を使用します。

NSX Edge を管理プレーンに追加するには、次のコマンドを使用します。

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username> password <manager password>
```

- 2 2 つのインターフェイスを作成します。1 つは管理用で、もう 1 つは DHCP サービスと TFTP サービス用です。

DHCP/TFTP インターフェイスが、NSX Edge が配置されているサブネットにあることを確認します。

たとえば、NSX Edge の管理インターフェイスを 192.168.210.0/24 サブネットに配置する場合は、eth1 を同じサブネットに配置します。

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
```

```

auto eth0
iface eth0 inet static
    address 192.168.110.81
    gateway 192.168.110.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
    address 192.168.210.82
    gateway 192.168.210.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10

```

3 DHCP サーバ ソフトウェアをインストールします。

```
sudo apt-get install isc-dhcp-server -y
```

4 /etc/default/isc-dhcp-server ファイルを編集し、DHCP サービスを提供するインターフェイスを追加します。

```
INTERFACES="eth1"
```

5 (オプション) この DHCP サーバをローカル ネットワークの正式な DHCP サーバにする場合は、/etc/dhcp/dhcpd.conf ファイルで [authoritative;] 行をコメント解除します。

```
...
authoritative;
...
```

6 /etc/dhcp/dhcpd.conf ファイルで、PXE ネットワークの DHCP 設定を定義します。

次はその例です。

```

subnet 192.168.210.0 netmask 255.255.255.0 {
    range 192.168.210.90 192.168.210.95;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.110.10;
    option routers 192.168.210.1;
    option broadcast-address 192.168.210.255;
    default-lease-time 600;
    max-lease-time 7200;
}

```

7 DHCP サービスを開始します。

```
sudo service isc-dhcp-server start
```

8 DHCP サービスが動作することを確認してください。

```
service --status-all | grep dhcp
```


- 9 Apache、TFTP、PXE ブートに必要なその他のコンポーネントをインストールします。

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```

- 10 TFTP と Apache が実行されていることを確認します。

```
service --status-all | grep tftpd-hpa  
service --status-all | grep apache2
```

- 11 次の行を /etc/default/tftpd-hpa ファイルに追加します。

```
RUN_DAEMON="yes"  
OPTIONS="-l -s /var/lib/tftpboot"
```

- 12 次の行を /etc/inetd.conf ファイルに追加します。

```
tftp      dgram    udp       wait      root      /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/  
tftpboot
```

- 13 TFTP サービスを再起動します。

```
sudo /etc/init.d/tftpd-hpa restart
```

- 14 NSX Edge インストーラ ISO ファイルを一時フォルダにコピーするかダウンロードします。

- 15 ISO ファイルをマウントし、インストール コンポーネントを TFTP サーバと Apache サーバにコピーします。

```
sudo mount -o loop ~/nsx-edge.<build>.iso /mnt  
cd /mnt  
sudo cp -fr install/netboot/* /var/lib/tftpboot/  
sudo mkdir /var/www/html/nsx-edge  
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```

- 16** (オプション) `/var/www/html/nsx-edge/preseed.cfg` ファイルを編集して、暗号化されているパスワードを変更します。

`mkpasswd` などの Linux ツールを使用してパスワード ハッシュを作成できます。

```
sudo apt-get install whois
sudo mkpasswd -m sha-512

Password:
$6$SUFGqs[...]FcoHLijOuFD
```

- a root パスワードを変更し、`/var/www/html/nsx-edge/preseed.cfg` を編集して、次の行を検索します。

```
d-i passwd/root-password-crypted password $6$tgmlNLMP$9BuAHhN...
```

- b ハッシュ文字列を置換します。

`$`、`'`、`"`、`\` などの特殊文字をエスケープする必要はありません。

- c `usermod` コマンドを `preseed.cfg` に追加して、root または admin、あるいはその両方のパスワードを設定します。

たとえば、`echo 'VMware NSX Edge'` 行を検索して、次のコマンドを追加します。

```
usermod --password '\$6\$VS3exId0aKzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/'
root; \
usermod --password '\$6\$VS3exId0aKzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/'
admin; \
```

このハッシュ文字列は一例です。特殊文字はすべてエスケープする必要があります。最初の `usermod` コマンドの root パスワードが、`d-i passwd/root-password-crypted password 6tgml...` で設定したパスワードに置き換わります。

`usermod` コマンドを使用してパスワードを設定した場合、ユーザーは初めてログインするときにパスワードの変更を求められません。それ以外の場合、ユーザーは初回のログイン時にパスワードを変更する必要があります。

- 17** 次の行を `/var/lib/tftpboot/pxelinux.cfg/default` ファイルに追加します。

192.168.210.82 は、実際の TFTP サーバの IP アドレスに置き換えます。

```
label nsxedge
    kernel ubuntu-installer/amd64/linux
    ipappend 2
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-lvm/
device_remove_lvm=true netcfg/choose_interface=auto debian-installer/
allow_unauthenticated=true preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg mirror/
country=manual mirror/http/hostname=192.168.210.82 nsx-kickstart/url=http://192.168.210.82/
nsx-edge/nsxcli.install mirror/http/directory=/nsx-edge initrd=ubuntu-installer/amd64/
initrd.gz mirror/suite=xenial --
```

18 次の行を /etc/dhcp/dhcpd.conf ファイルに追加します。

192.168.210.82 は、実際の DHCP サーバの IP アドレスに置き換えます。

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 DHCP サービスを再起動します。

```
sudo service isc-dhcp-server restart
```

注： 「stop: Unknown instance: start: Job failed to start」などのエラーが返された場合、
`sudo /etc/init.d/isc-dhcp-server stop` を実行してから `sudo /etc/init.d/isc-dhcp-server start` を実行します。
`sudo /etc/init.d/isc-dhcp-server start` コマンドは、エラーの原因に関する情報を返します。

次のステップ

ISO ファイルを使用してベア メタルに NSX Edge をインストールします。[ISO ファイルを使用した NSX Edge の自動インストール](#) を参照してください。

ISO ファイルを使用した NSX Edge の自動インストール

NSX Edge デバイスを手動でベア メタルにインストールするには、ISO ファイルを使用します。このファイルには、IP アドレス、ゲートウェイ、ネットワーク マスク、NTP、DNS などのネットワーク設定が含まれます。

前提条件

- システム BIOS モードがレガシー BIOS に設定されていることを確認します。
- [NSX Edge のインストール要件](#)で NSX Edge のネットワーク要件を参照してください。

手順

- 1 MyVMware アカウント (myvmware.com) に移動し、[VMware NSX-T Data Center] - [ダウンロード] の順に移動します。
- 2 ベアメタルの NSX Edge の ISO ファイルを見つけて、ダウンロードします。
- 3 HP iLO (Integrated Lights-Out) などのベアメタルのアウトオブバンド管理インターフェイスにログインします。
- 4 仮想コンソール プレビューで [起動] をクリックします。
- 5 [仮想メディア] - [仮想メディアに接続] の順に選択します。
 仮想メディアの接続を数秒間待機します。
- 6 [仮想メディア] - [CD/DVD のマッピング] の順に選択し、ISO ファイルを参照します。
- 7 [次回起動] - [仮想 CD/DVD/ISO] の順に選択します。

- 8 [電源] - [システムのリセット (ウォーム ブート)] の順に選択します。

インストール時間は、ベア メタル環境によって異なります。

- 9 [自動インストール] を選択します。

Enter キーを押した後、開始するまでに 10 秒程かかる可能性があります。

- 10 適切なプライマリ ネットワーク インターフェイスを選択します。

パワーオン中に、インストーラから DHCP を介したネットワーク構成を求められます。環境内で DHCP を使用できない場合は、インストーラに IP アドレスの設定を求めるプロンプトが表示されます。

デフォルトでは、root のログイン パスワードは [vmware] で、admin のログイン パスワードは [default] です。

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

コンソール ウィンドウが開かない場合は、ポップアップが許可されていることを確認してください。

- 12 NSX Edge が起動したら、管理者認証情報を使用して CLI にログインします。

注： NSX Edge の起動後、最初のログイン時に管理者認証情報を使用しなかった場合、データ プレーン サービスは NSX Edge で自動的に開始されません。

- 13 再起動後、管理者または root のいずれかの認証情報でログインできます。デフォルトの root パスワードは **vmware** です。

- 14 管理インターフェイスの設定方法は 3 つあります。

注： サーバが Mellanox NIC カードを使用している場合は、インバンド管理インターフェイスで Edge を設定しないでください。

- タグのないインターフェイス。このインターフェイス タイプは、アウトオブバンド管理インターフェイスを作成します。

```
(DHCP) set interface eth0 dhcp plane mgmt
```

```
(静的) set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt
```

- タグ付きインターフェイス。

```
set interface eth0 vlan <vlan_ID> plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(静的) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- インバンド インターフェイス。

```
set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(静的) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- (オプション) 複数のインターフェイスを持つ HA 管理インターフェイスに **bond0** インターフェイスを作成します。

次の CLI コマンドを使用すると、NSX Edge でボンディング管理インターフェイスを設定できます。ボンディングを作成してインターフェイスを追加する前に、コンソールを使用して既存の管理 IP アドレスを消去します。

注： ボンディング インターフェイスでは、アクティブ/バックアップ モードのみが許可されます。VLAN を設定することはできません。そのため、物理スイッチに近いアクセス VLAN に VLAN を設定する必要があります。

```
set interface bond0 ip x.x.x.x/mask gateway x.x.x.x plane mgmt mode
active-backup members eth0, eth1 primary eth0
```

- 15 `get interface eth0` コマンド (VLAN なし) または `get interface eth0.<vlan_ID>` コマンド (VLAN あり) を実行し、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。

```
nsx-edge-1> [get interface eth0.100]

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

注： NSX で管理されていないホストで NSX Edge 仮想マシンを起動する場合は、データ NIC の物理ホストスイッチで MTU 設定が 1500 ではなく 1600 に設定されていることを確認します。

- 16 (タグ付きインターフェイスとインバンド インターフェイス) 新しいインターフェイスを作成する前に、既存の VLAN 管理インターフェイスをクリアする必要があります。

```
clear interface eth0.<vlan_ID>
```

新しいインターフェイスを設定するには、手順 13 を参照してください。

- 17 使用可能な PCI デバイスのリストから、NSX-T Data Center データプレーンが使用する物理 NIC を設定します。

- a `get dataplace device list`
- b `set dataplane device list <NIC1>, <NIC2>, <NIC3>`
- c `restart service dataplane`
- d `get physical-port`

物理 NIC を選択したら、NSX-T Data Center データプレーン サービスを再起動して変更を有効にします。

注： 最大 16 個までの物理 NIC を要求できます。

18 ネットワーク構成エラーを回避するため、選択した物理 NIC がトランスポート ノード プロファイルの NIC と一致していることを確認します。

19 トランスポート ノードとして NSX Edge を作成する前に、データプレーンの NIC リストをリセットします。

```
reset dataplane nic list
```

20 NSX Edge アプライアンスで必要な接続が可能であることを確認します。

SSH を有効にした場合は、SSH を使用して NSX Edge に接続できることを確認します。

- NSX Edge に ping を実行できます。
- NSX Edge は、デフォルト ゲートウェイに ping を実行できます。
- NSX Edge は、NSX Edge と同じネットワーク上のハイパーバイザー ホストに ping を実行できます。
- NSX Edge は、DNS サーバと NTP サーバに ping を実行できます。

21 接続問題のトラブルシューティングを行います。

注： 接続が確立されていない場合は、仮想マシン ネットワーク アダプタが適切なネットワークまたは VLAN に置かれていることを確認します。

デフォルトでは、NSX Edge データパスは、管理 NIC (IP アドレスとデフォルト ルートを持つ NIC) を除くすべての仮想マシン NIC を要求します。管理インターフェイスとして NIC を誤って割り当てた場合は、次の手順に従って DHCP を使用し、正しい NIC に管理 IP アドレスを割り当てます。

- a CLI にログインして **stop service dataplane** コマンドを入力します。
- b **set interface interface dhcp plane mgmt** コマンドを入力します。
- c *interface* を DHCP ネットワークに置き、IP アドレスが *interface* に割り当てられるまで待ちます。
- d **start service dataplane** コマンドを入力します。

VLAN アップリンクとトンネル オーバーレイに使用するデータパス fp-ethX ポートが、NSX Edge 上で [get interfaces] コマンドと [get physical-port] コマンドに示されます。

次のステップ

管理プレーンに NSX Edge を参加させなかった場合は、[NSX Edge の管理プレーンへの追加](#)を参照してください。

ISO ファイルを使用した NSX Edge のインタラクティブ インストール

ISO ファイルを使用して、インタラクティブ モードで NSX Edge デバイスをベアメタルにインストールします。

前提条件

- システム BIOS モードがレガシー BIOS に設定されていることを確認します。
- [NSX Edge のインストール要件](#)で NSX Edge のネットワーク要件を参照してください。

手順

- 1 MyVMware アカウント (myvmware.com) に移動し、[VMware NSX-T Data Center] - [ダウンロード] の順に移動します。
- 2 ベアメタルの NSX Edge の ISO ファイルを見つけて、ダウンロードします。
- 3 ベア メタルの ILO にログインします。
- 4 仮想コンソール プレビューで [起動] をクリックします。
- 5 [仮想メディア] - [仮想メディアに接続] の順に選択します。
仮想メディアの接続を数秒間待機します。
- 6 [仮想メディア] - [CD/DVD のマッピング] の順に選択し、ISO ファイルを参照します。
- 7 [次回起動] - [仮想 CD/DVD/ISO] の順に選択します。
- 8 [電源] - [システムのリセット (ウォーム ブート)] の順に選択します。
インストール時間は、ベア メタル環境によって異なります。
- 9 [インタラクティブ インストール] を選択します。
Enter キーを押した後、開始するまでに 10 秒程かかる可能性があります。
- 10 [キーボードの設定] 画面で、インストーラがキーボードを自動検出する必要がある場合は **Yes** を選択します。
必要がない場合は、**No** を選択します。
- 11 言語として [英語 US] を選択します。
- 12 [ネットワークの設定] 画面で、該当するプライマリ ネットワーク インターフェイスを選択します。
- 13 選択したプライマリ インターフェイスに接続するホスト名を入力し、**Ok** をクリックします。

パワーオン中に、インストーラから DHCP を介したネットワーク構成を求められます。環境内で DHCP を使用できない場合は、インストーラに IP アドレスの設定を求めるプロンプトが表示されます。

デフォルトでは、root のログイン パスワードは [vmware] で、admin のログイン パスワードは [default] です。
- 14 [kickstart を使用して NSX アプライアンスを設定] 画面で、次の操作を行います。
 - ベアメタル サーバで NSX の構成を自動化する場合は、NSX kickstart 構成ファイルの URL を入力します。
 - ベアメタル サーバで NSX を手動で構成する場合は、このフィールドを空白のままにします。
- 15 [パーティション ディスク] 画面で、次のいずれかのオプションを選択します。
 - 既存のパーティションのマウントを解除して、ディスクに新しいパーティションを作成できるようにするには、**Yes** を選択します。
 - 既存のパーティションを使用する場合は、**No** を選択します。

- 16 NSX Edge が起動したら、管理者認証情報を使用して CLI にログインします。

注： NSX Edge の起動後、最初のログイン時に管理者認証情報を使用しなかった場合、データ プレーン サービスは NSX Edge で自動的に開始されません。

- 17 `get interface eth0` コマンド (VLAN なし) または `get interface eth0.<vlan_ID>` コマンド (VLAN あり) を実行し、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。

```
nsx-edge-1> [get interface eth0.100]

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

注： NSX で管理されていないホストで NSX Edge 仮想マシンを起動する場合は、データ NIC の物理ホストスイッチで MTU 設定が 1500 ではなく 1600 に設定されていることを確認します。

- 18 接続問題のトラブルシューティングを行います。

注： 接続が確立されていない場合は、仮想マシン ネットワーク アダプタが適切なネットワークまたは VLAN に置かれていることを確認します。

デフォルトでは、NSX Edge データパスは、管理 NIC (IP アドレスとデフォルト ルートを持つ NIC) を除くすべての仮想マシン NIC を要求します。管理インターフェイスとして NIC を誤って割り当てた場合は、次の手順に従って DHCP を使用し、正しい NIC に管理 IP アドレスを割り当てます。

- a CLI にログインして **stop service dataplane** コマンドを入力します。
- b **set interface interface dhcp plane mgmt** コマンドを入力します。
- c *interface* を DHCP ネットワークに置き、IP アドレスが *interface* に割り当てられるまで待ちます。
- d **start service dataplane** コマンドを入力します。

VLAN アップリンクとトンネル オーバーレイに使用するデータパス fp-ethX ポートが、NSX Edge 上で `[get interfaces]` コマンドと `[get physical-port]` コマンドに示されます。

次のステップ

管理プレーンに NSX Edge を追加しなかった場合は、[NSX Edge の管理プレーンへの追加](#)を参照してください。

NSX Edge の管理プレーンへの追加

NSX Edge を管理プレーンに追加すると、NSX Manager と NSX Edge が相互に通信できるようになります。

前提条件

NSX Edge および NSX Manager アプライアンスにログインするための管理者権限を持っていることを確認します。

手順

- 1 NSX Manager アプライアンスのいずれかと SSH セッションまたはコンソール セッションを開きます。
- 2 NSX Edge ノード仮想マシンとの SSH セッションまたはコンソール セッションを開きます。
- 3 NSX Manager アプライアンスで `get certificate api thumbprint` コマンドを実行します。

コマンド出力は、この NSX Manager に固有の一連の英数字です。

次はその例です。

```
NSX-Manager1> get certificate api thumbprint
659442c1435350edbbc0e87ed5a6980d892b9118f851c17a13ec76a8b985f57
```

- 4 NSX Edge ノード仮想マシンで `[join management-plane]` コマンドを実行します。

このとき、次の情報を指定します。

- NSX Manager のホスト名または IP アドレスとオプションでポート番号
- NSX Manager のユーザー名
- NSX Manager の証明書サムプリント
- NSX Manager のパスワード

```
NSX-Edge1> join management-plane <Manager-IP> thumbprint <Manager-thumbprint> username
admin
```

このコマンドを各 NSX Edge ノード仮想マシンで繰り返します。

- 5 NSX Edge ノード仮想マシンで `get managers` コマンドを実行して結果を確認します。

```
nsx-edge-1> get managers
- 10.173.161.17 Connected (NSX-RPC)
- 10.173.161.140 Connected (NSX-RPC)
- 10.173.160.204 Connected (NSX-RPC)
```

- 6 NSX Manager ユーザー インターフェイスで [システム] - [ファブリック] - [ノード] - [Edge トランスポート ノード] の順に移動します。

[NSX Edge トランスポート ノード] ページで、次の操作を行います。

- [設定の状態] 列に [NSX の設定] が表示されます。[NSX の設定] をクリックして、ノードでの構成を開始します。ノードにインストールされているバージョン番号が [NSX バージョン] 列に表示されていない場合は、ブラウザ画面を更新してください。

- NSX Edge ノードで NSX を設定する前に、[ノードの状態] 列と [トンネルの状態] 列に「使用不可」が表示されます。[トランスポート ゾーン] 列と [N-VDS スイッチ] 列に、0 が表示されます。これは、接続されたトランスポート ゾーンまたは NSX Edge ノードに設定されている N-VDS スイッチがないことを示しています。

次のステップ

NSX Manager を使用して NSX Edge をインストールする場合は、[NSX Edge トランスポート ノードの作成](#)を参照してください。

NSX Edge を手動でインストールする場合は、[トランスポート ノードとしての NSX Edge の設定](#)を参照してください。

トランスポート ノードとしての NSX Edge の設定

ESXi またはベアメタルに NSX Edge を手動でインストールした後に、NSX Edge をトランスポート ノードとして NSX-T Data Center ファブリックに設定します。

トランスポート ノードは、NSX-T Data Center オーバーレイまたは NSX-T Data Center VLAN ネットワークに参加できるノードです。N-VDS が含まれているノードは、トランスポート ノードとして機能します。これらのノードには NSX Edge が含まれていますが、これらに限定されません。

NSX Edge は、1つのオーバーレイ トランスポート ゾーンおよび複数の VLAN トランスポート ゾーンに属することができます。仮想マシンから外部へのアクセスが必要な場合は、NSX Edge が、仮想マシンの論理スイッチが属しているの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。通常、NSX Edge は1つ以上の VLAN トランスポート ゾーンに属して、アップリンク アクセスを提供します。

前提条件

- トランスポート ゾーンが設定されている必要があります。
- コンピュート マネージャが設定されていることを確認します。[コンピュー ト マネージャの追加](#) を参照してください。
- アップリンク プロファイルが設定されている必要があります。設定されていない場合は、ベア メタル NSX Edge ノード用のデフォルトのアップリンク プロファイルを使用できます。
- IP アドレス プールが設定されているか、ネットワーク環境内の IP アドレス プールを使用できる必要があります。
- ホストまたは NSX Edge ノード上で1個以上の未使用の物理 NIC が必要です。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] > [ファブリック] > [ノード] > [Edge トランスポート ノード] > [Edge の編集] の順に選択します。
- 3 Edge ノードを選択して、[編集] をクリックします。

- 4 このトランスポート ノードが属するトランスポート ゾーンを選択します。

NSX Edge トランスポート ノードは 2 つ以上のトランスポート ゾーン（NSX-T Data Center 接続用のオーバーレイとアップリンク接続用の VLAN）に属します。

注： トランスポート ゾーン内の複数の VTEP を同じネットワーク セグメントに設定する必要があります。トランスポート ゾーンの VTEP を異なるネットワーク セグメントに設定すると、VTEP 間で BFD セッションを確立できません。

- 5 N-VDS の情報を入力します。

オプション	説明
Edge スイッチ名	ドロップダウン メニューから VLAN スイッチを選択します。
アップリンク プロファイル	ドロップダウン メニューからアップリンク プロファイルを選択します。 使用可能なアップリンクは、選択したアップリンク プロファイルでの設定によって異なります。
IP の割り当て	オーバーレイ N-VDS に [IP プールを使用] または [固定 IP のリストを使用] を選択します。 これらの IP アドレスは、VTEP として NSX Edge トランスポート ノードに割り当てられます。 NSX Edge 上に複数の VTEP がある場合、同じサブネット内に存在する必要があります。 <ul style="list-style-type: none"> ■ [固定 IP アドレスのリストを使用] を選択した場合は、IP アドレス、ゲートウェイ、およびサブネット マスクのコンマ区切りのリストを指定する必要があります。 ■ IP 割り当てに [IP プールを使用] を選択した場合は、IP プール名を指定します。
DPPK Fastpath インターフェイス/仮想 NIC	アップリンク インターフェイスのデータ パス インターフェイス名を選択します。 <p>注： 指定されたチーミング ポリシーで設定された論理スイッチを経由してトラフィックが送信されるようにするには、デフォルトのチーミング ポリシーのすべてのアップリンクを NSX Edge 仮想マシンの物理ネットワーク インターフェイスにマッピングします。</p>

- 6 [トランスポート ノード] ページで接続ステータスを表示します。

NSX Edge をトランスポート ノードとして追加した後、接続状態は 10 ～ 12 分後に [稼動中] に変わります。

- 7 （オプション） GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API 呼び出しを使用して、トランスポート ノードを確認します。
- 8 （オプション） 状態の情報を確認するには、GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 呼び出しを使用します。
- 9 vCenter Server を使用して NSX Edge ノードを新しいホストに移行した後、NSX Manager ユーザー インターフェイスに NSX Edge の古い設定情報（コンピュート、データストア、ネットワーク、SSH、NTP、DNS、検索ドメイン）が表示されることがあります。新しいホストで NSX Edge の最新の設定情報を取得するには、API コマンドを実行します。

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

次のステップ

NSX Edge ノードを NSX Edge クラスタに追加します。[NSX Edge クラスタの作成](#) を参照してください。

トランスポート ゾーンとトランスポート ノード

10

トランスポート ゾーンとトランスポート ノードは、NSX-T Data Center における重要な概念です。

この章には、次のトピックが含まれています。

- トランスポート ゾーンの作成
- トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成
- 拡張データ バス
- プロファイルの設定
- スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成
- NSX-T Data Center カーネル モジュールの手動インストール
- 最小の vSphere クラスタ NSX-T の展開

トランスポート ゾーンの実成

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ホストと仮想マシンを指定します。トランスポート ゾーンで論理スイッチを認識できるホストを制限し、論理スイッチに接続できる仮想マシンを制限することで、この制御が実現します。1つのトランスポート ゾーンの範囲が、1つ以上のクラスタにまたがることができます。

NSX-T Data Center 環境には、要件に基づいて1つ以上のトランスポート ゾーンを含めることができます。1台のホストが、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 ゾーンのみ属することができます。

NSX-T Data Center では、レイヤー 2 ネットワークの異なるトランスポート ゾーンにある仮想マシンに接続できません。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。

オーバーレイ トランスポート ゾーンは、ホスト トランスポート ノードと NSX Edge の両方で使用されます。ホストまたは NSX Edge トランスポート ノードがオーバーレイ トランスポート ゾーンに追加されると、N-VDS がそのホストまたは NSX Edge にインストールされます。

VLAN トランスポート ゾーンは、NSX Edge およびホストのトランスポート ゾーンが VLAN アップリンクに使用します。NSX Edge が VLAN トランスポート ゾーンに追加されると、VLAN N-VDS が NSX Edge にインストールされます。

N-VDS によって論理ルーター アップリンクおよびダウンリンクが物理 NIC にバインドされることで、仮想から物理へのパケット フローが可能になります。

トランスポート ゾーンを作成する際には、そのトランスポート ゾーンに後で追加されるトランスポート ノードにインストールされる、N-VDS の名前を指定する必要があります。N-VDS には任意の名前を付けることができます。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [トランスポート ゾーン] - [追加] を選択します。
- 3 トランスポート ゾーンの名前と、必要に応じて説明を入力します。
- 4 N-VDS の名前を入力します。
- 5 N-VDS モードを選択します。
 - [標準] モードはサポートされているすべてのホストに適用されます。
 - [拡張データパス] はネットワーク スタック モードで、トランスポート ゾーンに属することができる、ESXi ホスト バージョン 6.7 以降のタイプのトランスポート ノードのみに適用されます。
- 6 N-VDS モードを [標準] に設定した場合は、トラフィック タイプを選択します。
オプションは、[オーバーレイ] と [VLAN] です。
- 7 N-VDS モードを [拡張データパス] に設定した場合は、トラフィック タイプを選択します。
オプションは、[オーバーレイ] と [VLAN] です。

注： [拡張データパス] モードでは、特定の NIC 構成のみがサポートされます。サポート対象の NIC を構成していることを確認します。

- 8 1 つ以上のアップリンク チーミング ポリシー名を入力します。これらの名前付きチーミング ポリシーは、トランスポート ゾーンに接続される論理スイッチで使用できます。論理スイッチで一致する名前付きチーミング ポリシーが見つからない場合は、デフォルトのアップリンク チーミング ポリシーが使用されます。
- 9 [トランスポート ゾーン] ページで、新規トランスポート ゾーンを確認します。
- 10 (オプション) 新しいトランスポート ゾーンは、GET <https://<nsx-mgr>/api/v1/transport-zones> API 呼び出しで確認することもできます。

```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ]
}
```

```

    }
  ],
  "_create_time": 1459547126454,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_last_modified_time": 1459547126454,
  "_create_user": "admin",
  "_revision": 0,
  "_schema": "/v1/schema/TransportZone"
},
{
  "resource_type": "TransportZone",
  "description": "comp vlan transport zone",
  "id": "9b661aed-1eaa-4567-9408-ccbcfe50b416",
  "display_name": "tz-vlan",
  "host_switch_name": "vlan-uplink-hostswitch",
  "transport_type": "VLAN",
  "transport_zone_profile_ids": [
    {
      "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
      "resource_type": "BfdHealthMonitoringProfile"
    }
  ],
  "_create_time": 1459547126505,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_last_modified_time": 1459547126505,
  "_create_user": "admin",
  "_revision": 0,
  "_schema": "/v1/schema/TransportZone"
}
]
}

```

次のステップ

オプションで、カスタム トランスポート ゾーン プロファイルを作成し、それをトランスポート ゾーンにバインドします。カスタム トランスポート ゾーン プロファイルは、POST /api/v1/transportzone-profiles API を使用して作成できます。トランスポート ゾーン プロファイルの作成にユーザー インターフェイスを使用するワークフローはありません。トランスポート ゾーン プロファイルの作成後は、PUT /api/v1/transport-zones/<transport-zone-id> API を使用してトランスポート ゾーンで確認できます。

トランスポート ノードを作成します。 [スタンドアロン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成

トンネル エンドポイント用に IP アドレス プールを使用できます。トンネル エンドポイントは、NSX-T Data Center でカプセル化されたオーバーレイ フレームの送信と終了を行うハイパーバイザー ホストを識別するために外部 IP ヘッダで使用される、送信先 IP アドレスと宛先 IP アドレスです。トンネル エンドポイントの IP アドレスには、DHCP または手動で設定した IP アドレス プールも使用できます。

ESXi ホストと KVM ホストの両方を使用している場合、設計オプションの 1 つとして、ESXi トンネル エンドポイント IP アドレス プール (sub_a) と KVM トンネル エンドポイント IP アドレス プール (sub_b) 用に 2 つの異なるサブネットを使用できます。この場合、専用のデフォルト ゲートウェイを使用して、KVM ホスト上で sub_a へのスタティック ルートを追加する必要があります。

次の例は、sub_a が 192.168.140.0 で sub_b が 192.168.150.0 の、Ubuntu ホスト上のルーティング テーブルを示しています（たとえば、管理サブネットは 192.168.130.0 になります）。

カーネル IP アドレス ルーティング テーブル：

Destination	Gateway	Genmask	Iface
0.0.0.0	192.168.130.1	0.0.0.0	eth0
192.168.122.0	0.0.0.0	255.255.255.0	virbr0
192.168.130.0	0.0.0.0	255.255.255.0	eth0
192.168.140.0	192.168.150.1	255.255.255.0	nsx-vtep0.0
192.168.150.0	0.0.0.0	255.255.255.0	nsx-vtep0.0

root は複数の方法で追加できます。たとえば次の 2 つの方法があります。2 つの方法のうち、インターフェイスを編集してルートを追加した場合のみ、ホストの再起動後もルートが維持されます。route add コマンドを使用して追加したルートは、ホストの再起動後は維持されません。

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

/etc/network/interfaces の「up ifconfig nsx-vtep0.0 up」の前に、このスタティック ルートを追加します。

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [ネットワークとセキュリティの詳細設定] - [インベントリ] - [グループ] - [IP アドレス プール] - [追加] を選択します。
- 3 IP アドレス プールの詳細を入力します。

オプション	パラメータの例
名前と説明	IP アドレス プールとオプションの説明を入力します。
IP アドレス範囲	IP アドレス割り当ての範囲 192.168.200.100 - 192.168.200.115
ゲートウェイ	192.168.200.1
CIDR	CIDR 形式のネットワーク アドレス 192.168.200.0/24
DNS サーバ	DNS サーバのカンマ区切りのリスト 192.168.66.10
DNS サフィックス	corp.local

結果

IPv4 または IPv6 アドレスのプールは、[IP アドレス プール] の画面にリストされます。

IP アドレス プールのリストは、GET <https://<nsx-mgr>/api/v1/pools/ip-pools> API 呼び出しを使用して表示することもできます。

次のステップ

アップリンク プロファイルを作成します。[アップリンク プロファイルの作成](#) を参照してください。

拡張データ パス

拡張データ パスはネットワーク スタック モードであり、これを構成することで優れたネットワーク パフォーマンスを実現します。これは主に NFV ワークロードを対象としたもので、DPDK 機能を利用してパフォーマンスを向上させます。

N-VDS スイッチは、ESXi ホスト上でのみ拡張データ パス モードで設定できます。ENS は、Edge 仮想マシンを通過するトラフィックもサポートします。

拡張データ パス モードでは、両方のトラフィック モードがサポートされます。

- オーバーレイ トラフィック
- VLAN トラフィック

サポートされる VMkernel NIC

複数の ENS ホスト スイッチをサポートする NSX-T Data Center では、ホストあたりのサポートされる VMkernel NIC の最大数は 32 です。

拡張データ パスを構成する手順の概要

ネットワーク管理者は、拡張データ パス モードで N-VDS をサポートするトランスポート ゾーンを作成する前に、サポートされている NIC カードおよびドライバを使用してネットワークを準備する必要があります。ネットワーク パフォーマンスを向上させるために、ロード バランシングされた送信元チーミング ポリシーを有効にして、NUMA ノードを認識させることができます。

手順の概要は次のとおりです。

- 1 拡張データ パスをサポートする NIC カードを使用します。

拡張データ パスをサポートする NIC カードについては、[VMware 互換性ガイド](#) を参照してください。

VMware 互換性ガイドのページの [I/O デバイス] カテゴリで、[ESXi 6.7]、I/O デバイスのタイプに [ネットワーク]、機能に [N-VDS 拡張データパス] を選択します。

- 2 [My VMware ページ](#) から最新の NIC ドライバをダウンロードしてインストールします。

- a [ドライバ & ツール] > [ドライバ CD] の順に移動します。
- b NIC ドライバをダウンロードします。

VMware ESXi 6.7 ixgben-ens 1.1.3 NIC Driver for Intel Ethernet
Controllers 82599, x520, x540, x550, and x552 family

Intel Ethernet Controllers X710、XL710、XXV710、X722 ファミリー向け VMware ESXi
6.7 i40en-ens 1.1.3 NIC ドライバ

- c ホストを ENS ホストとして使用するには、システムで少なくとも 1 つの ENS 対応 NIC が使用可能である必要があります。ENS 対応 NIC が 1 つも存在しない場合、管理プレーンは、ENS トランスポート ゾーンへのホストの追加を許可しません。

- d ENS ドライバを一覧表示します。

```
esxcli software vib list | grep -E "i40|ixgben"
```

- e NIC が ENS データパス トラフィックを処理できるかどうか確認します。

```
esxcfg-nics -e
```

Name	Driver	ENS Capable	ENS Driven	MAC Address
Description				
vmnic0	ixgben	True	False	e4:43:4b:7b:d2:e0 Intel(R) Ethernet Controller X550
vmnic1	ixgben	True	False	e4:43:4b:7b:d2:e1 Intel(R) Ethernet Controller X550
vmnic2	ixgben	True	False	e4:43:4b:7b:d2:e2 Intel(R) Ethernet Controller X550
vmnic3	ixgben	True	False	e4:43:4b:7b:d2:e3 Intel(R) Ethernet Controller X550
vmnic4	i40en	True	False	3c:fd:fe:7c:47:40 Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic5	i40en	True	False	3c:fd:fe:7c:47:41 Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic6	i40en	True	False	3c:fd:fe:7c:47:42 Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic7	i40en	True	False	3c:fd:fe:7c:47:43 Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T

- f ENS ドライバをインストールします。

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- g あるいは、システムにドライバをダウンロードしてインストールします。

```
wget <DriverInstallerURL>
```

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- h ホストを再起動して、ドライバを読み込みます。次の手順に進みます。

- i ドライバをアンロードするには、次の手順を実行します。

```
vmkload_mod -u i40en
```

```
ps | grep vmkdevmgr
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
ps | grep vmkdevmgr
kill -HUP <vmkdevmgrProcessID>
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

- j ENS ドライバをアンインストールするには、`esxcli software vib remove --vibName=i40en-ens --force --no-live-install` を実行します。

- 3 アップリンク ポリシーを作成します。

[アップリンク プロファイルの作成](#) を参照してください。

- 4 N-VDS を持つトランスポート ゾーンを拡張データ パス モードで作成します。

[トランスポート ゾーンの作成](#) を参照してください。

注： オーバーレイ トラフィック用に設定された ENS トランスポート ゾーン：バージョン 11.0.0 より前の VMware Tools を実行し、vNIC タイプが VMXNET3 の Microsoft Windows 仮想マシンの場合、MTU が 1500 に設定されていることを確認します。vSphere 6.7 U1 とバージョン 11.0.0 以降の VMware Tools を実行している Microsoft Windows 仮想マシンの場合、MTU が 8900 未満の値に設定されていることを確認します。サポートされている他の OS を実行している仮想マシンの場合、仮想マシンの MTU が 8900 未満の値に設定されていることを確認します。

- 5 ホスト トランスポート ノードを作成します。論理コアと NUMA ノードを持つ拡張データ パス N-VDS を設定します。

[スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

NUMA を認識するロード バランシングされた送信元チーミング ポリシー モード

拡張データパス N-VDS に定義されたロード バランシングされた送信元チーミング ポリシー モードは、次の条件が満たされると、NUMA を認識します。

- 仮想マシンの [遅延感知] は [高] です。
- 使用されるネットワーク アダプタのタイプは VMXNET3 です。

仮想マシンまたは物理 NIC のいずれかの NUMA ノードの場所が利用できない場合、ロード バランシングされた送信元チーミング ポリシーは、NUMA が認識されるかどうかは考慮せずに、仮想マシンおよび NIC を調整します。

次の条件では、チーミング ポリシーは NUMA を認識せずに機能します。

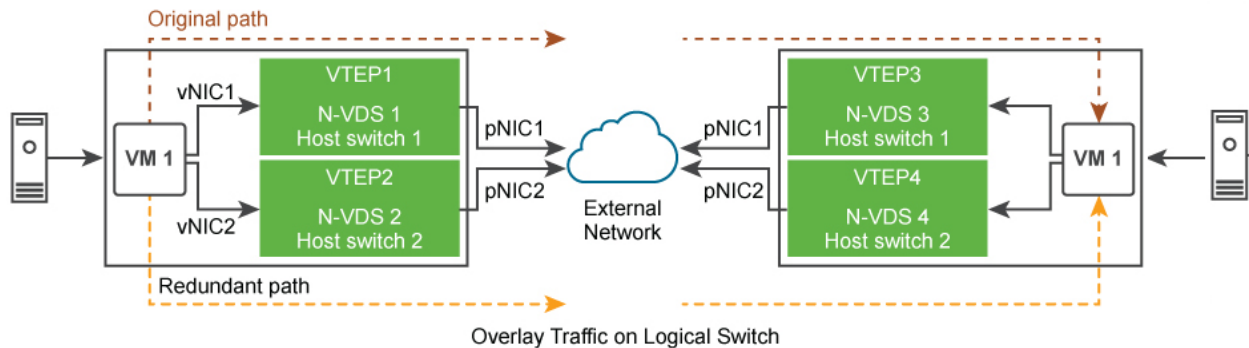
- LAG アップリンクが複数の NUMA ノードからの物理リンクで構成されている。
- 仮想マシンに複数の NUMA ノードとのアフィニティがある。
- ESXi ホストが仮想マシンまたは物理リンクのいずれかの NUMA 情報を定義できない。

トラフィックの信頼性を必要とするアプリケーションの ENS サポート

アプリケーションで実行されているトラフィックの回復性と信頼性を向上させるため、NFV ワークロードは SCTP (Stream Control Transmission Protocol) によって提供されるマルチホーミング機能と冗長化機能を使用する場合があります。マルチホーミングは、ソース仮想マシンからターゲット仮想マシンへの冗長パスをサポートする機能です。

オーバーレイまたは VLAN ネットワークのアップリンクとして使用可能な物理 NIC の数によっては、これらの多くの冗長ネットワークパスは、仮想マシンがトラフィックをターゲット仮想マシンに送信する際に使用できます。論理スイッチに固定された物理 NIC が失敗すると、冗長パスが使用されます。拡張データパススイッチは、ホスト間の冗長ネットワークパスを提供します。

図 10-1. ENS でのトラフィックのマルチホーミングと冗長性



タスクの概要は次のとおりです。

- 1 ホストを NSX-T Data Center トランスポート ノードとして準備します。
- 2 拡張データパス モードで、2 台の N-VDS スイッチを含む VLAN またはオーバーレイ トランスポート ゾーンを準備します。
- 3 N-VDS 1 で、スイッチに最初の物理 NIC を固定します。
- 4 N-VDS 2 で、スイッチに 2 台目の物理 NIC を固定します。

拡張データパス モードの N-VDS では、pNIC1 が使用できなくなった場合でも、VM 1 からのトラフィックは冗長パス vNIC 1 → トンネル エンドポイント 2 → pNIC 2 → VM 2 を経路するようにルーティングされます。

プロファイルの設定

プロファイルを使用すると、複数のホストやノードのネットワーク アダプタに同じ機能を一貫した方法で設定できます。

プロファイルは、ネットワーク アダプタに設定するプロパティや機能のコンテナです。ネットワーク アダプタごとにプロパティや機能を個別に設定するのではなく、プロファイルで機能を指定し、このプロファイルを複数のホストまたはノードに適用することができます。

アップリンク プロファイルの作成

アップリンクは、NSX Edge ノードからトップオブラック スイッチまたは NSX-T Data Center 論理スイッチへのリンクです。リンクは、NSX Edge ノード上の物理ネットワーク インターフェイスからスイッチへのリンクです。

アップリンク プロファイルは、アップリンクのポリシーを定義します。アップリンク プロファイルでは、チーミング ポリシー、アクティブ/スタンバイ リンク、トランスポート VLAN ID、MTU 設定などを定義します。

仮想マシン アプライアンス ベースの NSX Edge ノードとホスト トランスポート ノードのアップリンクの設定：

- アップリンク プロファイルにフェイルオーバー チーミング ポリシーが設定されている場合、チーミング ポリシーに設定できるアクティブ アップリンクは1つのみです。スタンバイ アップリンクはサポートされていないため、フェイルオーバー チーミング ポリシーで設定することはできません。仮想アプライアンスまたはホスト トランスポート ノードとして NSX Edge をインストールする場合は、デフォルトのアップリンク プロファイルを使用します。
- ロード バランシングされたソース チーミング ポリシーがアップリンク プロファイルに設定されている場合は、同じ N-VDS 上に複数のアクティブ アップリンクを設定できます。それぞれのアップリンクには、一意の名前と IP アドレスを持つ1つの物理 NIC が関連付けられます。アップリンク エンドポイントに割り当てられた IP アドレスは、N-VDS の IP 割り当てを使用して設定できます。

トラフィックのロード バランシングには、[ロード バランシングされた送信元] チーミング ポリシーを使用する必要があります。

前提条件

- [NSX Edge のインストール要件](#)で NSX Edge のネットワーク要件を参照してください。
- アップリンク プロファイル内の各アップリンクは、ハイパーバイザー ホストまたは NSX Edge ノードの、稼動中で使用可能な物理リンクに対応している必要があります。

たとえば、ハイパーバイザー ホストで稼動中の物理リンクとして、vmnic0 と vmnic1 の 2 つがあるとします。vmnic0 は管理ネットワークとストレージ ネットワークに使用され、vmnic1 は未使用であるとします。この場合、vmnic1 を NSX-T Data Center のアップリンクとして使用できますが、vmnic0 は使用できません。リンクのチーミングを行うには、vmnic1 と vmnic2 など、未使用の物理リンクが 2 つ必要です。

NSX Edge については、トンネル エンドポイントと VLAN アップリンクに同じ物理リンクを使用できます。たとえば、vmnic0/eth0/em0 を管理ネットワークに使用し、vmnic1/eth1/em1 を fp-ethX リンクに使用することが可能です。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [アップリンク プロファイル] - [追加] を選択します。

3 アップリンク プロファイルの詳細を入力します。

オプション	説明
名前と説明	<p>アップリンク プロファイルの名前を入力します。</p> <p>オプションで、アップリンク プロファイルの説明を追加します。</p>
LAG	<p>(オプション) リンク集約グループ (LAG) がトランスポート ネットワークで Link Aggregation Control Protocol (LACP) を使用する場合は、LAG セクションで [追加] をクリックします。</p> <p>注： LACP の場合、複数の LAG は KVM ホストでサポートされません。</p> <p>作成するアクティブ アップリンクとスタンバイ アップリンクの名前には、物理リンクを表す任意のテキストを指定できます。これらのアップリンク名は、後でトランスポート ノードを作成するときに参照します。トランスポート ノードのユーザー インターフェイス/API で、各アップリンク名に対応する物理リンクを指定できます。</p> <p>LAG ハッシュ メカニズムで使用可能なオプション：</p> <ul style="list-style-type: none"> ■ 送信元の MAC アドレス ■ 宛先の MAC アドレス ■ 送信元および宛先の MAC アドレス ■ 送信元および宛先の IP アドレスおよび VLAN ■ 送信元および宛先の MAC アドレス、IP アドレス、TCP/UDP ポート
チーミング	<p>[チーミング] セクションでは、デフォルトのチーミング ポリシーを入力できます。名前付きのチーミング ポリシーを入力することもできます。名前付きチーミング ポリシーを追加するには、[追加] をクリックします。チーミング ポリシーは、N-VDS で冗長性とトラフィックのロード バランシングのためにアップリンクをどのように使用するかを定義します。次のモードで、チーミング ポリシーを設定できます。</p> <ul style="list-style-type: none"> ■ [フェイルオーバーの順序]：1つのアクティブ アップリンクと、オプションでスタンバイ アップリンクのリストを選択します。アクティブ アップリンクに障害が発生した場合、スタンバイ リスト内の次のアップリンクで置き換えられます。このオプションでは、ロード バランシングは実際には実行されません。 ■ [ロード バランシングの送信元]：アクティブ アップリンクのリストを選択します。トランスポート ノードを構成するときに、トランスポート ノードの各インターフェイスを1つのアクティブ アップリンクに固定できます。この構成では、同時に複数のアクティブ アップリンクを使用できます。 ■ [ロード バランシングの送信元の MAC アドレス]：ソースのイーサネット MAC アドレスのハッシュに基づいてアップリンクを選択します。 <p>注：</p> <ul style="list-style-type: none"> ■ KVM ホスト：フェイルオーバー順序のチーミング ポリシーのみがサポートされますが、ロード バランシングの送信元とロード バランシングの送信元の MAC アドレスのチーミング ポリシーはサポートされません。 ■ NSX Edge：デフォルトのチーミング ポリシーでは、ロード バランシングの送信元とフェイルオーバー順序のチーミング ポリシーがサポートされます。名前付きのチーミング ポリシーでは、フェイルオーバー順序ポリシーのみがサポートされます。 ■ ESXi ホスト：ロード バランシングの送信元の MAC アドレス、ロード バランシングの送信元、フェイルオーバー順序のチーミング ポリシーがサポートされます。 <p>(ESXi ホストと NSX Edge) トランスポート ゾーンに次のポリシーを定義できます。</p> <ul style="list-style-type: none"> ■ セグメントまたは VLAN ベースの論理スイッチごとの名前付きチーミング ポリシー。 ■ N-VDS 全体のデフォルトのチーミング ポリシー。

オプション	説明
	<p>名前付きのチーミング ポリシー：名前付きのチーミング ポリシーを使用すると、VLAN ベースの論理スイッチまたはセグメントごとに特定のチーミング ポリシー モードとアップリンク 名を定義できます。このポリシー タイプを使用すると、トラフィックのステアリング ポリシー に応じて、特定のアップリンクを選択できます。たとえば、帯域幅の要件に基づいて選択できます。</p> <ul style="list-style-type: none"> ■ 名前付きのチーミング ポリシーを定義した場合、N-VDS が VLAN ベースのトランスポート ゾーンに接続し、最終的にホストの特定の VLAN ベースの論理スイッチまたはセグメントに選択されるときに、N-VDS はその名前付きチーミング ポリシーを使用します。 ■ 名前付きのチーミング ポリシーを定義しない場合、N-VDS はデフォルトのチーミング ポリシーを使用します。

- 4 トランスポート VLAN の値を入力します。アップリンク プロファイルに設定されたトランスポート VLAN がオーバーレイ トラフィックにのみタグ付けし、VLAN ID が TEP エンドポイントによって使用されます。
- 5 MTU 値を入力します。

アップリンク プロファイル MTU のデフォルト値は 1600 です。

グローバル物理アップリンク MTU には、NSX-T Data Center ドメイン内のすべての N-VDS インスタンスの MTU 値を構成します。グローバル物理アップリンク MTU 値が指定されていない場合、アップリンク プロファイル MTU が設定されているか、デフォルトの 1600 が使用されていれば、この MTU 値が使用されます。アップリンク プロファイル MTU 値は、特定のホストのグローバル物理アップリンク MTU 値を上書きできます。

グローバル論理インターフェイス MTU には、すべての論理ルーター インターフェイスの MTU を構成します。グローバル論理インターフェイス MTU 値が指定されていない場合、MTU 値は、Tier-0 論理ルーターから取得されます。論理ルーターのアップリンク MTU 値は、特定のポートのグローバル論理インターフェイスの MTU 値を上書きできます。

結果

ユーザー インターフェイスの他に、API 呼び出し `GET /api/v1/host-switch-profiles` でアップリンク プロファイルを表示することもできます。

次のステップ

トランスポート ゾーンを作成します。[トランスポート ゾーンの作成](#) を参照してください。

Network I/O Control プロファイルの設定

Network I/O Control (NIOC) プロファイルを使用して、ビジネス上不可欠なアプリケーションにネットワーク バンド幅を割り当てたり、いくつかの種類のトラフィックが共通のリソースで競合する問題を解決したりします。

NIOC プロファイルは、ホスト上の物理アダプタのキャパシティに基づいて、システム トラフィックのバンド幅を予約するメカニズムを導入しています。Network I/O Control のバージョン 3 の機能では、ネットワーク リソース予約とスイッチ全体への割り当てが向上しています。

NSX-T Data Center 向け Network I/O Control バージョン 3 は、仮想マシンや、vSphere Fault Tolerance のインフラストラクチャ サービスに関連するシステム トラフィックのリソース管理をサポートします。システム トラフィックは、ESXi ホストに完全に関連付けられています。

注： NIOC プロファイルは、NSX Edge トランスポート ノードに適用できません。

システム トラフィックに対するバンド幅の確保

Network I/O Control バージョン 3 では、シェア、予約、および制限の構造を使用して、仮想マシンのネットワーク アダプタにバンド幅をプロビジョニングします。これらの構造は、NSX-T Data Center Manager ユーザー インターフェイスで定義できます。仮想マシン トラフィックのバンド幅予約は、アドミッション コントロールでも使用されます。仮想マシンをパワーオンすると、アドミッション コントロール ユーティリティは、十分なバンド幅が使用できることを確認してから、リソース キャパシティの提供が可能なホストに仮想マシンを配置します。

システム トラフィックのバンド幅割り当て

vSphere Fault Tolerance、vSphere vMotion、仮想マシンなどによって生成されるトラフィックに一定量のバンド幅を割り当てるように Network I/O Control を設定できます。

- 管理トラフィック：ホスト管理のトラフィックです。
- Fault Tolerance (FT) トラフィック：フェイルオーバーとリカバリのトラフィックです。
- NFS トラフィック：ネットワーク ファイル システムでのファイル転送に関連したトラフィックです。
- vSAN トラフィック：仮想ストレージ エリア ネットワークによって生成されるトラフィックです。
- vMotion トラフィック：コンピューティング リソースの移行トラフィックです。
- vSphere Replication トラフィック：レプリケーションのトラフィックです。
- vSphere Data Protection バックアップ トラフィック：データのバックアップによって生成されるトラフィックです。
- 仮想マシン トラフィック：仮想マシンによって生成されるトラフィックです。
- iSCSI トラフィック：iSCSI (Internet Small Computer System Interface) のトラフィック。

vCenter Server は、Distributed Switch の割り当てを、スイッチに接続されているホストの各物理アダプタに伝達します。

システム トラフィックのバンド幅割り当てパラメータ

Network I/O Control サービスでは、いくつかの構成パラメータを使用して、vSphere システムの基本機能からのトラフィックにバンド幅を割り当てます。システム トラフィックの割り当てパラメータ。

システム トラフィックの割り当てパラメータ

- シェア：シェアは、同じ物理アダプタ上で有効な他のシステム トラフィック タイプを基に、システム トラフィック タイプの相対的な優先度を 1 から 100 で示します。システム トラフィック タイプに割り当てられた相対的なシェアと、他のシステム機能で転送されたデータの量により、システム トラフィック タイプに使用できるバンド幅が決まります。

- 予約：単一の物理アダプタ上で確保する必要のある最小バンド幅 (Mbps)。すべてのシステム トラフィック タイプで予約される合計バンド幅は、最低キャパシティを備えた物理ネットワーク アダプタが提供できるバンド幅の 75% を超過することはできません。未使用の予約バンド幅は、システム トラフィックの他のタイプで利用できるようになります。ただし、Network I/O Control では、システム トラフィックが使用しないキャパシティを仮想マシンの配置に再配分しません。
- 制限：単一物理アダプタでシステム トラフィック タイプが使用できる最大バンド幅 (Mbps)。

注： 物理ネットワーク アダプタのバンド幅は最大 75% まで予約することができます。

たとえば、10 GbE ネットワーク アダプタが ESXi ホストに接続されている場合、各トラフィック タイプには 7.5 Gbps のバンド幅のみを割り当てることができます。未予約の容量が多く残ることがあります。ホストは、未予約のバンド幅をシェア、制限、使用量に応じて動的に割り当てることができます。ホストは、システム機能の処理に十分なバンド幅のみを予約します。

N-VDS のシステム トラフィックに対する Network I/O Control およびバンド幅割り当ての設定

NSX-T Data Center のホストで実行されるシステム トラフィックに最小バンド幅を確保するには、N-VDS でネットワーク リソース管理を有効にして設定します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [NIOC プロファイル] - [追加] を選択します。
- 3 NIOC プロファイルの詳細を入力します。

オプション	説明
名前と説明	NIOC プロファイル名を入力します。 必要に応じて、有効なトラフィック タイプなどのプロファイルの詳細を入力できます。
状態	トラフィック リソースで規定されたバンド幅割り当てを有効に切り替えます。
ホストのインフラストラクチャ トラフィック リソース	規定されたデフォルトのトラフィック リソースを受け入れることができます。 [追加] をクリックしてトラフィック リソースを入力し、NIOC プロファイルをカスタマイズします。 (オプション) 既存のトラフィック タイプを選択して、[削除] をクリックし、NIOC プロファイルからリソースを削除します。

新しい NIOC プロファイルは NIOC プロファイル リストに追加されます。

API を使用した Network I/O Control と N-VDS 上のシステム トラフィックの帯域幅割り当ての設定

NSX-T Data Center API を使用して、ネットワークと、ホスト上で実行しているアプリケーションの帯域幅を設定できます。

手順

- 1 ホストに対して、システム定義およびユーザー定義の両方のホスト スイッチ プロファイルを表示するよう問い合わせます。
- 2 GET https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true を参照してください。

サンプル応答には、ホストに適用されている NIOC プロファイルが示されています。

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
    "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
    "type-identifier": "NiocProfile"
  },
  "properties": {
    "_create_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of resource creation",
      "readonly": true
    },
    "_create_user": {
      "description": "ID of the user who created this resource",
      "readonly": true,
      "type": "string"
    },
    "_last_modified_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of last modification",
      "readonly": true
    },
    "_last_modified_user": {
      "description": "ID of the user who last modified this resource",
      "readonly": true,
      "type": "string"
    },
    "_links": {
      "description": "The server will populate this field when returning the resource. Ignored
on PUT and POST.",
      "items": {
        "$ref": "ResourceLink"+
      },
      "readonly": true,
      "title": "References related to this resource",
      "type": "array"
    }
  }
}
```

```

    },
    "_protection": {
      "description": "Protection status is one of the following:
        PROTECTED - the client who retrieved the entity is not allowed to modify it.
        NOT_PROTECTED - the client who retrieved the entity is allowed to modify it
        REQUIRE_OVERRIDE - the client who retrieved the entity is a super user and can modify
it,
        but only when providing the request header X-Allow-Overwrite=true.
        UNKNOWN - the _protection field could not be determined for this entity.",
      "readonly": true,
      "title": "Indicates protection status of this resource",
      "type": "string"
    },

    "_revision": {
      "description": "The _revision property describes the current revision of the resource.
        To prevent clients from overwriting each other's changes, PUT operations must include
the
        current _revision of the resource,
        which clients should obtain by issuing a GET operation.
        If the _revision provided in a PUT request is missing or stale, the
operation will be rejected.",
      "readonly": true,
      "title": "Generation of this resource config",
      "type": "int"
    },

    "_schema": {
      "readonly": true,
      "title": "Schema for this resource",
      "type": "string"
    },

    "_self": {
      "$ref": "SelfResourceLink+",
      "readonly": true,
      "title": "Link to this resource"
    },

    "_system_owned": {
      "description": "Indicates system owned resource",
      "readonly": true,
      "type": "boolean"
    },

    "description": {
      "can_sort": true,
      "maxLength": 1024,
      "title": "Description of this resource",
      "type": "string"
    },

    "display_name": {
      "can_sort": true,
      "description": "Defaults to ID if not set",

```

```

    "maxLength": 255,
    "title": "Identifier to use when displaying entity in logs or GUI",
    "type": "string"
  },

  "enabled": {
    "default": true,
    "description": "The enabled property specifies the status of NIOC feature.

    When enabled is set to true, NIOC feature is turned on and the bandwidth allocations
      specified for the traffic resources are enforced.
    When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is
    guaranteed.

    By default, enabled will be set to true.",
    "nsx_feature": "Nioc",
    "required": false,
    "title": "Enabled status of NIOC feature",
    "type": "boolean"
  },

  "host_infra_traffic_res": {
    "description": "host_infra_traffic_res specifies bandwidth allocation for various
    traffic resources.",
    "items": {
      "$ref": "ResourceAllocation"+
    },
    "nsx_feature": "Nioc",
    "required": false,
    "title": "Resource allocation associated with NiocProfile",
    "type": "array"
  },

  "id": {
    "can_sort": true,
    "readonly": true,
    "title": "Unique identifier of this resource",
    "type": "string"
  },

  "required_capabilities": {
    "help_summary":
      "List of capabilities required on the fabric node if this
    profile is used.
      The required capabilities is determined by whether specific features are enabled
    in the profile.",
    "items": {
      "type": "string"
    },
    "readonly": true,
    "required": false,
    "type": "array"
  },

```

```

"resource_type": {
"$ref": "HostSwitchProfileType",
"required": true
},

"tags": {
"items": {
"$ref": "Tag"
},

"maxItems": 30,
"title": "Opaque identifiers meaningful to the API user",
"type": "array"
},
},
"title": "Profile for NIOC",
"type": "object"
}

```

3 NIOC プロファイルがない場合は、作成します。

POST <https://<nsx-mgr>/api/v1/host-switch-profiles>

```

{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
  Values for limit and reservation are expressed in percentage. And for shares,
  the value is expressed as a number between 1-100.\n\nThe overall reservation among all
  traffic types should not exceed 75%.
  Otherwise, the API request will be rejected.",
  "id": "ResourceAllocation",
  "module_id": "NIOCProfile",
  "nsx_feature": "NIOC",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a
given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\nand will be
      rejected by the API.",
      "maximum": 100,
      "minimum": -1,
      "required": true,
      "title": "Maximum bandwidth percentage",
      "type": "number"
    },
    "reservation": {
      "default": 0.0,
      "maximum": 75,
      "minimum": 0,
      "required": true,
      "title": "Minimum guaranteed bandwidth percentage",

```

```

    "type": "number"
  },

  "shares": {
    "default": 50,
    "maximum": 100,
    "minimum": 1,
    "required": true,
    "title": "Shares",
    "type": "int"
  },

  "traffic_type": {
    "$ref": "HostInfraTrafficType+",
    "required": true,
    "title": "Resource allocation traffic type"
  }
},

"title": "Resource allocation information for a host infrastructure traffic type",
"type": "object"

```

- 4 新規に作成された NIOC プロファイルの NIOC プロファイル ID を使用して、トランスポート ノードの設定を更新します。

PUT <https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>>

```

{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  "display_name": "NSX Configured TN",
  "host_switch_spec": {
    "resource_type": "StandardHostSwitchSpec",
    "host_switches": [
      {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
          {
            "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
            "key": "LldpHostSwitchProfile"
          }
        ]
      },
      {
        "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
        "key": "NiocProfile"
      }
    ],
    "host_switch_name": "nsxvswitch",
    "pnics": [
      {
        "device_name": "vmnic1",

```

```

    "uplink_name": "uplink1"
  }
],
"ip_assignment_spec": {
  "resource_type": "StaticIpPoolSpec",
  "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
}
},
"transport_zone_endpoints": [
  {
    "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ]
  }
],
"host_switches": [
  {
    "host_switch_profile_ids": [
      {
        "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
        "key": "UplinkHostSwitchProfile"
      },
      {
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
      }
    ]
  }
],
"host_switch_name": "nsxvswitch",
"pnics": [
  {
    "device_name": "vmnic1",
    "uplink_name": "uplink1"
  }
],
"static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
},
"node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
"_revision": 0
}

```

- 5 `com.vmware.common.respools.cfg` ファイル内の NIOC プロファイル パラメータが更新されていることを確認します。

```
# [root@ host:] net-dvs -l
```

```
switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,      propType = CONFIG
com.vmware.nsx.kcp.enable = true ,        propType = CONFIG
com.vmware.common.alias = nsxvswitch ,    propType = CONFIG
com.vmware.common.uplinkPorts: uplink1    propType = CONFIG
com.vmware.common.portset.mtu = 1600, propType = CONFIG
com.vmware.etherswitch.cdp = LLDP, listen propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:
netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255
netsched.pools.persist.nfs:0:50:-1:255
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG
```

- 6 ホスト カーネルの NIOC プロファイルを確認します。

```
# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/niocVnicInfo
```

```
Vnic NIOC Info
{
  Uplink reserved on:vmnic4
  Reservation in Mbps:200
  Shares:50
  Limit in Mbps:4294967295
  World ID:1001400726
  vNIC Index:0
  Respool Tag:0
  NIOC Version:3
  Active Uplink Bit Map:15
  Parent Respool ID:netsched.pools.persist.vm
}
```

- 7 NIOC プロファイル情報を確認します。

```
# [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo
```

```
Uplink NIOC Info
{
  Uplink device:vmnic4
}
```

```

Link Capacity in Mbps:750
vm respool reservation:275
link status:1
NetSched Ready:1
Infrastructure reservation:0
Total VM reservation:200
Total vnics on this uplink:1
NIOC Version:3
Uplink index in BitMap:0
}

```

結果

NIOC プロファイルは、NSX-T Data Center ホスト上で実行しているアプリケーションに事前定義された帯域幅割り当てを使用して設定されています。

NSX Edge クラスタ プロファイルの追加

NSX Edge クラスタ プロファイルは、NSX Edge トランスポート ノードのポリシーを定義します。

前提条件

NSX Edge クラスタが使用可能であることを確認します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [Edge クラスタ プロファイル] - [追加] を選択します。
- 3 NSX Edge クラスタ プロファイルの詳細を入力します。

オプション	説明
名前と説明	NSX Edge クラスタ プロファイルの名前を入力します。 必要に応じて、双方向フォワーディング検出 (BFD) 設定などのプロファイルの詳細を入力できます。
BFD プローブ間隔	デフォルト設定を受け入れます。 BFD は、転送パスの障害を識別するために使用される検出プロトコルです。BFD が転送パスの障害を検出する間隔を設定できます。
BFD 最大ホップ数	デフォルト設定を受け入れます。 プロファイルで許可されるマルチホップ BFD セッションの数を設定できます。
BFD デッド検知係数	デフォルト設定を受け入れます。 BFD パケットが受信されなかった回数の基準値を設定して、その値に達した場合、セッションに停止のフラグが設定されるようにすることができます。
スタンバイ再配置のしきい値	デフォルト設定を受け入れます。

NSX Edge ブリッジ プロファイルの追加

NSX Edge ブリッジ プロファイルは、ESXi ブリッジ クラスタのポリシーを定義します。

ブリッジ クラスタは、ESXi ホスト トランスポート ノードの集まりです。

前提条件

- NSX Edge クラスタが使用可能であることを確認します。
- ESXi ブリッジ クラスタが使用可能であることを確認します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [Edge ブリッジ プロファイル] - [追加] を選択します。
- 3 NSX Edge クラスタ プロファイルの詳細を入力します。

オプション	説明
名前と説明	NSX Edge ブリッジ クラスタ プロファイルの名前を入力します。 必要に応じて、プライマリ ノードとバックアップ ノードの詳細など、プロファイルの詳細を入力できます。
Edge クラスタ	使用できる NSX Edge クラスタを選択します。
プライマリ ノード	クラスタ内の優先 NSX Edge ノードを指定します。
バックアップ ノード	プライマリ ノードが失敗した場合は、バックアップ NSX Edge ノードを指定します。
フェイルオーバー モード	[プリエンプティブ] モードまたは [非プリエンプティブ] モードを選択します。 デフォルトの HA モードはプリエンプティブであるため、優先 NSX Edge ノードがオンラインに戻ったときに、トラフィック速度が低下することがあります。非プリエンプティブ モードの場合は、トラフィック速度が低下しません。

トランスポート ノード プロファイルの追加

トランスポート ノード プロファイルには、トランスポート ノードを作成するために必要な設定が取り込まれています。トランスポート ノード プロファイルを既存の vCenter Server クラスタに適用して、メンバー ホスト用のトランスポート ノードを作成できます。トランスポート ノード プロファイルは、トランスポート ゾーン、メンバー ホスト、N-VDS スイッチの設定（アップリンク プロファイル、IP アドレスの割り当て、物理 NIC とアップリンク仮想インターフェイスのマッピングなど）を定義します。

注： トランスポート ノード プロファイルは、NSX Edge トランスポート ノードに適用する必要はありません。

トランスポート ノード プロファイルが vCenter Server クラスタに適用されると、トランスポート ノードの作成が開始します。NSX Manager はクラスタ内のホストを準備し、すべてのホストに NSX-T Data Center コンポーネントをインストールします。トランスポート ノード プロファイルで指定された設定に基づいて、ホストのトランスポート ノードが作成されます。

トランスポート ノード プロファイルを削除するには、まず関連付けられているクラスタからプロファイルを接続解除する必要があります。既存のトランスポート ノードは影響を受けません。クラスタに追加された新しいホストは、トランスポート ノードに自動的に変換されなくなります。

トランスポート ノード プロファイルの作成に関する考慮事項：

- 構成ごとに最大 4 台の N-VDS スイッチを追加できます（VLAN トランスポート ゾーン用に作成された拡張 N-VDS、オーバーレイ トランスポート ゾーン用に作成された標準 N-VDS、オーバーレイ トランスポート ゾーン用に作成された拡張 N-VDS）。

- VLAN トランスポート ゾーン用に作成された標準の N-VDS スイッチの数に制限はありません。
- 複数の標準オーバーレイ N-VDS スイッチと Edge 仮想マシンが同じホストで実行されている単一ホスト クラスタ トポロジの場合、NSX-T Data Center はトラフィックを分離して、1 番目の N-VDS を経由するトラフィックが 2 番目以降の N-VDS を経由するトラフィックから分離されるようにします。North-South トラフィックと外部ネットワークとの接続を許可するには、各 N-VDS 上の物理 NIC をホスト上の Edge 仮想マシンにマッピングする必要があります。1 番目のトランスポート ゾーンの仮想マシンから送信されるパケットは、外部ルーターまたは外部仮想マシンを経由して、2 番目のトランスポート ゾーン上の仮想マシンにルーティングする必要があります。
- 各 N-VDS スイッチの名前は一意である必要があります。NSX-T Data Center では、重複するスイッチ名を使用できません。
- 各トランスポート ゾーン ID は一意である必要があります。NSX-T Data Center では、重複する ID を使用できません。
- トランスポート ノード プロファイルには、最大 1,000 個のトランスポート ゾーンを追加できます。
- トランスポート ゾーンを追加するには、トランスポート ノード プロファイル内にあるいずれかの N-VDS でこのトランスポート ゾーンが認識されている必要があります。

前提条件

- ホストが vCenter Server クラスタに含まれていることを確認します。
- vCenter Server には、1 つ以上のクラスタが必要です。
- トランスポート ゾーンが設定されていることを確認します。 [トランスポート ゾーンの作成](#) を参照してください。
- クラスタが使用可能であることを確認します。 [クラスタを構成する NSX Manager ノードをユーザー インターフェイスから展開](#) を参照してください。
- IP アドレス プールが設定されていることを確認します。IP アドレス プールが設定されていない場合は、ネットワーク環境で DHCP が使用可能になっている必要があります。 [トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成](#) を参照してください。
- コンピュート マネージャが設定されていることを確認します。 [コンピュート マネージャの追加](#) を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [トランスポート ノード プロファイル] - [追加] を選択します。
- 3 トランスポート ノード プロファイルを識別する名前を入力します。
必要に応じて、トランスポート ノード プロファイルについての説明を追加できます。
- 4 使用可能なトランスポート ゾーンを選択し、[>] ボタンをクリックして、トランスポート ノード プロファイルにトランスポート ゾーンを含めます。

注： 複数のトランスポート ゾーンを追加できます。

5 [N-VDS] タブをクリックして、スイッチの詳細を入力します。

オプション	説明
N-VDS 名	<p>トランスポート ノードがトランスポート ゾーンに接続されている場合は、N-VDS 用に入力した名前がトランスポート ゾーンで指定された N-VDS の名前と同じであることを確認します。トランスポート ゾーンをトランスポート ゾーンに接続しなくても、トランスポート ノードを作成できます。</p>
関連付けられたトランスポート ゾーン	<p>関連付けられているホスト スイッチで認識されているトランスポート ゾーンが表示されます。トランスポート ノード プロファイル内にある N-VDS で認識されていないトランスポート ゾーンは、追加できません。</p>
NIOC プロファイル	<p>ドロップダウン メニューから NIOC プロファイルを選択します。</p> <p>トラフィック リソース用にプロファイル内で指定した帯域幅の割り当てが適用されます。</p>
アップリンク プロファイル	<p>ドロップダウン メニューから既存のアップリンク プロファイルを選択するか、アップリンクのカスタム プロファイルを作成します。</p> <p>デフォルトのアップリンク プロファイルも使用できます。</p>
LLDP プロファイル	<p>デフォルトでは、NSX-T は LLDP ネイバーから LLDP パケットの受信のみを行います。</p> <p>ただし、LLDP パケットを LLDP ネイバーに送信し、LLDP ネイバーから LLDP パケットを受信するように NSX-T を設定できます。</p>
IP の割り当て	<p>[DHCP を使用]、[IP アドレス プールを使用]、または [固定 IP アドレスのリストを使用] を選択して、IP アドレスをトランスポート ノードの仮想トンネル エンドポイント (VTEP) に割り当てます。</p> <p>[固定 IP アドレスのリストを使用] を選択した場合は、IP アドレス、ゲートウェイ、およびサブネット マスクのコンマ区切りのリストを指定する必要があります。トランスポート ノードのすべての VTEP が同じサブネット内に配置されている必要があります。そうでない場合は、双方向フロー (BFD) セッションが確立されません。</p>
IP アドレス プール	<p>IP アドレスの割り当てに [IP アドレス プールを使用] を選択した場合は、IP アドレス プール名を指定します。</p>
物理 NIC	<p>トランスポート ノードに物理 NIC を追加します。デフォルトのアップリンクを使用すること、ドロップ ダウン メニューから既存のアップリンクを割り当てることもできます。</p> <p>[物理 NIC の追加] をクリックして、トランスポート ノードに追加の物理 NIC を設定します。</p> <p>注： このフィールドで追加した物理 NIC の移行は、[物理 NIC のみの移行]、[インストール用のネットワーク マッピング]、および [アンインストール用のネットワーク マッピング] の設定方法によって決まります。</p> <ul style="list-style-type: none"> ■ 標準 vSwitch または vSphere Distributed Switch を使用するなどの手段によって使用済みの物理 NIC を移行し、関連付けられた VMkernel マッピングを移行しないようにするには、[物理 NIC のみの移行] が有効になっていることを確認します。すでに使用されている場合、トランスポート ノードは [部分的成功] 状態になり、ファブリック ノードの LCP 接続の確立に失敗します。 ■ 使用済みの物理 NIC を、関連付けられた VMkernel ネットワーク マッピングとともに移行するには、[物理 NIC のみの移行] を無効にして、VMkernel ネットワーク マッピングを設定します。 ■ 空いている物理 NIC を移行するには、[物理 NIC のみの移行] を有効にします。

オプション	説明
物理 NIC のみの移行	<p>このフィールドを設定する前に、次の点を考慮してください。</p> <ul style="list-style-type: none"> ■ 定義されている物理 NIC が使用済み NIC であるか、使用されていない NIC であるかを確認します。 ■ ホストの VMkernel インターフェイスを物理 NIC とともに移行する必要があるかどうかを判断します。 <p>フィールドを次のように設定します。</p> <ul style="list-style-type: none"> ■ VSS スイッチまたは VDS スイッチから N-VDS スイッチに物理 NIC のみを移行する場合は、[物理 NIC のみの移行] を有効にします。 ■ 使用済みの物理 NIC と関連付けられた VMkernel インターフェイス マッピングを移行する場合は、[物理 NIC のみの移行] を無効にします。VMkernel インターフェイスの移行マッピングが指定されている場合は、使用されていない、または使用可能な物理 NIC が N-VDS スイッチに接続されます。 <p>複数のホスト スイッチを使用しているホストで、次の操作を実行します。</p> <ul style="list-style-type: none"> ■ すべてのホスト スイッチで物理 NIC のみを移行する場合は、物理 NIC を 1 回の操作で移行できます。 ■ VMkernel インターフェイスを移行するホスト スイッチと、物理 NIC のみを移行するホスト スイッチが混在している場合は、次の操作を実行します。 <ol style="list-style-type: none"> 1 最初の操作で、物理 NIC のみを移行します。 2 次の操作で、VMkernel インターフェイスを移行します。[物理 NIC のみの移行] が無効になっていることを確認します。 <p>物理 NIC のみの移行と VMkernel インターフェイスの移行は、複数のホストで同時にサポートされません。</p> <p>注： 管理ネットワークの NIC を移行するには、関連付けられた VMkernel ネットワークのマッピングを設定し、[物理 NIC のみの移行] を無効のままにします。管理 NIC のみを移行する場合、ホストの接続は切断されます。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>

オプション	説明
インストール用のネットワーク マッピング	<p>インストール中に VMkernel を N-VDS スイッチに移行するには、VMkernel を既存の論理スイッチにマッピングします。NSX Manager により、VMkernel が N-VDS 上のマッピングされた論理スイッチに移行されます。</p> <p>注意： 管理 NIC が接続されていた VLAN と同じ VLAN に論理スイッチが接続されていて、そこに管理 NIC および管理 VMkernel インターフェイスが移行されることを確認します。vmnic<n> および VMkernel<n> が異なる VLAN に移行された場合は、ホストとの接続が切断されます。</p> <p>注意： 固定された物理 NIC の場合は、物理 NIC から VMkernel インターフェイスへのホスト スイッチのマッピングが、トランスポート ノード プロファイルで指定されている設定と一致することを確認します。検証手順の一環として、NSX-T Data Center はマッピングを検証します。検証が成功すると、VMkernel インターフェイスが正常に N-VDS スイッチに移行したことになります。VMkernel インターフェイスを N-VDS スイッチに移行すると、NSX-T Data Center にホスト スイッチのマッピング設定が保存されなくなるため、アンインストール用のネットワーク マッピングも設定する必要があります。このマッピングが設定されていない場合は、VSS スイッチまたは VDS スイッチに移行し直した後に、vSAN などのサービスとの接続が切断されることがあります。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>
アンインストール用のネットワーク マッピング	<p>アンインストール中に VMkernel の移行を元に戻すには、VSS または VDS のポート グループに VMkernel をマッピングして、VMkernel を移行し直す VSS または VDS 上のポート グループを NSX Manager が認識できるようにします。VDS スイッチの場合は、ポート グループのタイプが短期であることを確認します。</p> <p>注意： 固定された物理 NIC の場合は、物理 NIC から VMkernel インターフェイスへのトランスポート ノード プロファイルのマッピングが、ホスト スイッチで指定されている設定と一致することを確認します。VMkernel インターフェイスを N-VDS スイッチに移行すると、NSX-T Data Center にホスト スイッチのマッピング設定が保存されなくなるため、アンインストール用のネットワーク マッピングを設定する必要があります。このマッピングが設定されていない場合は、VSS スイッチまたは VDS スイッチに移行し直した後に、vSAN などのサービスとの接続が切断されることがあります。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>

- 複数のトランスポート ゾーンを選択した場合は、[+ N-VDS の追加] を再度クリックして、他のトランスポート ゾーンのスイッチを設定します。

- [終了] をクリックして、設定を完了します。

次のステップ

既存の vSphere クラスタにトランスポート ノード プロファイルを適用します。[管理対象ホストのトランスポート ノードの構成](#) を参照してください。

VMkernel の N-VDS スイッチへの移行

VMkernel インターフェイスを VSS または Distributed Switch から N-VDS スイッチにクラスタ レベルで移行するには、移行（VMkernel インターフェイスの論理スイッチへのマッピング）に必要なネットワーク マッピングの詳細を含むトランスポート ノード プロファイルを設定します。同様に、ホスト ノード上の VMkernel インターフェイスを移行するには、トランスポート ノードの設定を実行します。VMkernel インターフェイスを VSS または Distributed Switch に移行して戻すには、トランスポート ノード プロファイルでアンインストール ネットワ

ーク マッピング（論理ポートの VMkernel インターフェイスへのマッピング）を、アンインストール中に認識されるように設定します。

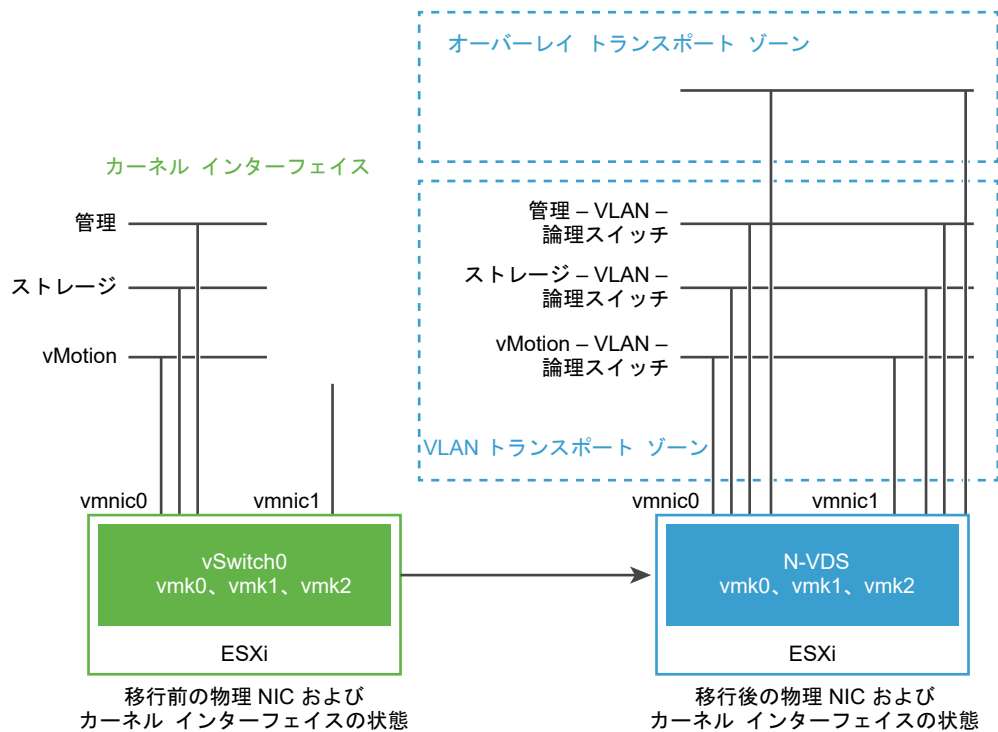
移行時に、現在使用中の物理 NIC は N-VDS スイッチに移行され、使用されていない物理 NIC は移行後に N-VDS に接続されます。

注： トランスポート ノード プロファイルは、クラスタ内のすべてのメンバー ホストに適用されます。特定のホストで VMkernel インターフェイスの移行を制限する場合は、ホストを直接構成できます。移行後、N-VDS は、N-VDS スイッチに接続されたこれらのインターフェイスの VLAN およびオーバーレイ ネットワーク上のトラフィックを処理します。

重要： ホストに個別に行った設定は Overridden フラグでマークされます。トランスポート ノード プロファイルへの更新はこれらのオーバーライドされたホストには適用されません。これらのホストは、NSX-T Data Center がアンインストールされるまで、オーバーライドされた状態になります。

以下の図では、ホストにある物理 NIC が 2 つのみの場合には、これらの NIC を冗長性を確保するために N-VDS に割り当て、さらに関連付けられた VMkernel インターフェイスに割り当てることで、インターフェイスがホストとの接続を失わないようにすることが推奨されます。

図 10-2. N-VDS へのネットワーク インターフェイスの移行前と移行後



移行前は、ESXi ホストに 2 つの物理ポート（vmnic0 と vmnic1）から派生した 2 つのアップリンクがあります。このとき、vmnic0 はアクティブな状態に設定され、VSS に接続されますが、vmnic1 は使用されません。さらに、vmk0、vmk1、vmk2 という 3 つの VMkernel インターフェイスがあります。

NSX-T Data Center Manager ユーザー インターフェイスまたは NSX-T Data Center API を使用して、VMkernel インターフェイスを移行できます。NSX-T Data Center API ガイド を参照してください。

移行後には、vmnic0、vmnic1、およびそれらの VMkernel インターフェイスが N-VDS スイッチに移行されます。vmnic0 と vmnic1 の両方が、VLAN およびオーバーレイ トランスポート ゾーンを介して接続されます。

VMkernel の移行の考慮事項

- 物理 NIC と VMkernel の移行：固定物理 NIC および関連付けられた VMkernel インターフェイスを N-VDS スイッチに移行する前に、ホスト スイッチ上のネットワーク マッピング（物理 NIC からポート グループへのマッピング）を書き留めます。
- 物理 NIC のみの移行：物理 NIC のみを移行する場合は、管理用 VMkernel インターフェイスに接続された管理用の物理 NIC が移行されないようにします。ホストとの接続が失われることになります。詳細については、[トランスポート ノード プロファイルの追加](#)の [物理 NIC のみの移行] フィールドを参照してください。
- 移行を戻す：固定物理 NIC で、VMkernel インターフェイスから VSS または Distributed Switch ホスト スイッチに戻す前に、ホスト スイッチ上のネットワーク マッピング（物理 NIC からポート グループへのマッピング）を書き留めます。[アンインストールのネットワーク マッピング] フィールドで、トランスポート ノード プロファイルをホスト スイッチ マッピングとともに構成する必要があります。このマッピングがない場合、NSX-T Data Center は、VMkernel インターフェイスが戻る移行先のポート グループを判断できなくなります。この状況では、vSAN ネットワークへの接続が失われる可能性があります。
- 移行前の vCenter Server の登録：Distributed Switch に接続された VMkernel または物理 NIC を移行する場合は、NSX Manager に vCenter Server が登録されていることを確認します。
- VLAN ID の一致：移行後、管理用 NIC および管理用 VMkernel インターフェイスは、移行前に管理用 NIC が接続されていた同一の VLAN 上にある必要があります。vmnic0 と vmk0 が管理ネットワークに接続されている際に、異なる VLAN に移行された場合は、ホストへの接続が失われます。
- VSS スイッチへの移行：VSS スイッチの同じポート グループには、2 つの VMkernel インターフェイスを移行して戻すことはできません。
- vMotion：VMkernel または 物理 NIC の移行の前に、vMotion を実行して仮想マシンのワークロードを別のホストに移行します。移行が失敗した場合、ワークロード仮想マシンは影響を受けません。
- vSAN：vSAN トラフィックがホスト上で実行されている場合は、vCenter Server からホストをメンテナンスモードに切り換え、vMotion 機能で仮想マシンをホストから移行してから、VMkernel または物理 NIC を移行します。
- 移行：VMkernel がすでにターゲット スイッチに接続されている場合は、同じスイッチへの移行を選択できます。このプロパティを使用すると、VMK または物理 NIC の移行操作をべき等にできます。これは、ターゲット スイッチに物理 NIC のみを移行する場合に役立ちます。移行では、常に少なくとも 1 つの VMkernel と物理 NIC が必要です。ターゲット スイッチに物理 NIC のみを移行する場合は、ターゲット スイッチにすでに移行されている VMkernel を選択します。VMkernel を移行する必要がない場合は、vCenter Server でソース スイッチまたはターゲット スイッチのいずれかに一時 VMkernel を作成します。次に、それを物理 NIC と一緒に移行し、移行の終了後に vCenter Server から一時 VMkernel を削除します。
- MAC 共有：VMkernel インターフェイスと物理 NIC が同じ MAC を共有し、これらが同じスイッチにあり、移行後にこの両方を使用する場合は、これらを同じターゲット スイッチに移行する必要があります。同じスイッチで vmk0 と vmnic0 を維持します。

次のコマンドを実行して、ホストのすべての VMK と物理 NIC で使用されている MAC を確認します。


```
esxcfg-vmknic -l
```

```
esxcfg-nics -l
```

- 移行後に作成された VIF 論理ポート：VSS または DVS スイッチから VMkernel を N-VDS スイッチに移行した後、VIF タイプの論理スイッチポートが NSX Manager に作成されます。これらの VIF 論理スイッチポートに分散ファイアウォール ルールを作成しないでください。

VMkernel インターフェイスの N-VDS スイッチへの移行

VMkernel インターフェイスを N-VDS スイッチに移行する際のワークフローの概要は次のとおりです。

- 1 必要に応じて、論理スイッチを作成します。
- 2 VMkernel インターフェイスと物理 NIC を N-VDS スイッチに移行したホスト上の仮想マシンをパワーオフにします。
- 3 トランスポート ノードの作成時に VMkernel インターフェイスの移行に使用するネットワークのマッピングを使用して、トランスポート ノード プロファイルを構成します。ネットワーク マッピングとは、VMkernel インターフェイスから論理スイッチへのマッピングを指します。

詳細については、[トランスポート ノード プロファイルの追加](#)を参照してください。

- 4 vCenter Server のネットワーク アダプタのマッピングが VMkernel スイッチと N-VDS スイッチの新しい関連付けを反映していることを確認します。固定物理 NIC の場合は、NSX-T Data Center のマッピングが vCenter Server の物理 NIC に固定されたすべての VMkernel を反映していることを確認します。
- 5 NSX Manager で、[ネットワークとセキュリティの詳細設定] > [ネットワーク] > [スイッチング] の順に移動します。[スイッチ] 画面で、VMkernel インターフェイスが、新規作成された論理ポートを介して論理スイッチに接続されていることを確認します。
- 6 [システム] > [ノード] > [ホスト トランスポート ノード] の順に移動します。各トランスポート ノードで、[ノードの状態] 列に「成功」と表示されていることを確認し、トランスポート ノードの設定が正常に検証されていることを確認します。
- 7 [ホスト トランスポート ノード] 画面で、[設定の状態] の状態が「成功」になっていることを確認し、ホストが指定した設定で正常に認識されていることを確認します。

NSX-T UI またはトランスポート ノード API を使用して VDS から VMkernel インターフェイスと物理 NIC を移行すると、vCenter Server に VDS の警告が表示されます。ホストを VDS に接続する必要がある場合は、そのホストを VDS から削除します。vCenter Server に VDS の警告が表示されなくなります。

移行中に発生する可能性のあるエラーについては、[VMkernel の移行エラー](#)を参照してください。

VSS または Distributed Switch に VMkernel インターフェイスの移行を戻す

NSX-T Data Center のアンインストール時に VMkernel インターフェイスの移行を N-VDS スイッチから VSS または Distributed Switch に戻す際のワークフローの概要は次のとおりです。

- 1 ESXi ホストで、移行後に VMkernel インターフェイスをホストする論理ポートに接続された仮想マシンをパワーオフします。

- 2 アンインストール プロセスで VMkernel インターフェイスの移行に使用するネットワークのマッピングを使用して、トランスポート ノード プロファイルを構成します。アンインストール時のネットワーク マッピングで、VMkernel インターフェイスを ESXi ホスト上の VSS または Distributed Switch のポート グループにマッピングします。

注： Distributed Switch 上のポート グループに VMkernel の移行を戻すと、ポート グループのタイプが Ephemeral に設定されていることを確認します。

詳細については、[トランスポート ノード プロファイルの追加](#)を参照してください。

- 3 vCenter Server のネットワーク アダプタのマッピングが VMkernel スイッチと VSS または Distributed Switch との新しい関連付けを反映していることを確認します。
- 4 NSX Manager で、[ネットワークとセキュリティの詳細設定] > [ネットワーク] > [スイッチング] の順に移動します。[スイッチ] 画面で、VMkernel インターフェイスを含む論理スイッチが削除されていることを確認します。

移行中に発生する可能性のあるエラーについては、[VMkernel の移行エラー](#)を参照してください。

ホスト スイッチ マッピングの更新

重要：

- ステートフル ホスト：追加および更新操作がサポートされます。既存のマッピングを更新するには、ネットワーク マッピング設定に新しい VMkernel インターフェイスのエントリを追加できます。すでに N-VDS スイッチに移行された VMkernel インターフェイスのネットワーク マッピング設定を更新しても、更新されたネットワーク マッピングはホストで認識されません。
- ステートレス ホスト：追加、更新、削除操作がサポートされます。ネットワーク マッピング設定に加えた変更は、ホストの再起動後に認識されます。

VMkernel インターフェイスを新しい論理スイッチに更新するために、トランスポート ノード プロファイルを編集し、クラスタ レベルでネットワーク マッピングを適用できます。更新を単一のホストにのみ適用する場合は、ホスト レベルの API を使用してトランスポート ノードを設定します。

注： ホストで個別にトランスポート ノード設定を更新すると、トランスポート ノード プロファイルを使用して適用された新しい更新はホストに適用されません。このホストの状態は overridden に変更されます。

- 1 クラスタ内のすべてのホストを更新するには、[インストール時のネットワーク マッピング] フィールドを編集して論理スイッチへの VMkernel マッピングを更新します。

詳細については、[トランスポート ノード プロファイルの追加](#)を参照してください。

- 2 変更を保存します。トランスポート ノード プロファイルに加えられた変更は、クラスタのすべてのメンバー ホストに自動的に適用されます。ただし、overridden 状態とマークされているホスト上のメンバーは除外されます。

3 同様に、ホストを個別に更新するには、トランスポート ノード設定で、VMkernel マッピングを編集します。

注： 新しい VMkernel マッピングで [インストール時のネットワーク マッピング] フィールドを更新する場合は、[アンインストール時のネットワーク マッピング] フィールドに同一の VMkernel インターフェイスを追加する必要があります。

移行中に発生する可能性のあるエラーについては、[VMkernel の移行エラー](#)を参照してください。

ステートレス クラスタでの VMkernel インターフェイスの移行

- 1 トランスポート ノード API を使用して、ホストをリファレンス ホストとして準備および構成します。
- 2 リファレンス ホストからホスト プロファイルを抽出します。
- 3 vCenter Server で、ステートレス クラスタにホスト プロファイルを適用します。
- 4 NSX-T Data Center で、ステートレス クラスタにトランスポート ノード プロファイルを適用します。
- 5 クラスタの各ホストを再起動します。

クラスタのホストが更新の状態を認識するのに数分間かかることがあります。

移行の失敗のシナリオ

- 移行が何らかの理由で失敗した場合、ホストは物理 NIC と VMkernel インターフェイスの移行を 3 回試行します。
- 移行の失敗が解消しない場合、ホストは、管理用の物理 NIC である vmnic0 への VMkernel 接続を維持することで以前の構成へのロールバックを実行します。
- ロールバックも失敗して、管理用の物理 NIC に構成された VMkernel が切断された場合は、ホストをリセットする必要があります。

サポート対象外の移行シナリオ

次のシナリオはサポートされません。

- 異なる VSS または Distributed Switch からの 2 つの VMkernel インターフェイスを同時に移行する。
- ステートフル ホストで、ネットワーク マッピングを更新して VMkernel インターフェイスを別の論理スイッチにマッピングする。たとえば、移行前に、VMkernel を論理スイッチ 1 にマッピングし、VMkernel インターフェイスを論理スイッチ 2 にマッピングする。

VMkernel の移行エラー

VMkernel インターフェイスと物理 NIC を VSS または VDS スイッチから N-VDS スイッチに移行する際、またはインターフェイスを VSS または VDS ホスト スイッチに逆に移行する際にエラーが発生することがあります。

表 10-1. VMkernel の移行エラー

エラー コード	問題	原因	解決方法
8224	トランスポート ノードの設定で指定されたホスト スイッチが見つからない。	ホスト スイッチ ID が見つかりません。	<ul style="list-style-type: none"> ■ トランスポート ゾーンがホスト スイッチ名を使用して作成されていることを確認し、トランスポート ノードを作成します。 ■ トランスポート ノードの設定で有効なホスト スイッチが使用されていることを確認します。
8225	VMkernel の移行が進行中である。	移行が進行中です。	別のアクションを実行する前に移行が完了するのを待ちます。
8226	VMkernel の移行が ESXi ホスト以外でサポートされない。	移行は ESXi ホストのみで有効です。	移行の開始前にホストが ESXi ホストであることを確認します。
8227	VMkernel インターフェイスにホスト スイッチ名が付加されない。	複数のホスト スイッチがあるホストでは、NSX-T Data Center は各 VMkernel インターフェイスとホスト スイッチの関連付けを識別できません。	<p>ホストに複数の N-VDS ホスト スイッチがある場合、VMkernel インターフェイスに、N-VDS にホストが接続する N-VDS のホスト スイッチ名を付加するようにします。</p> <p>たとえば、nsxvswitch1 という名前の N-VDS ホスト スイッチおよび VMkernel1 と、nsxvswitch2 という名前の別の N-VDS ホスト スイッチおよび VMkernel2 を持つホストのアンインストールのネットワーク マッピングは、次のように定義されます：</p> <pre>device_name: VMkernel1@nsxvswitch1、 destination_network: DPortGroup。</pre>
8228	device_name フィールドで使用されているホスト スイッチがホスト上に見つからない。	ホスト スイッチ名が無効です。	適切なホスト スイッチ名を入力します。
8229	トランスポート ノードで論理スイッチのトランスポート ゾーンが指定されていない。	トランスポート ゾーンが追加されていません。	トランスポート ノードの設定にトランスポート ゾーンを追加します。
8230	ホスト スイッチに物理 NIC がない。	ホスト スイッチには 1 つ以上の物理 NIC が必要です。	アップリンク プロファイルに 1 つ以上の物理 NIC を指定し、論理スイッチに VMkernel ネットワーク マッピングの設定を指定します。
8231	ホスト スイッチ名が一致しない。	vmk1@host_switch で使用されているホスト スイッチ名が、インターフェイスのターゲット論理スイッチが使用するホスト スイッチ名と一致しません。	ネットワーク マッピングの設定で指定されたホスト スイッチ名が、インターフェイスの論理スイッチが使用する名前と一致するようにします。
8232	論理スイッチがホストで認識されない。	ホスト上の論理スイッチの認識に失敗します。	ホストを NSX Manager と同期します。

表 10-1. VMkernel の移行エラー（続き）

エラー コード	問題	原因	解決方法
8233	ネットワーク インターフェイス マッピングで予期しない論理スイッチのエラーが発生する。	インストールおよびアンインストールのネットワーク インターフェイス マッピングで、論理スイッチとポート グループの両方がリストされます。	インストールのネットワーク マッピングには、ターゲットとして論理スイッチのみを含める必要があります。同様に、アンインストールのネットワーク マッピングには、ターゲットとしてポート グループのみを含める必要があります。
8294	ネットワーク インターフェイスのマッピングに論理スイッチがない。	論理スイッチが指定されていません。	論理スイッチがネットワーク インターフェイス マッピングの設定で指定されていることを確認します。
8296	ホスト スイッチが一致しない。	アンインストールのネットワーク インターフェイス マッピングが無効なホスト スイッチ名で設定されています。	マッピングの設定で使用されているホスト スイッチ名が、VMkernel インターフェイスが配置されているホスト スイッチで入力した名前と一致していることを確認します。
8297	VMkernel が重複している。	重複する VMkernels が移行に指定されています。	インストールまたはアンインストール マッピングの設定で VMkernel インターフェイスが重複して指定されていないことを確認します。
8298	VMkernel インターフェイスとターゲットの数不一致。	構成が無効です。	各 VMkernel インターフェイスに、対応するターゲットが設定で指定されていることを確認します。
8299	VMkernel インターフェイスが N-VDS 上のポートを使用しているため、トランスポート ノードを削除できない。	VMkernel インターフェイスが N-VDS スイッチからポートを使用しています。	すべての VMkernel インターフェイスの移行を N-VDS スイッチから VSS/VDS スイッチに戻します。トランスポート ノードを削除します。
9412	VMkernel が N-VDS から別の N-VDS に移行できない。	サポートされていないアクションです。	VSS または VDS スイッチに VMkernel インターフェイスの移行を戻します。これにより、別の N-VDS スイッチに VMkernel インターフェイスを移行することができます。
9413	VMkernel インターフェイスを別の論理スイッチに移行できない。	ステートフル ホストの場合は、論理スイッチに接続されている VMkernel を別の論理スイッチに移行することはできません。	VMkernel の移行を論理スイッチから VSS/VDS スイッチに戻します。次に、N-VDS の別の論理スイッチに VMkernel を移行します。
9414	VMkernel インターフェイスが重複している。	インストールおよびアンインストール マッピングの設定で VMkernel インターフェイスが重複してマッピングされています。	各 VMkernel インターフェイスがインストールおよびアンインストール マッピングで一意であることを確認します。
9415	ホスト上で仮想マシンがパワーオン状態である。	仮想マシンがパワーオン状態の場合、移行は続行されません。	VMkernel インターフェイスの移行を開始する前に、ホスト上の仮想マシンをパワーオフします。
9416	ホストに VMkernel が見つからない。	ネットワーク マッピングの設定で、ホスト上に配置されている VMkernel が指定されていません。	ネットワーク マッピングの設定で、配置されている VMkernel を指定します。

表 10-1. VMkernel の移行エラー（続き）

エラー コード	問題	原因	解決方法
9417	ポート グループが見つからない。	ネットワーク マッピングの設定で、ホスト上に配置されているポート グループが指定されていません。	ネットワーク マッピングの設定で、配置されているポート グループを指定します。
9419	論理スイッチが移行中に見つからない。	ネットワーク インターフェイス マッピングの設定で定義されている論理スイッチが見つかりません。	ネットワーク インターフェイス マッピングの設定で配置されている論理スイッチを指定します。
9420	論理ポートが移行中に見つからない。	移行中、NSX-T Data Center が論理スイッチに作成されたポートを検出しません。	移行が正常に実行されるには、論理スイッチから論理ポートが削除されていないことを確認します。
9421	移行プロセスの検証に必要なホストの情報がない。	インベントリからホストの情報を取得できません。	移行プロセスを再実行します。
9423	VMkernel インターフェイスに固定された物理 NIC が、正しいホスト スイッチに移行されない。	固定された物理 NIC が環境内に見つかりますが、VMkernel と物理 NIC が同じホスト スイッチに移行されていません。	VMkernel インターフェイスに固定された物理 NIC には、VMkernel とともに物理 NIC を同じホスト スイッチにマッピングするトランスポート ノード設定が必要です。
600	オブジェクトが見つかりません。	論理スイッチによって使用された、指定したトランスポート ゾーンが見つからない。 VMK マッピング先にある論理スイッチが見つかりません。	<ul style="list-style-type: none"> ■ 環境内にあるトランスポート ゾーンを指定します。 ■ 目的の論理スイッチを作成するか、既存の VLAN 論理スイッチを使用します。
8310	論理スイッチのタイプが無効である。	論理スイッチのタイプがオーバーレイになっています。	VLAN 論理スイッチを作成します。
9424	インストールまたはアンインストール設定に物理 NIC のみの移行とネットワーク マッピングの両方を同時に行うと、移行ができない。	移行は、これらのいずれかが設定されている場合にのみ、進行されます。	インストールまたはアンインストール設定に物理 NIC のみの移行か、またはネットワーク マッピングのいずれかのみを設定するようにします。

スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成

まず ESXi ホスト、KVM ホスト、またはベア メタル サーバを NSX-T Data Center ファブリックに追加してから、トランスポート ノードを設定する必要があります。

ファブリック ノードは、NSX-T Data Center 管理プレーンに登録されているノードであり、NSX-T Data Center のモジュールがインストールされています。ホストまたはベア メタル サーバを NSX-T Data Center オーバーレイの一部にするには、まず NSX-T Data Center ファブリックに追加する必要があります。

トランスポート ノードは、NSX-T Data Center オーバーレイまたは NSX-T Data Center VLAN ネットワークに参加するノードです。

KVM ホストまたはベア メタル サーバの場合は、N-VDS を事前に設定できます。また、NSX Manager で設定を実行することも可能です。ESXi ホストの場合、N-VDS は常に NSX Manager によって設定されます。

注： テンプレート仮想マシンを使用してトランスポート ノードを作成する場合は、ホストの `/etc/vmware/nsx/` に証明書がないことを確認してください。証明書がある場合、netcpa エージェントは証明書を作成しません。

ベア メタル サーバは、オーバーレイおよび VLAN トランスポート ゾーンをサポートします。管理インターフェイスを使用して、ベア メタル サーバを管理することができます。アプリケーション インターフェイスを使用すると、ベア メタル サーバ上のアプリケーションにアクセスできます。

単一の物理 NIC は、管理 IP インターフェイスとアプリケーション IP インターフェイスの両方に使用される IP アドレスを 1 つ提供します。

デュアル構成物理 NIC は、管理インターフェイス用の物理 NIC および一意の IP アドレスを 1 つずつ提供します。アプリケーション インターフェイス用の物理 NIC および一意の IP アドレスも提供します。

結合構成内の複数の物理 NIC は、管理インターフェイス用のデュアル構成物理 NIC および一意の IP アドレスを 1 つずつ提供します。アプリケーション インターフェイス用のデュアル構成物理 NIC および一意の IP アドレスも 1 つずつ提供します。

構成ごとに最大 4 台の N-VDS スイッチを追加できます (VLAN トランスポート ゾーン用に作成された標準 N-VDS、VLAN トランスポート ゾーン用に作成された拡張 N-VDS、オーバーレイ トランスポート ゾーン用に作成された標準 N-VDS、オーバーレイ トランスポート ゾーン用に作成された拡張 N-VDS)。

複数の標準オーバーレイ N-VDS スイッチと Edge 仮想マシンが同じホストで実行されている単一ホスト クラスタ トポロジの場合、NSX-T Data Center はトラフィックを分離して、1 番目の N-VDS を経由するトラフィックが 2 番目以降の N-VDS を経由するトラフィックから分離されるようにします。North-South トラフィックと外部ネットワークとの接続を許可するには、各 N-VDS 上の物理 NIC をホスト上の Edge 仮想マシンにマッピングする必要があります。1 番目のトランスポート ゾーンの仮想マシンから送信されるパケットは、外部ルーターまたは外部仮想マシンを経由して、2 番目のトランスポート ゾーン上の仮想マシンにルーティングする必要があります。

前提条件

- ホストが管理プレーンに追加されていて、接続が確立されている必要があります。
- トランスポート ゾーンが設定されている必要があります。
- アップリンク プロファイルが設定されている必要があります。設定されていない場合は、デフォルトのアップリンク プロファイルを使用できます。
- IP アドレス プールが設定されているか、ネットワーク環境 DHCP が使用できる必要があります。
- ホスト上で 1 個以上の未使用の物理 NIC が必要です。
- ホスト名
- 管理 IP アドレス
- ユーザー名
- パスワード
- (オプション) (KVM) SHA-256 SSL サンプリント

- (オプション) (ESXi) SHA-256 SSL サンプリント
- 必要なサードパーティ製パッケージがインストールされていることを確認します。[KVM ホストへのサードパーティ製パッケージのインストール](#) を参照してください。

手順

- 1 (オプション) ハイパーバイザー サンプリントを取得して、ホストをファブリックに追加するときに提供できるようにします。

- a ハイパーバイザー サンプリントの情報を収集します。

Linux シェルを使用します。

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509
-noout -fingerprint -sha256
```

ホストで ESXi CLI を使用します。

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:
0A:9E:A2:4E:3C:C4:F4
```

- b KVM ハイパーバイザーから SHA-256 サンプリントを取得して、KVM ホストでコマンドを実行します。

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed
's/ .*$/ /' | xxd -r -p | base64
```

- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 [管理元] フィールドで [スタンドアローン ホスト] を選択し、[+ 追加] をクリックします。
- 4 ファブリックに追加するスタンドアローン ホストまたはベア メタル サーバの詳細を入力します。

オプション	説明
名前と説明	<p>スタンドアローン ホストまたはベア メタル サーバを識別する名前を入力します。</p> <p>必要に応じて、ホストまたはベア メタル サーバで使用するオペレーティング システムの説明を追加することもできます。</p>
IP アドレス	<p>ホストまたはベア メタル サーバの IP アドレスを入力します。</p>
オペレーティング システム	<p>ドロップダウン メニューからオペレーティング システムを選択します。</p> <p>ホストまたはベア メタル サーバに応じて、いずれかのサポート対象オペレーティング システムを選択できます。システム要件 を参照してください。</p> <p>重要： サポートされている Linux の種類によっては、Linux ディストリビューションを実行しているベアメタル サーバと、ハイパーバイザー ホストとして使用される Linux ディストリビューションの違いを把握しておく必要があります。たとえば、オペレーティング システムとして Ubuntu サーバを選択すると、Linux サーバを実行するベアメタル サーバがセットアップされますが、Ubuntu KVM を選択すると、Linux ハイパーバイザーとして Ubuntu が展開されます。</p>

オプション	説明
ユーザー名とパスワード	ホストのユーザー名とパスワードを入力します。
SHA-256 サムプリント	認証用のホストのサムプリント値を入力します。 サムプリント値を空白のままにすると、サーバ指定の値を使用するように指示されます。 NSX-T Data Center がホストを検出して認証するまで数秒かかります。

5 (必須) KVM ホストまたはベア メタル サーバの場合は、N-VDS タイプを選択します。

オプション	説明
NSX 作成	NSX Manager は N-VDS を作成します。 このオプションはデフォルトで選択されています。
事前設定済み	N-VDS はすでに設定されています。

ESXi ホストの場合、N-VDS タイプは常に [NSX 作成] に設定されています。

6 標準 N-VDS の詳細を入力します。複数の N-VDS スイッチを単一ホスト上に構成できます。

オプション	説明
トランスポート ゾーン	ドロップダウン メニューから、このトランスポート ノードが属するトランスポート ゾーンを選択します。
N-VDS 名	このノードが属するトランスポート ゾーンの N-VDS 名と同じにする必要があります。
NIOC プロファイル	ESXi ホストの場合は、ドロップダウン メニューから NIOC プロファイルを選択します。
アップリンク プロファイル	ドロップダウン メニューから既存のアップリンク プロファイルを選択するか、アップリンクのカスタム プロファイルを作成します。 デフォルトのアップリンク プロファイルも使用できます。
LLDP プロファイル	デフォルトでは、NSX-T は LLDP ネイバーから LLDP パケットの受信のみを行います。 ただし、LLDP パケットを LLDP ネイバーに送信し、LLDP ネイバーから LLDP パケットを受信するように NSX-T を設定できます。
IP の割り当て	[DHCP を使用]、[IP アドレス プールを使用] または [固定 IP リストを使用] を選択します。 [固定 IP アドレスのリストを使用] を選択した場合は、IP アドレス、ゲートウェイ、およびサブネット マスクのコンマ区切りのリストを指定する必要があります。
IP アドレス プール	IP 割り当てに [IP アドレス プールを使用] を選択した場合は、IP アドレス プール名を指定します。

オプション	説明
物理 NIC	<p>トランスポート ノードに物理 NIC を追加します。デフォルトのアップリンクを使用すること、ドロップ ダウン メニューから既存のアップリンクを割り当てることもできます。</p> <p>[物理 NIC の追加] をクリックして、トランスポート ノードに追加の物理 NIC を構成します。</p> <p>注： このフィールドで追加した物理 NIC の移行は、[物理 NIC のみの移行]、[インストール用のネットワーク マッピング]、および [アンインストール用のネットワーク マッピング] の設定方法によって決まります。</p> <ul style="list-style-type: none"> ■ 標準 vSwitch または vSphere Distributed Switch を使用するなどの手段によって使用済みの物理 NIC を移行し、関連付けられた VMkernel マッピングを移行しないようにするには、[物理 NIC のみの移行] が有効になっていることを確認します。すでに使用されている場合、トランスポート ノードは [部分的成功] 状態になり、ファブリック ノードの LCP 接続の確立に失敗します。 ■ 使用済みの物理 NIC を、関連付けられた VMkernel ネットワーク マッピングとともに移行するには、[物理 NIC のみの移行] を無効にして、VMkernel ネットワーク マッピングを構成します。 ■ 空いている物理 NIC を移行するには、[物理 NIC のみの移行] を有効にします。
物理 NIC のみの移行	<p>このフィールドを設定する前に、次の点を考慮してください。</p> <ul style="list-style-type: none"> ■ 定義されている物理 NIC が使用済み NIC であるか、使用されていない NIC であるかを確認します。 ■ ホストの VMkernel インターフェイスを物理 NIC とともに移行する必要があるかどうかを判断します。 <p>フィールドを次のように設定します。</p> <ul style="list-style-type: none"> ■ VSS スイッチまたは VDS スイッチから N-VDS スイッチに物理 NIC のみを移行する場合は、[物理 NIC のみの移行] を有効にします。 ■ 使用済みの物理 NIC と関連付けられた VMkernel インターフェイス マッピングを移行する場合は、[物理 NIC のみの移行] を無効にします。VMkernel インターフェイスの移行マッピングが指定されている場合は、使用されていない、または使用可能な物理 NIC が N-VDS スイッチに接続されます。 <p>複数のホスト スイッチを使用しているホストで、次の操作を実行します。</p> <ul style="list-style-type: none"> ■ すべてのホスト スイッチで物理 NIC のみを移行する場合は、物理 NIC を 1 回の操作で移行できます。 ■ VMkernel インターフェイスを移行するホスト スイッチと、物理 NIC のみを移行するホスト スイッチが混在している場合は、次の操作を実行します。 <ol style="list-style-type: none"> 1 最初の操作で、物理 NIC のみを移行します。 2 次の操作で、VMkernel インターフェイスを移行します。[物理 NIC のみの移行] が無効になっていることを確認します。 <p>物理 NIC のみの移行と VMkernel インターフェイスの移行は、複数のホストで同時にサポートされません。</p> <p>注： 管理ネットワークの NIC を移行するには、関連付けられた VMkernel ネットワークのマッピングを設定し、[物理 NIC のみの移行] を無効のままにします。管理 NIC のみを移行する場合、ホストの接続は切断されます。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>

オプション	説明
インストール用のネットワーク マッピング	<p>インストール中に VMkernel を N-VDS スイッチに移行するには、VMkernel を既存の論理スイッチにマッピングします。NSX Manager により、VMkernel が N-VDS 上のマッピングされた論理スイッチに移行されます。</p> <p>注意： 管理 NIC が接続されていた VLAN と同じ VLAN に論理スイッチが接続されていて、そこに管理 NIC および管理 VMkernel インターフェイスが移行されることを確認します。vmnic<n> および VMkernel<n> が異なる VLAN に移行された場合は、ホストとの接続が切断されます。</p> <p>注意： 固定された物理 NIC の場合は、物理 NIC から VMkernel インターフェイスへのホスト スイッチのマッピングが、トランスポート ノード プロファイルで指定されている設定と一致することを確認します。検証手順の一環として、NSX-T Data Center はマッピングを検証します。検証が成功すると、VMkernel インターフェイスが正常に N-VDS スイッチに移行したことになります。また、VMkernel インターフェイスを N-VDS スイッチに移行すると、NSX-T Data Center にホスト スイッチのマッピング設定が保存されなくなるため、アンインストール用のネットワーク マッピングを設定する必要があります。このマッピングが設定されていない場合は、VSS スイッチまたは VDS スイッチに移行し直した後に、vSAN などのサービスとの接続が切断されることがあります。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>
アンインストール用のネットワーク マッピング	<p>アンインストール中に VMkernel の移行を元に戻すには、VSS または VDS のポート グループに VMkernel をマッピングして、VMkernel を移行し直す VSS または VDS 上のポート グループを NSX Manager が認識できるようにします。VDS スイッチに移行する場合は、ポート グループのタイプが短期であることを確認します。</p> <p>注意： 固定された物理 NIC の場合は、物理 NIC から VMkernel インターフェイスへのトランスポート ノード プロファイルのマッピングが、ホスト スイッチで指定されている設定と一致することを確認します。VMkernel インターフェイスを N-VDS スイッチに移行すると、NSX-T Data Center にホスト スイッチのマッピング設定が保存されなくなるため、アンインストール用のネットワーク マッピングを設定する必要があります。このマッピングが設定されていない場合は、VSS スイッチまたは VDS スイッチに移行し直した後に、vSAN などのサービスとの接続が切断されることがあります。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>

7 拡張データパス N-VDS の詳細を入力します。複数の N-VDS スイッチを単一ホスト上に構成できます。

オプション	説明
N-VDS 名	このノードが属するトランスポート ゾーンの N-VDS 名と同じにする必要があります。
IP の割り当て	[DHCP を使用]、[IP アドレス プールを使用] または [固定 IP リストを使用] を選択します。 [固定 IP アドレスのリストを使用] を選択した場合は、IP アドレス、ゲートウェイ、およびサブネット マスクのコンマ区切りのリストを指定する必要があります。
IP アドレス プール	IP の割り当てに [IP アドレス プールを使用] を選択した場合は、IP アドレス プール名を指定します。

オプション	説明
物理 NIC	<p>トランスポート ノードに物理 NIC を追加します。デフォルトのアップリンクを使用すること、ドロップ ダウン メニューから既存のアップリンクを割り当てることもできます。</p> <p>[物理 NIC の追加] をクリックして、トランスポート ノードに追加の物理 NIC を構成します。</p> <p>注： このフィールドで追加した物理 NIC の移行は、[物理 NIC のみの移行]、[インストール用のネットワーク マッピング]、および [アンインストール用のネットワーク マッピング] の設定方法によって決まります。</p> <ul style="list-style-type: none"> ■ 標準 vSwitch または vSphere Distributed Switch を使用するなどの手段によって使用済みの物理 NIC を移行し、関連付けられた VMkernel マッピングを移行しないようにするには、[物理 NIC のみの移行] が有効になっていることを確認します。すでに使用されている場合、トランスポート ノードは [部分的成功] 状態になり、ファブリック ノードの LCP 接続の確立に失敗します。 ■ 使用済みの物理 NIC を、関連付けられた VMkernel ネットワーク マッピングとともに移行するには、[物理 NIC のみの移行] を無効にして、VMkernel ネットワーク マッピングを構成します。 ■ 空いている物理 NIC を移行するには、[物理 NIC のみの移行] を有効にします。
アップリンク	ドロップダウン メニューからアップリンク プロファイルを選択します。
CPU の設定	<p>[NUMA ノード インデックス] ドロップダウン メニューで、N-VDS スイッチに割り当てる NUMA ノードを選択します。ノード上にある最初の NUMA ノードは、値 0 で表されます。</p> <p><code>esxcli hardware memory get</code> コマンドを実行して、ホスト上の NUMA ノード数を確認できます。</p> <p>注： N-VDS スイッチとアフィニティがある NUMA ノードの数を変更する場合は、NUMA ノード インデックス値を更新することができます。</p> <p>[NUMA ノードあたりの Lcore 数] ドロップダウン メニューで、拡張データバスで使用する必要がある論理コアの数を選択します。</p> <p><code>esxcli network ens maxLcores get</code> コマンドを実行して、NUMA ノード上に作成できる論理コアの最大数を確認できます。</p> <p>注： 使用可能な NUMA ノードと論理コアがすべて使用されている場合、トランスポート ノードに追加した新しいスイッチは ENS トラフィック用に有効にすることができません。</p>

8 事前構成済みの N-VDS の場合は、次の詳細を提供します。

オプション	説明
N-VDS の外部 ID	このノードが属するトランスポート ゾーンの N-VDS 名と同じにする必要があります。
VTEP	仮想トンネル エンドポイントの名前。

9 [ホスト トランスポート ノード] 画面で接続状態を表示します。

ホストまたはベア メタル サーバをトランスポート ノードとして追加すると、NSX Manager との接続は 3 ～ 4 分後に [稼動中] に変わります。

注： 構成ハッシュの不一致が原因でホストの準備が失敗し、検出ループが発生する場合は、次のいずれかのオプションを試してください。

- FQDN を false に設定し、ホストで nsx-proxy を再起動します。これにより、ホストと NSX Manager は FQDN を使用しなくなります。

- または

FQDN モードを使用する場合は、ホスト名に FQDN を使用して NSX Manager アプライアンスを展開します。大文字と小文字を区別したスペルが、NSX Manager IP アドレスの正引きと逆引きの両方の DNS 参照と一致していることを確認します。この設定は、すべての NSX Manager ノードで一致している必要があります。

10 または、CLI コマンドを使用して、接続ステータスを表示します。

- ◆ ESXi の場合は、`esxcli network ip connection list | grep 1234` コマンドを入力します。

```
# esxcli network ip connection list | grep 1234
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 [ESTABLISHED] 1000144459
newreno netcpa
```

- ◆ KVM の場合には、`netstat -anp --tcp | grep 1234` コマンドを入力します。

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp    0    0 192.168.210.54:57794 192.168.110.34:1234 [ESTABLISHED] -
```

11 ホストまたはベア メタル サーバに NSX-T Data Center モジュールがインストールされていることを確認します。

ホストまたはベア メタル サーバを NSX-T Data Center ファブリックに追加すると、一連の NSX-T Data Center モジュールがホストまたはベア メタル サーバにインストールされます。

次のように、さまざまなホストのモジュールがパッケージ化されています。

- RHEL または CentOS の KVM - RPM
- Ubuntu の KVM - DEB
- ESXi で `esxcli software vib list | grep nsx` コマンドを入力します。

日付は、インストールの実行日です。

- RHEL または CentOS で `yum list installed` コマンドまたは `rpm -qa` コマンドを入力します。
- Ubuntu で `dpkg --get-selections` コマンドを入力します。

- 12 (オプション) 500 台以上のハイパーバイザーを使用している場合は、特定のプロセッサのポーリング間隔を変更します。

500 台を超えるハイパーバイザーがある場合は、NSX Manager の CPU 使用率が上昇し、パフォーマンス上の問題が発生することがあります。

- a NSX-T Data Center CLI コマンド `copy file` または API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` を使用して、`aggsvc_change_intervals.py` スクリプトをホストにコピーします。
- b NSX-T Data Center ファイル ストアにあるスクリプトを実行します。

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

- c (オプション) ポーリング間隔をデフォルト値に戻します。

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```

結果

注： NSX-T Data Center で作成された N-VDS の場合、トランスポート ノードの作成後に、トンネル エンドポイントへの IP アドレスの割り当てなどの設定を変更するには、ホストの CLI ではなく NSX Manager の GUI から行う必要があります。

次のステップ

vSphere 標準スイッチから N-VDS にネットワーク インターフェイスを移行します。[VMkernel の N-VDS スイッチへの移行](#) を参照してください。

管理対象ホストのトランスポート ノードの構成

vCenter Server がある場合、手動で設定しなくてもすべての NSX-T Data Center ホストで、トランスポート ノードのインストールと作成を自動化できます。

トランスポート ノードがすでに設定されている場合は、そのノードではトランスポート ノードの自動作成は実行できません。

前提条件

- vCenter Server 内のすべてのホストがパワーオンされていることを確認します。
- システム要件を満たしていることを確認します。[システム要件](#)を参照してください。
- トランスポート ゾーンが使用可能であることを確認します。[トランスポート ゾーンの作成](#) を参照してください。
- トランスポート ノード プロファイルが設定されていることを確認します。[トランスポート ノード プロファイルの追加](#) を参照してください。

- vSphere ロックダウン モードの例外リストに期限切れのユーザー アカウントが含まれていると、vSphere での NSX-T Data Center のインストールは失敗します。インストールを開始する前に、期限切れのユーザー アカウントをすべて削除してください。ロックダウン モードでアクセス権を持つアカウントの詳細については、『vSphere セキュリティ ガイド』で「ロックダウン モードでのアクセス権を持つアカウントの指定」を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 [管理対象] ドロップダウン メニューから既存の vCenter Server を選択します。

この画面には、選択した vCenter Server で使用可能な vSphere クラスタまたは ESXi ホストが表示されます。ESXi ホストを表示するには、クラスタの展開が必要になることがあります。

- 4 リストから 1 台のホストを選択し、[NSX の設定] をクリックします。
[NSX の設定] ダイアログ ボックスが開きます。
 - a [ホストの詳細] パネルでホスト名を確認します。必要に応じて、説明を追加できます。
 - b [次へ] をクリックして、[NSX の設定] パネルに移動します。
 - c 使用可能なトランスポート ゾーンを選択し、[>] ボタンをクリックして、トランスポート ノード プロファイルにトランスポート ゾーンを含めます。
- 5 [ホストの詳細] パネルでホスト名を確認し、[次へ] をクリックします。
必要に応じて、説明を追加できます。
- 6 [NSX の設定] パネルで、必要なトランスポート ゾーンを選択します。
複数のトランスポート ゾーンを選択できます。
- 7 [N-VDS] タブをクリックして、スイッチの詳細を入力します。

オプション	説明
N-VDS 名	トランスポート ノードがトランスポート ゾーンに接続されている場合は、N-VDS 用に入力した名前がトランスポート ゾーンで指定された N-VDS の名前と同じであることを確認します。トランスポート ゾーンをトランスポート ゾーンに接続しなくても、トランスポート ノードを作成できます。
関連付けられたトランスポート ゾーン	関連付けられているホスト スイッチで認識されているトランスポート ゾーンが表示されます。トランスポート ノード プロファイル内にある N-VDS で認識されていないトランスポート ゾーンは、追加できません。
NIOC プロファイル	ドロップダウン メニューから NIOC プロファイルを選択します。 トラフィック リソース用にプロファイル内で指定した帯域幅の割り当てが適用されます。
アップリンク プロファイル	ドロップダウン メニューから既存のアップリンク プロファイルを選択するか、アップリンクのカスタム プロファイルを作成します。 デフォルトのアップリンク プロファイルも使用できます。

オプション	説明
LLDP プロファイル	<p>デフォルトでは、NSX-T は LLDP ネイバーから LLDP パケットの受信のみを行います。</p> <p>ただし、LLDP パケットを LLDP ネイバーに送信し、LLDP ネイバーから LLDP パケットを受信するように NSX-T を設定できます。</p>
IP の割り当て	<p>[DHCP を使用]、[IP アドレス プールを使用]、または [固定 IP アドレスのリストを使用] を選択して、IP アドレスをトランスポート ノードの仮想トンネル エンドポイント (VTEP) に割り当てます。</p> <p>[固定 IP アドレスのリストを使用] を選択した場合は、IP アドレス、ゲートウェイ、およびサブネット マスクのコンマ区切りのリストを指定する必要があります。トランスポート ノードのすべての VTEP が同じサブネット内に配置されている必要があります。そうでない場合は、双方向フロー (BFD) セッションが確立されません。</p>
IP アドレス プール	<p>IP アドレスの割り当てに [IP アドレス プールを使用] を選択した場合は、IP アドレス プール名を指定します。</p>
物理 NIC	<p>トランスポート ノードに物理 NIC を追加します。デフォルトのアップリンクを使用すること、ドロップ ダウン メニューから既存のアップリンクを割り当てることもできます。</p> <p>[物理 NIC の追加] をクリックして、トランスポート ノードに追加の物理 NIC を設定します。</p> <p>注： このフィールドで追加した物理 NIC の移行は、[物理 NIC のみの移行]、[インストール用のネットワーク マッピング]、および [アンインストール用のネットワーク マッピング] の設定方法によって決まります。</p> <ul style="list-style-type: none"> ■ 標準 vSwitch または vSphere Distributed Switch を使用するなどの手段によって使用済みの物理 NIC を移行し、関連付けられた VMkernel マッピングを移行しないようにするには、[物理 NIC のみの移行] が有効になっていることを確認します。すでに使用されている場合、トランスポート ノードは [部分的成功] 状態になり、ファブリック ノードの LCP 接続の確立に失敗します。 ■ 使用済みの物理 NIC を、関連付けられた VMkernel ネットワーク マッピングとともに移行するには、[物理 NIC のみの移行] を無効にして、VMkernel ネットワーク マッピングを設定します。 ■ 空いている物理 NIC を移行するには、[物理 NIC のみの移行] を有効にします。

オプション	説明
物理 NIC のみの移行	<p>このフィールドを設定する前に、次の点を考慮してください。</p> <ul style="list-style-type: none"> ■ 定義されている物理 NIC が使用済み NIC であるか、使用されていない NIC であるかを確認します。 ■ ホストの VMkernel インターフェイスを物理 NIC とともに移行する必要があるかどうかを判断します。 <p>フィールドを次のように設定します。</p> <ul style="list-style-type: none"> ■ VSS スイッチまたは VDS スイッチから N-VDS スイッチに物理 NIC のみを移行する場合は、[物理 NIC のみの移行] を有効にします。 ■ 使用済みの物理 NIC と関連付けられた VMkernel インターフェイス マッピングを移行する場合は、[物理 NIC のみの移行] を無効にします。VMkernel インターフェイスの移行マッピングが指定されている場合は、使用されていない、または使用可能な物理 NIC が N-VDS スイッチに接続されます。 <p>複数のホスト スイッチを使用しているホストで、次の操作を実行します。</p> <ul style="list-style-type: none"> ■ すべてのホスト スイッチで物理 NIC のみを移行する場合は、物理 NIC を 1 回の操作で移行できます。 ■ VMkernel インターフェイスを移行するホスト スイッチと、物理 NIC のみを移行するホスト スイッチが混在している場合は、次の操作を実行します。 <ol style="list-style-type: none"> 1 最初の操作で、物理 NIC のみを移行します。 2 次の操作で、VMkernel インターフェイスを移行します。[物理 NIC のみの移行] が無効になっていることを確認します。 <p>物理 NIC のみの移行と VMkernel インターフェイスの移行は、複数のホストで同時にサポートされません。</p> <hr/> <p>注： 管理ネットワークの NIC を移行するには、関連付けられた VMkernel ネットワークのマッピングを設定し、[物理 NIC のみの移行] を無効のままにします。管理 NIC のみを移行する場合、ホストの接続は切断されます。</p> <hr/> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>

オプション	説明
インストール用のネットワーク マッピング	<p>インストール中に VMkernel を N-VDS スイッチに移行するには、VMkernel を既存の論理スイッチにマッピングします。NSX Manager により、VMkernel が N-VDS 上のマッピングされた論理スイッチに移行されます。</p> <p>注意： 管理 NIC が接続されていた VLAN と同じ VLAN に論理スイッチが接続されていて、そこに管理 NIC および管理 VMkernel インターフェイスが移行されることを確認します。vmnic<n> および VMkernel<n> が異なる VLAN に移行された場合は、ホストとの接続が切断されます。</p> <p>注意： 固定された物理 NIC の場合は、物理 NIC から VMkernel インターフェイスへのホスト スイッチのマッピングが、トランスポート ノード プロファイルで指定されている設定と一致することを確認します。検証手順の一環として、NSX-T Data Center はマッピングを検証します。検証が成功すると、VMkernel インターフェイスが正常に N-VDS スイッチに移行したことになります。VMkernel インターフェイスを N-VDS スイッチに移行すると、NSX-T Data Center にホスト スイッチのマッピング設定が保存されなくなるため、アンインストール用のネットワーク マッピングも設定する必要があります。このマッピングが設定されていない場合は、VSS スイッチまたは VDS スイッチに移行し直した後に、vSAN などのサービスとの接続が切断されることがあります。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>
アンインストール用のネットワーク マッピング	<p>アンインストール中に VMkernel の移行を元に戻すには、VSS または VDS のポート グループに VMkernel をマッピングして、VMkernel を移行し直す VSS または VDS 上のポート グループを NSX Manager が認識できるようにします。VDS スイッチの場合は、ポート グループのタイプが短期であることを確認します。</p> <p>注意： 固定された物理 NIC の場合は、物理 NIC から VMkernel インターフェイスへのトランスポート ノード プロファイルのマッピングが、ホスト スイッチで指定されている設定と一致することを確認します。VMkernel インターフェイスを N-VDS スイッチに移行すると、NSX-T Data Center にホスト スイッチのマッピング設定が保存されなくなるため、アンインストール用のネットワーク マッピングを設定する必要があります。このマッピングが設定されていない場合は、VSS スイッチまたは VDS スイッチに移行し直した後に、vSAN などのサービスとの接続が切断されることがあります。</p> <p>詳細については、VMkernel の N-VDS スイッチへの移行を参照してください。</p>

- 8 複数のトランスポート ゾーンを選択した場合は、[+ N-VDS の追加] を再度クリックして、他のトランスポート ゾーンのスイッチを設定します。

- 9 [終了] をクリックして、設定を完了します。

- 10 (オプション) ESXi の接続状況を確認します。

```
# esxcli network ip connection list | grep 1235
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 [ESTABLISHED] 1000144459
newreno netcpa
```

- 11 [ホスト トランスポート ノード] 画面で、クラスタ内のホストの NSX Manager 接続状態が [稼動中]、NSX-T Data Center の設定状態が [成功] であることを確認します。

トランスポート ゾーンがクラスタ内のホストに適用されていることも確認できます。

- 12 (オプション) トランスポート ゾーン内のホストから NSX-T Data Center のインストールとトランスポート ノードを削除します。

- a 1 台以上のホストを選択して、[アクション] - [NSX の削除] の順にクリックします。

アンインストールには最大で 3 分ほどかかります。NSX-T Data Center をアンインストールすると、ホストのトランスポート ノードの設定が削除され、ホストはトランスポート ゾーンおよび N-VDS スイッチから接続解除されます。vCenter Server クラスタに追加された新しいホストは、トランスポート ノード プロファイルがクラスタに再適用されるまで自動的に設定されません。

13 (オプション) トランスポート ゾーンからトランスポート ノードを削除します。

- a 1つのトランスポート ノードを選択して、[アクション] - [トランスポート ゾーンから削除] の順にクリックします。

次のステップ

論理スイッチを作成して、論理ポートを割り当てます。『NSX-T Data Center 管理ガイド』の「高度なスイッチング」セクションを参照してください。

リンク集約による ESXi ホスト トランスポート ノードの設定

この手順では、リンク集約グループが設定されたアップリンク プロファイルを作成する方法、およびそのアップリンク プロファイルを使用するように ESXi ホスト トランスポート ノードを設定する方法について説明します。

前提条件

- アップリンク プロファイルの作成手順について理解していること。[アップリンク プロファイルの作成](#) を参照してください。
- ホスト トランスポート ノードの作成手順について理解していること。[スタンドアローン ホストまたはベア メタル サーバ トランスポート ノードの作成](#) を参照してください。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [アップリンク プロファイル] - [追加] を選択します。
- 3 名前を入力します。必要に応じて説明も入力します。
たとえば、「**uplink-profile1**」という名前を入力します。
- 4 [LAG] の [追加] をクリックして、リンク集約グループを追加します。
たとえば、2つのアップリンクを持つ **lag1** という LAG を追加します。
- 5 [チーミング] で、[デフォルトのチーミング] を選択します。
- 6 [アクティブ アップリンク] フィールドに、手順 4 で追加した LAG の名前を入力します。この例では、LAG 名は **lag1** です。
- 7 [トランスポート VLAN] および [MTU] の値を入力します。
- 8 ダイアログ ボックスの下部にある [追加] をクリックします。
- 9 [チーミング] で [追加] をクリックして、リンク集約のエントリを追加します。
- 10 [ファブリック] - [ノード] - [ホスト トランスポート ノード] - [追加] の順に選択します。

- 11 [ホストの詳細] タブで、IP アドレス、OS 名、管理者認証情報、ホストの SHA-256 サムプリントを入力します。
- 12 [N-VDS] タブで、手順 3 で作成したアップリンク プロファイル **uplink-profile1** を選択します。
- 13 [物理 NIC] フィールドで、物理 NIC とアップリンクのドロップダウン リストに新しい NIC とアップリンク プロファイルが反映されます。ここでは、手順 4 で作成された LAG **lag1** に対応するアップリンク **lag1-0** と **lag1-1** が表示されます。**lag1-0** の物理 NIC および **lag1-1** の物理 NIC を選択します。
- 14 その他のフィールドの情報を入力します。

トランスポート ノードの状態の確認

トランスポート ノードの作成プロセスが正常に機能していることを確認します。

ホスト トランスポート ノードの作成後、ホスト上に N-VDS を配置します。

手順

- 1 NSX-T Data Center にログインします。
- 2 [トランスポート ノード] 画面に移動し、N-VDS の状態を確認します。
- 3 または、`esxcli network ip interface list` コマンドを使用して、ESXi 上の N-VDS を確認します。

ESXi でのコマンドの出力には、Distributed Switch (VDS) の名前がついた vmk インターフェイス (vmk10 など) が含まれます。この Distributed Switch の名前は、トランスポート ゾーンとトランスポート ノードを設定する際に使用した名前です。

```
# esxcli network ip interface list
...

vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: [overlay-hostswitch]
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network Type: N/A
  External ID: N/A
  MTU: 1600
  TSO MSS: 65535
  Port ID: 67108895

...
```

vSphere Client を使用している場合、ユーザー インターフェイスでホストの [設定] - [ネットワーク アダプタ] を順に選択し、インストールされている N-VDS を確認できます。

N-VDS を確認するための KVM のコマンドは、`ovs-vsctl show` です。KVM では、N-VDS の名前は `nsx-switch.0` と表示されます。トランスポート ノードの設定で使用した名前とは異なる点に注意してください。これは仕様です。

```
# ovs-vsctl show
...
    Bridge "nsx-switch.0"
      Port "nsx-uplink.0"
        Interface "em2"
      Port "nsx-vtep0.0"
        tag: 0
        Interface "nsx-vtep0.0"
          type: internal
      Port "nsx-switch.0"
        Interface "nsx-switch.0"
          type: internal
    ovs_version: "2.4.1.3340774"
```

4 トランスポート ノードに割り当てられているトンネル エンドポイント アドレスを確認します。

次に示すように、`vmk10` のインターフェイスは、NSX-T Data Center IP アドレス プールまたは DHCP から IP アドレスを受け取ります。

```
# esxcli network ip interface ipv4 get
```

Name	IPv4 Address	IPv4 Netmask	IPv4 Broadcast	Address Type	DHCP	DNS
-----	-----	-----	-----	-----	-----	-----
vmk0	192.168.210.53	255.255.255.0	192.168.210.255	STATIC	false	
vmk1	10.20.20.53	255.255.255.0	10.20.20.255	STATIC	false	
[vmk10	192.168.250.3]	255.255.255.0	192.168.250.255	STATIC	false	

KVM では、`ifconfig` コマンドを使用して、トンネル エンドポイントと IP アドレス割り当てを確認できます。

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet HWaddr ba:30:ae:aa:26:53
    inet addr:[192.168.250.4] Bcast:192.168.250.255 Mask:255.255.255.0
    ...
```

5 API でトランスポート ノードの状態を確認します。

GET <https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state> API 呼び出しを使用します。次はその例です。

```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}
```

ESXi の VMkernel アダプタおよび物理アダプタの移行

ホストをトランスポート ノードとして準備した後、VMkernel アダプタと物理アダプタの現在の移行設定を変更できます。

前提条件

- ホストに未使用の物理アダプタが1つ以上存在することを確認します。
- ホストに VMkernel アダプタとポート グループが存在していることを確認します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] > [ファブリック] > [ホスト トランスポート ノード] の順に移動します。
- 3 トランスポート ノードを選択して、[アクション] > [ESX の VMkernel アダプタおよび物理アダプタの移行] の順にクリックします。

4 [ESX の VMkernel アダプタおよび物理アダプタの移行] に、次の詳細を入力します。

フィールド	説明
方向	<p>次のように選択します。</p> <ul style="list-style-type: none"> ■ [論理スイッチに移行] : VMkernel アダプタを VSS または VDS スイッチから NSX-T Data Center の N-VDS スイッチに移行します。 ■ [ポート グループに移行] : VMkernel アダプタを N-VDS スイッチから VSS または VDS スイッチに移行します。
スイッチの選択	VMkernel アダプタと物理アダプタを移行するスイッチを選択します。使用可能なスイッチから選択できます。
移行する VMkernel アダプタの選択	[追加] をクリックして、VMkernel アダプタ名を入力します。移行先の場所に応じて、宛先に論理スイッチまたはポート グループを選択します。
N-VDS 内の物理アダプタの編集	[追加] をクリックして、物理アダプタ名を入力します。このアダプタをホスト スイッチ上のアップリンクにマッピングします。

5 [保存] をクリックして、VMkernel アダプタと物理アダプタの移行を開始します。

結果

更新された VMkernel アダプタと物理アダプタが N-VDS スイッチに移行されるか、ESXi ホストの VSS または VDS スイッチに移行されます。

NSX メンテナンス モード

機能していないトランスポート ノードへの仮想マシンの vMotion を回避するには、そのトランスポート ノードを NSX メンテナンス モードにします。

トランスポート ノードを NSX メンテナンス モードにするには、ノードを選択して、[アクション]、[NSX メンテナンス モード] のにクリックします。

ホストを NSX メンテナンス モードにすると、トランスポート ノードがネットワークに参加できなくなります。ホスト スイッチとして N-VDS または vSphere Distributed Switch を使用している他のトランスポート ノードで実行されている仮想マシンは、このトランスポート ノードに vMotion で移動できません。また、ESXi または KVM ホストで論理ネットワークを構成することはできません。

トランスポート ノードを NSX メンテナンス モードに切り替えるシナリオ：

- トランスポート ノードが機能していません。
- ホストで NSX-T に関係のないハードウェアまたはソフトウェアの問題がある場合や、NSX-T でノードとその構成を維持する場合は、ホストを NSX メンテナンス モードに切り替えます。
- トランスポート ノードでアップグレードに失敗すると、トランスポート ノードは自動的に NSX メンテナンス モードになります。

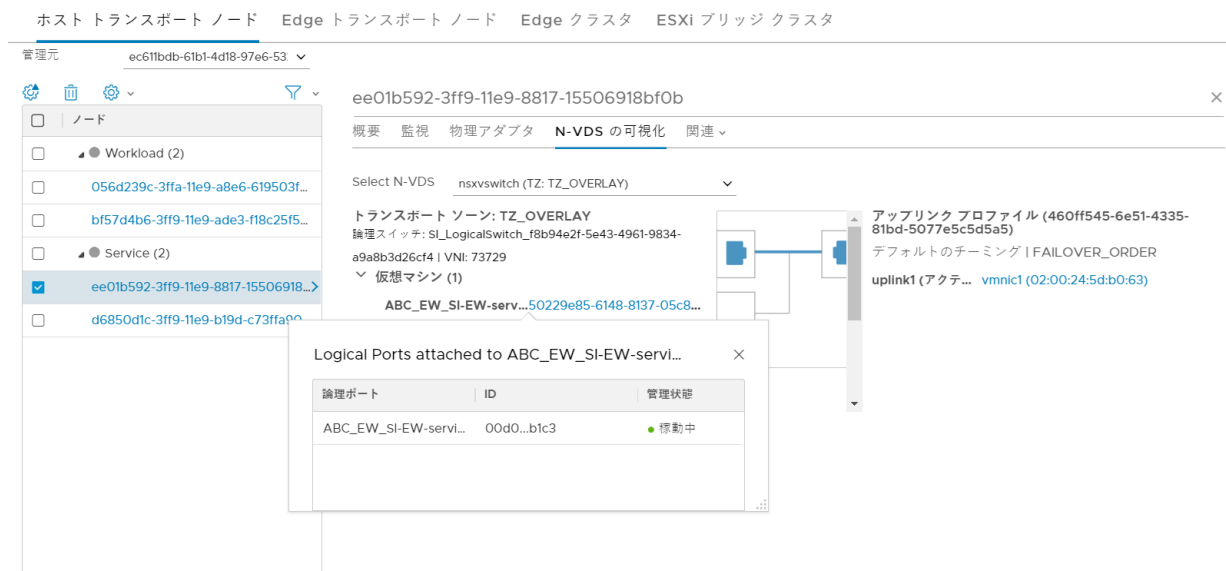
NSX メンテナンス モードのトランスポート ノードはアップグレードされません。

N-VDS の可視表示

N-VDS の詳細なビューを個別のホストのレベルで利用できます。NSX-T Data Center は、N-VDS のアップリンクとトランスポート ゾーンに関連付けられた仮想マシン間の接続状態の可視表示を提供します。可視表示されるオブジェクトには、チーミング ポリシー、仮想マシンに接続を提供するアップリンクと物理 NIC などがあります。それ以外に可視表示されるオブジェクトには、仮想マシン、関連付けられている論理ポートおよびスイッチ、仮想マシンの状態があります。可視表示により、N-VDS が管理しやすくなります。

注： N-VDS オブジェクトの可視化は、ESXi ホストのみでサポートされます。

図 10-3. N-VDS の可視化



手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 [管理元] フィールドで、[スタンドアローン ホスト] または *compute manager* を選択します。
- 4 ホストを選択します。
- 5 [N-VDS の可視化] タブをクリックします。
- 6 N-VDS を選択します。

NSX-T に仮想マシンに接続されているアップリンク プロファイル、仮想マシンに関連付けられている論理ポート、トランスポート ゾーンに接続されている論理スイッチが表示されます。

- 7 仮想マシンに接続されているアップリンク プロファイルと、仮想マシンが接続している論理ポートを表示するには、仮想マシンを選択します。

NSX-T に、仮想マシンとアップリンク プロファイル間の接続が表示されます。

- 8 アップリンク プロファイルに接続されている仮想マシンを表示するには、アップリンク プロファイルを選択します。

- 9 仮想マシンに関連付けられている論理ポートを表示するには、論理スイッチを展開して、仮想マシンをクリックします。

論理ポートの詳細が別のダイアログ ボックスに表示されます。

注： 論理ポートの管理状態は、ダイアログ ボックスに表示されます。運用状態が停止の場合、ダイアログ ボックスには表示されません。

VLAN ID 範囲と MTU 設定の健全性チェック

健全性チェックの API を実行し、指定した VLAN ID 範囲と物理スイッチの設定に対応するトランスポート ノードの MTU 設定との互換性を確認します。

VLAN または MTU の設定が一致していないと、構成エラーが発生し、接続停止の原因となる可能性があります。

注：

- 健全性チェックの結果は、ネットワーク構成エラーの可能性を示す指標となります。たとえば、異なる L2 ドメインのホストで健全性チェックを実行すると、トランキングなし VLAN ID が生成されます。健全性チェックツールで正しい結果を得るにはホストが同じ L2 ドメインに存在している必要があるため、この結果は構成エラーと見なすことはできません。
- 一度に実行される健全性チェック操作は 50 個までです。
- 健全性チェックの完了後、NSX-T Data Center は 24 時間分の結果を保持します。

健全性チェックの操作では、NSX-T Data Center opsAgent がトランスポート ノードから別のノードにプローブパケットを送信し、指定した VLAN ID 範囲と物理スイッチの設定に対応するトランスポート ノードの MTU 値との互換性を検証します。

検証する VLAN ID 範囲が増えると、待機時間が増加します。

VLAN の数	待機時間（秒）
[3073,4095]	150
[1025, 3072]	120
[513, 1024]	80
[128, 512]	60
[64, 127]	30
[1, 63]	20

前提条件

- VLAN と MTU のチェックが機能するように、2 つ以上のアップリンクが N-VDS に設定されている必要があります。
- 同じ L2 ドメインにトランスポート ノードが必要です。
- 健全性チェックは、v6.7U2 以降を実行している ESX ホストでサポートされます。

手順

1 手動の健全性チェックを作成します。

POST https://<NSXManager_IP>/api/v1/manual-health-checks

Example Request:

POST https://<nsx-mgr>/api/v1/manual-health-checks

```
{
  "resource_type": "ManualHealthCheck",
  "display_name": "Manual HealthCheck 002",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [{
      "start": 0,
      "end": 6
    }],
  },
}
```

Example Response:

```
{
  "operation_status": "FINISHED",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [
      {
        "start": 0,
        "end": 6
      }
    ]
  },
  "result": {
    "vlan_mtu_status": "UNTRUNKED",
    "results_per_transport_node": [
      {
        "transport_node_id": "dfcabffa-8839-11e9-b30e-6f45344d8a04",
        "result_on_host_switch": {
          "host_switch_name": "nsxvswitch",
          "results_per_uplink": [
            {
              "uplink_name": "uplink1",
              "vlan_and_mtu_allowed": [
                {
                  "start": 0,
                  "end": 0
                }
              ],
              "mtu_disallowed": [],
              "vlan_disallowed": [
                {
                  "start": 1,
                  "end": 6
                }
              ]
            }
          ]
        }
      }
    ]
  }
}
```

```

    ]
  },
  {
    "transport_node_id": "a300ea62-8839-11e9-a94e-31732bb71949",
    "result_on_host_switch": {
      "host_switch_name": "nsxvswitch",
      "results_per_uplink": [
        {
          "uplink_name": "uplink1",
          "vlan_and_mtu_allowed": [
            {
              "start": 0,
              "end": 0
            }
          ],
          "mtu_disallowed": [],
          "vlan_disallowed": [
            {
              "start": 1,
              "end": 6
            }
          ]
        }
      ]
    }
  ]
}
]
},
"resource_type": "ManualHealthCheck",
"id": "8a56ed9e-a31b-479e-987b-2dbfbde07c38",
"display_name": "mc1",
"_create_user": "admin",
"_create_time": 1560149933059,
"_last_modified_user": "system",
"_last_modified_time": 1560149971220,
"_system_owned": false,
"_protection": "NOT_PROTECTED",
"_revision": 0
}

```

ID が 8a56ed9e-a31b-479e-987b-2dbfbde07c38 の新しい健全性チェック オブジェクトが作成されます。

- 2 リストにあるすべての健全性チェック操作を手動で開始するには、API 呼び出しを行います。

GET https://<NSXManager_IP>/api/v1/manual-health-checks

- 3 手動の健全性チェックを削除するには、API 呼び出しを行います。

DELETE https://<NSXManager_IP>/api/v1/manual-health-checks/<Health-check-ID>

- 4 1つの健全性チェックを手動で開始するには、API 呼び出しを実行します。

GET https://<NSXManager_IP>/api/v1/manual-health-checks/<Health-check-ID>

結果

API 応答セクションには、健全性チェックの結果が含まれます。NSX Ops エージェントは、ターゲット トランスポート ノードから確認パケットを受信し、物理スイッチでサポートされている VLAN ID 範囲を取得します。

- トランキングなし：物理スイッチと互換性のない VLAN ID 範囲を返します。物理スイッチと互換性のある VLAN ID の範囲も返します。
- トランキング：物理スイッチと互換性のある VLAN ID 範囲のリストを返します。
- 不明：インフラストラクチャの問題または KVM や Edge などのサポートされていないプラットフォーム タイプが原因で、一部またはすべてのアップリンクに対して有効な結果がありません。

API 応答セクションのパラメータ：

- `vlan_and_mtu_allowed`：互換性のある VLAN ID 範囲を返します。
- `mtu_disallowed`：MTU 値が物理スイッチと互換性がない VLAN ID 範囲を返します。
- `vlan_disallowed`：物理スイッチと互換性のある VLAN ID 範囲のリストを返します。

次のステップ

- オーバーレイベースのトランスポート ゾーンで、N-VDS のアップリンク プロファイルの VLAN ID と MTU の両方の設定を更新します。同様に、物理スイッチの VLAN または MTU を更新します。
- VLAN ベースのトランスポート ゾーンで、アップリンク プロファイルの MTU 設定を更新します。また、そのトランスポート ゾーンの論理スイッチの VLAN 構成を更新します。同様に、物理スイッチの VLAN または MTU を更新します。

双方向フォワーディング検出の状態の表示

トランスポート ノード間の双方向フォワーディング検出 (BFD) の状態を表示します。各トランスポート ノードは、トンネルの状態から別のリモート トランスポート ノードとの接続状態を検出します。トンネルの状態には、BFD の状態だけでなく、ノードに関連する他の詳細も含まれます。

ホスト トランスポート ノード（スタンドアローンと vCenter Server に登録されたホスト）と Edge ノードの両方で、トンネルの状態が表示されます。BFD パケットは、GENEVE と STT の両方のカプセル化をサポートします。デフォルトのカプセル化は GENEVE です。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] に移動します。
- 3 [トンネル] 列で、表示されているトンネル番号をクリックします。

[監視] 画面に、トンネルの状態、BFD 診断コード、リモート ノードの UUID、BFD パケットのカプセル化、トンネル名が表示されます。

トンネルの BFD 診断コードは、セッション状態が変更された理由を表します。

コード	説明
0	診断なし
1	コントロール検出期間が終了しました
2	エコ機能に失敗しました
3	ネイバーがセッション ダウンを通知しました
4	転送プレーンがリセットされました
5	バスがダウンしました
6	連結バスがダウンしました
7	管理設定によりダウンしました
8	リバース連結バスがダウンしました

結果

BFD の状態が「停止」の場合は、診断コードを確認して、トランスポート ノード間の接続を確立します。

NSX-T Data Center カーネル モジュールの手動インストール

NSX-T Data Center の [ファブリック] > [ノード] > [ホスト] > [追加] ユーザー インターフェイスまたは `POST /api/v1/fabric/nodes` API を使用する方法以外にも、NSX-T Data Center カーネル モジュールはハイパーバイザーのコマンドラインから手動でインストールすることもできます。

注： ベアメタル サーバ上で NSX-T Data Center カーネル モジュールを手動でインストールすることはできません。

ESXi ハイパーバイザーへの NSX-T Data Center カーネル モジュールの手動インストール

ホストを NSX-T Data Center に追加するには、NSX-T Data Center カーネル モジュールを ESXi ホストにインストールする必要があります。インストールすると、NSX-T Data Center の制御プレーンと管理プレーン ファブリックを構築できます。VIB ファイルにパッケージされた NSX-T Data Center 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、ブリッジ機能などのサービスを提供します。

NSX-T Data Center の VIB を手動でダウンロードし、ホスト イメージに加えることができます。NSX-T Data Center の各リリースによって、ダウンロード バスが変わる場合があります。必ず NSX-T Data Center のダウンロード ページを確認し、適切な VIB を入手してください。

手順

- 1 root または管理者権限を持つユーザーでホストにログインします。

2 /tmp ディレクトリに移動します。

```
[root@host:~]: cd /tmp
```

3 nsx-lcp ファイルをダウンロードし、/tmp ディレクトリにコピーします。

4 インストール コマンドを実行します。

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: VMware_bootbank_nsx-aggsservice_<release>, VMware_bootbank_nsx-
da_<release>, VMware_bootbank_nsx-esx-datapath_<release>, VMware_bootbank_nsx-
exporter_<release>, VMware_bootbank_nsx-host_<release>, VMware_bootbank_nsx-
lldp_<release>, VMware_bootbank_nsx-mpa_<release>, VMware_bootbank_nsx-netcpa_<release>,
VMware_bootbank_nsx-python-protobuf_<release>, VMware_bootbank_nsx-sfhc_<release>,
VMware_bootbank_nsxa_<release>, VMware_bootbank_nsxcli_<release>
  VIBs Removed:
  VIBs Skipped:
```

ホストにインストール済みの要素に応じて、インストールされる VIB、削除される VIB、省略される VIB があります。コマンド出力に「Reboot Required: true」と表示されない限り、再起動は必要ありません。

結果

ESXi ホストが NSX-T Data Center ファブリックに追加されると、次の VIB がホストにインストールされます。

nsx-adf

(自動診断フレームワーク) パフォーマンス データを収集して分析し、ローカル (ホスト) と中央 (データセンター) の両方のパフォーマンス問題を診断します。

nsx-aggsservice

NSX-T Data Center 集約サービスのホスト側ライブラリを提供します。NSX-T Data Center アグリゲーション サービスは、管理プレーン ノードで実行され、NSX-T Data Center コンポーネントからランタイム状態を取得するサービスです。

nsx-cli-libs

ハイパーバイザー ホストで NSX-T Data Center CLI を提供します。

nsx-common-libs

AES、SHA-1、UUID、ビットマップなど、一部のユーティリティ クラスを提供します。

nsx-context-mux

NSX ゲスト イントロスペクション リレー機能を提供します。VMware Tools ゲスト エージェントが、内部または登録済みのサードパーティ パートナーのアプライアンスにゲスト コンテキストをリレーできるようになります。

nsx-esx-datapath

NSX-T Data Center データ プレーン パケットの処理機能を提供します。

nsx-exporter

管理プレーンで実行されている集約サービスにランタイム状態をレポートするホスト エージェントを提供します。

nsx-host

ホストにインストールされている VIB バンドルにメタデータを提供します。

nsx-metrics-libs

デーモン メトリックを収集するメトリック ユーティリティ クラスを提供します。

nsx-mpa

NSX Manager とハイパーバイザー ホストの間の通信を提供します。

nsx-nestdb-libs

NestDB は、ホストに関連する NSX 構成（望ましい状態/ランタイムの状態など）を格納するデータベースです。

nsx-netcpa

中央の制御プレーンとハイパーバイザーの間の通信を提供します。中央の制御プレーンから論理ネットワークの状態を受け取り、この状態をデータ プレーンにプログラミングします。

nsx-opsagent

トランスポート ノードの認識、Link Layer Discovery Protocol (LLDP)、トレースフロー、パケット キャプチャなどの操作エージェントと管理プレーンの通信を提供します。

nsx-platform-client

セントラル CLI と監査ログの収集用に共通の CLI 実行エージェントを提供します。

nsx-profiling-libs

デーモン プロセスのプロファイリングに使用される gpeftool に基づいてプロファイリング機能を提供します。

nsx-proxy

中央の制御プレーンや管理プレーンと通信する唯一の North バウンド コンタクト ポイント エージェントを提供します。

nsx-python-gevent

Python Gevent が含まれています。

nsx-python-greenlet

Python Greenlet ライブラリ（サードパーティ製ライブラリ）が含まれています。

nsx-python-logging

Python ログが含まれています。

nsx-python-protobuf

プロトコル バッファの Python バインドを提供します。

nsx-rpc-libs

このライブラリは、nsx-rpc 機能を提供します。

nsx-sfhc

サービス ファブリック ホスト コンポーネント (SFHC) です。管理プレーンのインベントリでハイパーバイザーのライフサイクルをファブリック ホストとして管理するホスト エージェントを提供します。ハイパーバイザーにおける NSX-T Data Center のアップグレードやアンインストール、NSX-T Data Center モジュールの監視などの操作のチャネルとなります。

nsx-shared-libs

共有 NSX ライブラリが含まれています。

nsx-upm-libs

クライアント側の構成をフラット化し、重複データの転送を回避する統合プロファイル管理機能を提供します。

nsx-vdpi

NSX-T Data Center 分散ファイアウォールの Deep Packet Inspection 機能を提供します。

nsxcli

ハイパーバイザー ホストに NSX-T Data Center CLI を提供します。

vsipfwlib

分散ファイアウォール機能を提供します。

検証するには、ESXi ホストで `esxcli software vib list | grep nsx` コマンドと `esxcli software vib list | grep vsipfwlib` コマンドを実行します。または、`esxcli software vib list | grep <yyyy-mm-dd>` コマンドを実行します。この場合、インストールを実行した日が日付になります。

次のステップ

NSX-T Data Center の管理プレーンにホストを追加します。[クラスタを構成する NSX Manager ノードを CLI を使用して展開](#) を参照してください。

Ubuntu KVM ハイパーバイザーへの NSX-T Data Center ソフトウェア パッケージの手動インストール

ホストを NSX-T Data Center に追加するときに、NSX-T Data Center カーネル モジュールを Ubuntu KVM ホストに手動でインストールできます。インストールすると、NSX-T Data Center の制御プレーンと管理プレーン

ファブリックを構築できます。DEB ファイルにパッケージされた NSX-T Data Center 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、ブリッジ機能などのサービスを提供します。

NSX-T Data Center の DEB を手動でダウンロードし、ホスト イメージに加えることができます。ダウンロードパスは NSX-T Data Center 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 NSX-T Data Center のダウンロード ページを確認し、適切な DEB を入手してください。

前提条件

- 必要なサードパーティ製パッケージがインストールされていることを確認します。[KVM ホストへのサードパーティ製パッケージのインストール](#) を参照してください。

手順

- 1 管理者権限を持つユーザーでホストにログインします。
- 2 (オプション) /tmp ディレクトリに移動します。

```
cd /tmp
```

- 3 nsx-lcp ファイルをダウンロードし、/tmp ディレクトリにコピーします。
- 4 パッケージを解凍します。

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty_amd64.tar.gz
```

- 5 パッケージ ディレクトリに移動します。

```
cd nsx-lcp-trusty_amd64/
```

- 6 パッケージをインストールします。

```
sudo dpkg -i *.deb
```

- 7 OVS カーネル モジュールを再読み込みします。

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

ハイパーバイザーが OVS インターフェイスで DHCP を使用している場合は、DHCP が構成されているネットワーク インターフェイスを再起動します。ネットワーク インターフェイス上で古い dhclient プロセスを手動で停止し、そのインターフェイスで新しい dhclient プロセスを再開できます。

- 8 確認するには、`dpkg -l | egrep 'nsx|openvswitch'` コマンドを実行します。

コマンドで出力されるインストールされたパッケージは、nsx-lcp-trusty_amd64 ディレクトリ内のパッケージと一致する必要があります。

発生するほとんどのエラーは不完全な依存関係が原因です。apt-get install -f コマンドは、依存関係を解決し、NSX-T Data Center のインストールを再実行しようとします。

次のステップ

NSX-T Data Center の管理プレーンにホストを追加します。[クラスタを構成する NSX Manager ノードを CLI を使用して展開](#) を参照してください。

RHEL および CentOS KVM ハイパーバイザーへの NSX-T Data Center ソフトウェア パッケージの手動インストール

ホストを NSX-T Data Center に追加する準備を行う際に、NSX-T Data Center カーネル モジュールを RHEL または CentOS KVM ホストに手動でインストールできます。

インストールすると、NSX-T Data Center の制御プレーンと管理プレーン ファブリックを構築できます。RPM ファイルにパッケージされた NSX-T Data Center 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、ブリッジ機能などのサービスを提供します。

NSX-T Data Center の RPM を手動でダウンロードし、ホスト イメージに加えることができます。ダウンロードパスは NSX-T Data Center 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 NSX-T Data Center のダウンロード ページを確認し、適切な RPM を入手してください。

前提条件

RHEL または CentOS リポジトリにアクセスできること。

手順

- 1 管理者としてホストにログインします。
- 2 nsx-lcp ファイルをダウンロードし、/tmp ディレクトリにコピーします。
- 3 パッケージを解凍します。

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

- 4 パッケージ ディレクトリに移動します。

```
cd nsx-lcp-rhel74_x86_64/
```

- 5 パッケージをインストールします。

```
sudo yum install *.rpm
```

yum インストール コマンドを実行すると、すべての NSX-T Data Center 依存関係が解決されます。ただし、RHEL または CentOS ホストからそれぞれのリポジトリにアクセスできることを前提とします。

- 6 OVS カーネル モジュールを再読み込みします。

```
/usr/share/openvswitch/scripts/ovs-systemd-reload force-reload-kmod
```

ハイパーバイザーが OVS インターフェイスで DHCP を使用している場合は、DHCP が構成されているネットワーク インターフェイスを再起動します。ネットワーク インターフェイス上で古い dhclient プロセスを手動で停止し、そのインターフェイスで新しい dhclient プロセスを再開できます。

- 7 確認するには、`rpm -qa | egrep 'nsx|openvswitch'` コマンドを実行します。

出力に表示されるインストールされたパッケージは、`nsx-rhel74` または `nsx-centos74` ディレクトリ内のパッケージと一致する必要があります。

次のステップ

NSX-T Data Center の管理プレーンにホストを追加します。[クラスタを構成する NSX Manager ノードを CLI を使用して展開](#) を参照してください。

SUSE KVM ハイパーバイザーへの NSX-T Data Center ソフトウェア パッケージの手動インストール

NSX-T Data Center に追加するホストを準備するときに、NSX-T Data Center カーネル モジュールを SUSE KVM ホストに手動でインストールできます。

インストールすると、NSX-T Data Center の制御プレーンと管理プレーン ファブリックを構築できます。RPM ファイルにパッケージされた NSX-T Data Center 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、ブリッジ機能などのサービスを提供します。

NSX-T Data Center の RPM を手動でダウンロードし、ホスト イメージに加えることができます。ダウンロードパスは NSX-T Data Center 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 NSX-T Data Center のダウンロード ページを確認し、適切な RPM を入手してください。

前提条件

SUSE リポジトリにアクセスできること。

手順

- 1 管理者としてホストにログインします。
- 2 `nsx-lcp` ファイルをダウンロードし、`/tmp` ディレクトリにコピーします。
- 3 パッケージを解凍します。

```
tar -zxvf nsx-lcp-3.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- 4 パッケージ ディレクトリに移動します。

```
cd nsx-lcp-linux64-sles12sp3
```

- 5 パッケージをインストールします。

```
sudo zypper --no-gpg-checks install -y *.rpm
```

`zypper` インストール コマンドを実行すると、すべての NSX-T Data Center 依存関係が解決されます。ただし、SUSE ホストからそれぞれのリポジトリにアクセスできることを前提とします。

- 6 OVS カーネル モジュールを再読み込みします。

```
/usr/share/openvswitch/scripts/ovs-systemd-reload force-reload-kmod
```

ハイパーバイザーが OVS インターフェイスで DHCP を使用している場合は、DHCP が構成されているネットワーク インターフェイスを再起動します。ネットワーク インターフェイス上で古い dhclient プロセスを手動で停止し、そのインターフェイスで新しい dhclient プロセスを再開できます。

- 7 確認するには、`zypper packages --installed-only | grep System | egrep 'openvswitch|nsx'` コマンドを実行します。

コマンドで表示されるインストールされたパッケージは、`nsx-lcp-linux64-sles12sp3` ディレクトリ内のパッケージと一致する必要があります。

次のステップ

NSX-T Data Center の管理プレーンにホストを追加します。[クラスタを構成する NSX Manager ノードを CLI を使用して展開](#) を参照してください。

最小の vSphere クラスタ NSX-T の展開

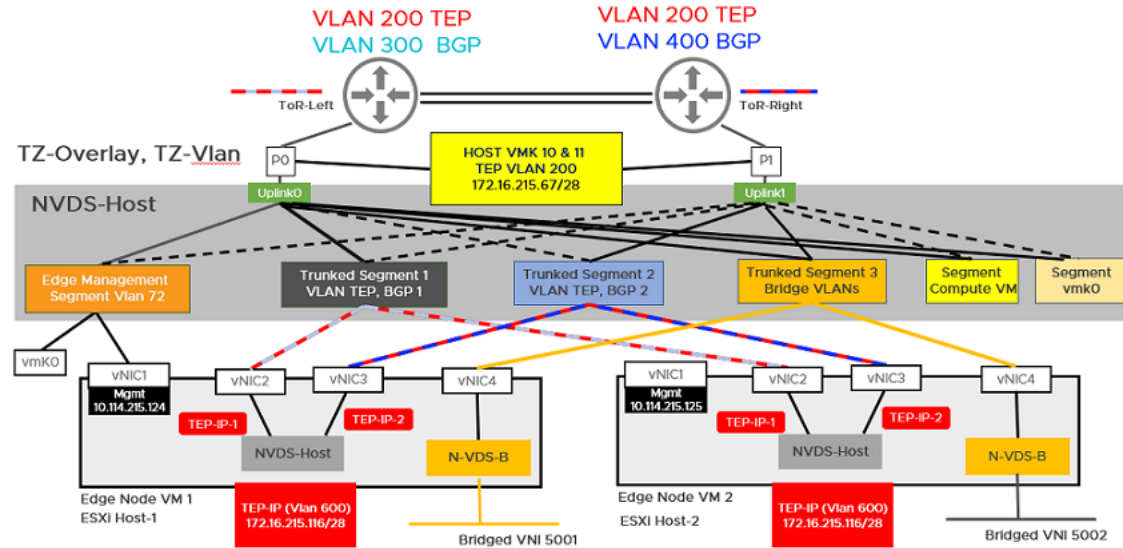
1 つのクラスタに NSX Manager、ホスト トランスポート ノード、NSX Edge 仮想マシンを設定できます。クラスタ内の各ホストには、NSX-T 用に設定された 2 つの物理 NIC があります。

重要： NSX-T 2.4.2 または 2.5 リリース以降では、最小の単一 vSphere クラスタ トポロジを展開してください。

この手順で説明するトポロジでは、次のものを使用します。

- クラスタ内のホストに設定された vSAN
- ホストごとに 2 個以上の物理 NIC
- vMotion と管理 VMkernel インターフェイス

図 10-4. トポロジ：NSX Edge またはゲスト仮想マシンとのホスト通信を管理する単一 N-VDS スイッチ

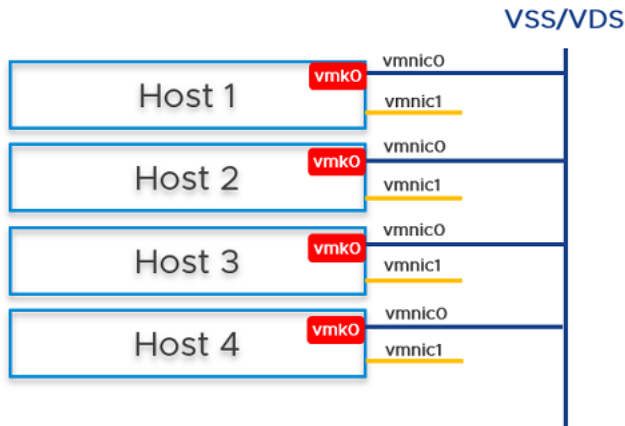


前提条件

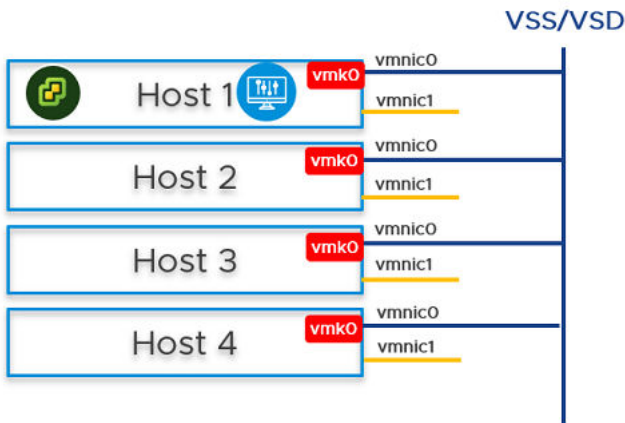
- すべてのホストが 1 つの vSphere クラスタを構成している必要があります。
- 各ホストでは、2 つの物理 NIC が有効になっている必要があります。
- すべてのホストを vCenter Server に登録します。
- 共有ストレージがホストで使用可能であることを vCenter Server で確認します。
- ホスト TEP の IP と NSX Edge TEP の IP は別の VLAN にある必要があります。ホストのワークロードからの North-South トラフィックは GENEVE でカプセル化され、送信元 IP がホスト TEP、宛先 IP が NSX Edge TEP の NSX Edge ノードに送信されます。これらの TEP は別の VLAN またはサブネットに配置する必要があるため、このトラフィックはトップオブラック (TOR) スイッチ経由でルーティングされる必要があります。ホストのトランスポート VLAN は VLAN 200 で、NSX Edge のトランスポート VLAN は VLAN 600 です。

手順

- 1 vSS または vDS 上の vmnic0 で 4 台の ESXi ホストを準備します。vmnic1 は解放します。



- 2 ホスト 1 で、vCenter Server をインストールし、VSS/VDS ポート グループを設定して、ホスト上で作成されたポート グループに NSX Manager をインストールします。

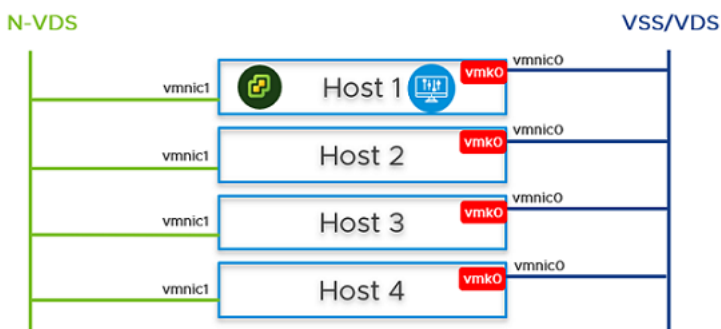


- 3 トランSPORT ノードとして ESXi ホスト 1、2、3、4 を準備します。
 - a 名前付きのチーミング ポリシーを使用して、VLAN トランSPORT ゾーンとオーバーレイ トランSPORT ゾーンを作成します。[トランSPORT ゾーンの作成](#) を参照してください。
 - b ホストのトンネル エンドポイント IP アドレス用の IP アドレス プールまたは DHCP を作成します。[トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成](#) を参照してください。
 - c Edge ノードのトンネル エンドポイント IP アドレス用の IP アドレス プールまたは DHCP を作成します。[トンネル エンドポイントの IP アドレス用 IP アドレス プールの作成](#) を参照してください。
 - d 名前付きチーミング ポリシーを使用してアップリンク プロファイルを作成します。[アップリンク プロファイルの作成](#) を参照してください。

- e トランスポート ノード プロファイルを適用して、トランスポート ノードとしてホストを設定します。この手順では、トランスポート ノード プロファイルで vmnic1（未使用の物理 NIC）のみを N-VDS スイッチに移行します。トランスポート ノード プロファイルがクラスタ ホストに適用されると、N-VDS スイッチが作成され、vmnic1 が N-VDS スイッチに接続します。[トランスポート ノード プロファイルの追加](#) を参照してください。

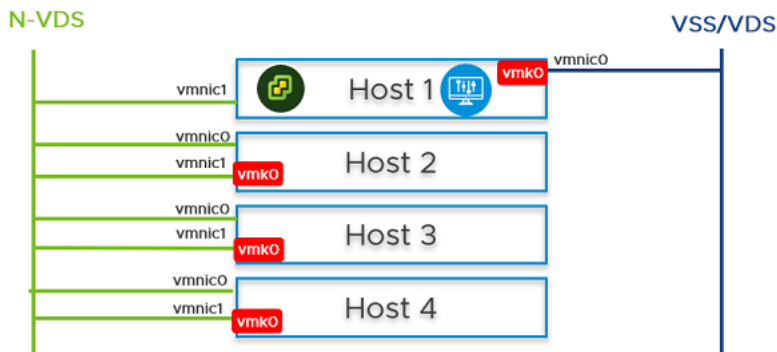
トランスポート ノード プロファイルの編集： T... [?](#)

N-VDS 名 *	vds-1	▼
関連付けられたトランスポート ゾーン	tz	
NIOC プロファイル *	nsx-default-nioc-hostswitch-profile	▼
NIOC プロファイルの新規作成		
アップリンク プロファイル *	hostnodeprofile	▼
アップリンク プロファイルの新規作成		
LLDP プロファイル *	LLDP [Send Packet Enabled]	▼
IP の割り当て *	IP プールを使用	▼
IP プール *	ippoolhostnode	▼
新規 IP プールの作成と使用		
物理 NIC	vmnic1	activeuplinkhost ▼
物理 NIC の追加		
物理 NIC のみの移行	<input checked="" type="checkbox"/> はい	
移行対象に選択した物理 NIC に vmk が存在しない場合は、このオプションを有効にします		
インストール用のネットワーク マッピング	マッピングの追加	
アンインストール用のネットワーク マッピング	マッピングの追加	

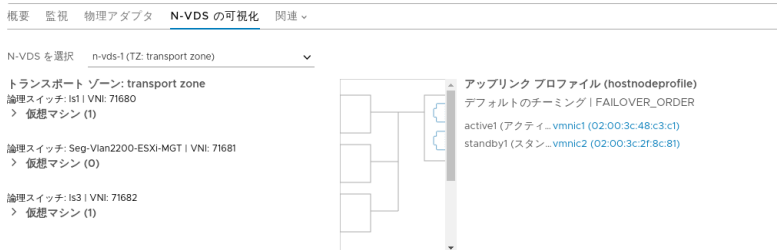


すべてのホストの vmnic1 が N-VDS スイッチに追加されます。そのため、2 つの物理 NIC のいずれかが N-VDS スイッチに移行されます。vmnic0 インターフェイスは、引き続き VSS または VDS スイッチに接続し、これにより、ホストとの接続が可能になります。

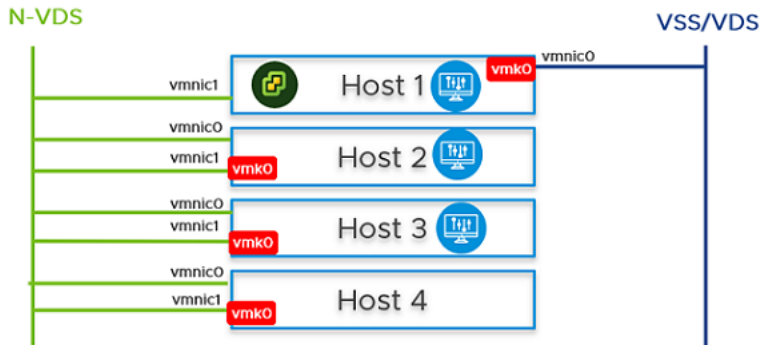
- 4 NSX Manager UI で、NSX Manager、vCenter Server、NSX Edge に VLAN でバックアップされたセグメントを作成します。VLAN でバックアップされた各セグメントに対して、正しいチーミング ポリシーを選択します。ターゲットとして VLAN トランク論理スイッチを使用しないでください。NSX Manager UI でターゲット セグメントを作成する場合は、[VLAN のリストの入力] フィールドに VLAN の値を 1 つだけ入力します。
- 5 ホスト 2、ホスト 3、ホスト 4 で、vmk0 アダプタと vmnic0 を VSS/VDS から N-VDS スイッチに移行する必要があります。各ホストで NSX-T の構成を更新します。移行中に次のことを確認します。
 - vmk0 が [Edge 管理セグメント] にマッピングされている。
 - vmnic0 がアクティブなアップリンク [uplink-1] にマッピングされている。



- 6 vCenter Server で、ホスト 2、ホスト 3、ホスト 4 に移動し、vmk0 アダプタが N-VDS の vmnic0 物理 NIC に接続し、到達可能であることを確認します。
- 7 NSX Manager UI で、ホスト 2、ホスト 3、ホスト 4 に移動し、両方の物理 NIC が N-VDS スイッチに接続していることを確認します。

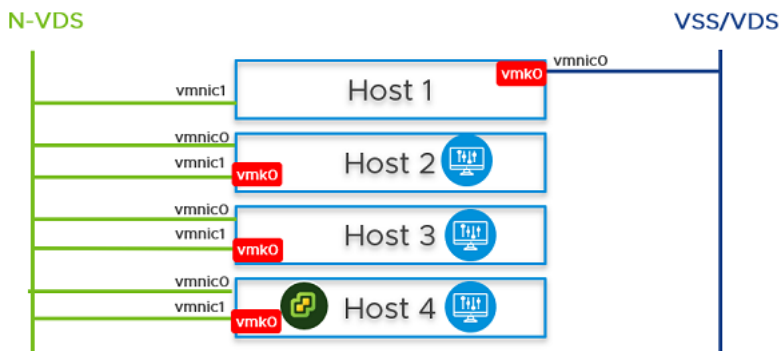


- 8 ホスト 2 とホスト 3 の NSX Manager UI で、NSX Manager をインストールして、NSX Manager をセグメントに接続します。クラスタが作成されるまで 10 分ほどかかります。約 10 分後に、クラスタが作成されていることを確認します。



- 9 最初の NSX Manager ノードをパワーオフします。10 分ほど待ちます。
- 10 以前に作成した論理スイッチに NSX Manager と vCenter Server を再接続します。ホスト 4 で、NSX Manager をパワーオンします。10 分ほど経過したら、クラスタの状態が安定していることを確認します。最初の NSX Manager がパワーオフ状態でコールド vMotion を実行し、ホスト 1 からホスト 4 に NSX Manager と vCenter Server を移行します。

vMotion の制限については、<https://kb.vmware.com/s/article/56991> を参照してください。



- 11 NSX Manager UI から、ホスト 1 に移動し、vmk0 と vmnic0 を VSS から N-VDS スイッチに移行します。

- 12 [インストールのネットワーク マッピング] フィールドで、vmk0 アダプタが N-VDS スイッチの [Edge 管理セグメント] にマッピングされていることを確認します。

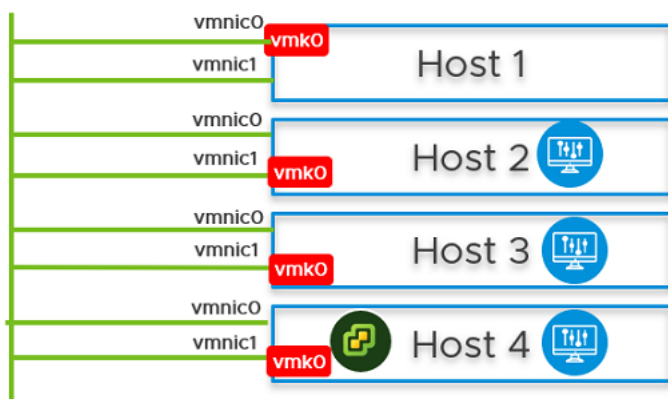
The screenshot shows the 'NSX の設定' (NSX Settings) window. On the left, a sidebar lists '1 ホストの詳細' (Host Details) and '2 NSX の設定' (NSX Settings), with the latter selected. The main panel displays the following configuration:

- IP の割り当て ***: 固定 IP のリストを使用 (Use fixed IP list)
- 固定 IP リスト ***: 172.16.228.36
- ゲートウェイ ***: 172.16.228.33
- サブネット マスク ***: 255.255.255.240
- 物理 NIC**:

vmnic1	uplink-1	[trash icon]
vmnic2	uplink-2	[trash icon]
- 物理 NIC のみの移行**: ☐ いいえ (Move only physical NICs: No)
- 移行対象に選択した物理 NIC に vmk が存在しない場合は、このオプションを有効にします (If the selected physical NIC does not contain a vmk, enable this option).
- インストール用のネットワーク マッピング**: [マッピングの追加](#) (Network mapping for installation: Add mapping)
- アンインストール用のネットワーク マッピング**: [マッピングの追加](#) (Network mapping for uninstallation: Add mapping)

At the bottom right, there are three buttons: 'キャンセル' (Cancel), '前へ' (Previous), and '終了' (Finish).

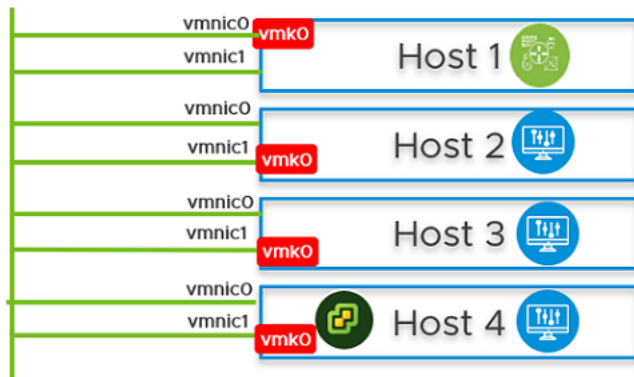
N-VDS



- 13 ホスト 1 で、NSX Manager ユーザー インターフェイスを使用して NSX Edge 仮想マシンをインストールします。

[NSX Edge トランスポート ノードの作成](#) を参照してください。

N-VDS



- 14 管理プレーンに NSX Edge 仮想マシンを追加します。

NSX Edge の管理プレーンへの追加 を参照してください。

- 15 North-South トラフィックの接続を確立するには、外部ルーターを使用して NSX Edge 仮想マシンを構成します。
- 16 NSX Edge 仮想マシンと外部ルーター間の North-South トラフィック接続を確認します。
- 17 クラスタ全体が再起動される電源障害が発生した場合、NSX-T 管理コンポーネントが起動しないために N-VDS と通信できなくなることがあります。このシナリオを回避するには、次の手順に従います。

注意： API コマンドが正しく実行されないと、NSX Manager との接続が失われます。

注： 単一クラスタ構成では、管理コンポーネントは N-VDS スイッチ上で仮想マシンとしてホストされます。セキュリティ上の理由から、管理コンポーネントがデフォルトで接続する N-VDS ポートはブロックポートとして初期化されます。4 台のホストすべてで再起動が必要になる電源障害が発生すると、管理仮想マシンのポートがブロック状態で初期化されます。このような循環依存を回避するため、N-VDS で非ブロック状態のポートを作成することをおすすめします。非ブロック状態のポートを作成することで、クラスタの再起動時に NSX-T 管理コンポーネントが N-VDS に接続し、通常の機能を再開できるようになります。

サブタスクが終了すると、移行コマンドは以下を使用します。

- NSX Manager が存在するホスト ノードの UUID。
- NSX Manager 仮想マシンの UUID。これは非ブロック状態にある固定論理ポートに移行されます。

すべてのホストがパワーオフ状態またはパワーオン状態の場合、または NSX Manager 仮想マシンが別のホストに移動した場合、NSX Manager が起動時に非ブロック状態のポートに接続できるため、NSX-T の管理コンポーネントとの接続を維持できます。

- a NSX Manager UI で、[ネットワークとセキュリティの詳細設定] タブに移動します (2.5.1 以前のリリース)。[セグメント コンピューティング仮想マシン] セグメントを検索します。[概要] タブで、UUID を検索してコピーします。この例で使用する UUID は、`c3fd8e1b-5b89-478e-abb5-d55603f04452` です。
- b 各 NSX Manager の JSON ペイロードを作成します。
 - JSON ペイロードで、`logical_switch_id` の値を以前に作成した [Edge 管理セグメント] の UUID で置き換えて、**UNBLOCKED_VLAN** 状態の論理ポートを作成します。
 - 各 NSX Manager のペイロードで、`attachment_type_id` と `display_name` の値は異なります。

重要： この手順を繰り返して、合計で 4 つの JSON ファイルを作成します。3 つは NSX Manager 用、1 つは vCenter Server Appliance (VCSA) 用です。

```
port1.json
{
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "VIF",
    "id": "nsxmgr-port-147"
  },
  "display_name": "NSX Manager Node 147 Port",
  "init_state": "UNBLOCKED_VLAN",
  "logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

説明：

- `admin_state`：ポートの状態。「稼動中」になっている必要があります。
- `attachment_type`：VIF に設定する必要があります。すべての仮想マシンが、VIF ID を使用して NSX-T スイッチポートに接続されます。
- `id`：VIF ID。NSX Manager ごとに一意である必要があります。3 つの NSX Manager がある場合、3 つのペイロードがあり、それぞれに異なる VIF ID が設定されている必要があります。一意の UUID を生成するには、NSX Manager のルート シェルにログインし、`/usr/bin/uuidgen` を実行して一意の UUID を生成します。
- `display_name`：NSX 管理者が他の NSX Manager 表示名と区別できるように、一意の名前にする必要があります。
- `init_state`：値が `UNBLOCKED_VLAN` に設定すると、NSX Manager が使用できない場合でも、NSX は NSX Manager のポートのブロックを解除します。
- `logical_switch_id`：[Edge 管理セグメント] の論理スイッチ ID。

- c 3つの NSX Manager が展開されている場合、NSX Manager の各論理ポートに1つのペイロードを作成する必要があります（合計で3つ作成します）。たとえば、port1.json、port2.json、port3.json のように作成します。

次のコマンドを実行して、ペイロードを作成します。

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json'
-d @port1.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json'
-d @port2.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json'
-d @port3.json https://nsxmgr/api/v1/logical-ports
```

論理ポートを作成する API 実行の例。

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
```

```
"_last_modified_user" : "admin",
"_last_modified_time" : 1574716624192,
"_system_owned" : false,
"_protection" : "NOT_PROTECTED",
"_revision" : 0
```

- d 論理ポートが作成されていることを確認します。

スイッチ ポート スイッチング プロファイル

+ 追加 編集 削除 アクション							検索
<input type="checkbox"/>	論理ポート ↑	ID	管理状態	運用状態	スイッチング プロファイル	接続	論理スイッチ
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	● 稼動中	● 稼動中	nsx-default-switch-security-non...	論理ルーター: 80fb...2662	ls3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	● 稼動中	● 稼動中	nsx-default-switch-security-non...	論理ルーター: 42ac...ad24	ls1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...alcb	● 稼動中	● 停止	nsx-default-switch-security-vif...	仮想マシン: nsx-mgr-147	ls1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	仮想マシン: vm1	ls1
<input type="checkbox"/>	vmknic@n-vds-1@94b323e6-1ee...	2021...4d76	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	VIF: abf2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	仮想マシン: vm3	ls3

- e 各 NSX Manager の仮想マシン インスタンス ID を確認します。インスタンス ID を取得するには、[インベントリ] > [仮想マシン] の順に移動して NSX Manager 仮想マシンを選択し、[概要] タブを選択してインスタンス ID をコピーします。または、vCenter Server の管理対象オブジェクト ブラウザ (MOB) でインスタンス ID を検索します。ID に **:4000** を追加して、NSX Manager 仮想マシンの vNIC ハードウェア インデックスを取得します。

たとえば、仮想マシンのインスタンス UUID が 503c9e2b-0abf-a91c-319c-1d2487245c08 の場合、vNIC インデックスは 503c9e2b-0abf-a91c-319c-1d2487245c08:4000 になります。3 つの NSX Manager の vNIC インデックスは次のとおりです。

```
mgr1 vnic: 503c9e2b-0abf-a91c-319c-1d2487245c08:4000
```

```
mgr2 vnic: 503c76d4-3f7f-ed5e-2878-cffc24df5a88:4000
```

```
mgr3 vnic: 503cafd5-692e-d054-6463-230662590758:4000
```

- f NSX Manager をホストするトランスポート ノード ID を確認します。3 つの NSX Manager があり、それぞれが異なるトランスポート ノードでホストされている場合は、トランスポート ノード ID をメモします。たとえば、3 つのトランスポート ノード ID は次のとおりです。

```
tn1: 12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea
```

```
tn2: 4b6e182e-0ee3-403f-926a-fb7c8408a9b7
```

```
tn3: d7cec2c9-b776-4829-beea-1258d8b8d59b
```

- g 新しく作成されたポートに NSX Manager を移行するときに、ペイロードとして使用されるトランスポート ノードの設定を取得します。

次はその例です。

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea > tn1.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/4b6e182e-0ee3-403f-926a-fb7c8408a9b7 > tn2.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/d7cec2c9-b776-4829-beea-1258d8b8d59b > tn3.json
```

- h 以前のポートから [Edge 管理セグメント] に新たに作成され、ブロック解除された論理ポートに NSX Manager を移行します。VIF-ID 値は、NSX Manager に以前に作成したポートの接続 ID です。

NSX Manager を移行するには、次のパラメータが必要です。

- トランスポート ノード ID
- トランスポート ノードの設定
- NSX Manager vNIC ハードウェア インデックス
- NSX Manager VIF ID

新しく作成され、ブロック解除されたポートに NSX Manager を移行する API コマンドは次のとおりです。

```
/api/v1/transport-nodes/<TN-ID>?vnic=<VNIC-ID>&vif=<VIF-ID>
```

次はその例です。

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'admin:VMware1!VMware1!' -H 'Content-Type:application/json' -d @mgr.json 'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?vnic=5028d756-d36f-719e-3db5-7ae24aa1d6f3:4000&vif=nsxmgr-port-147'
```

- i 静的に作成された論理ポートが Up 状態になっていることを確認します。

スイッチ ポート スイッチング プロファイル							
<div> + 追加 編集 削除 アクション </div> <div> <div>検索</div> </div>							
<input type="checkbox"/>	論理ポート ↑	ID	管理状態	運用状態	スイッチング プロファイル	接続	論理スイッチ
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	● 稼動中	● 稼動中	nsx-default-switch-security-non...	論理ルーター: 80fb...2662	Is3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	● 稼動中	● 稼動中	nsx-default-switch-security-non...	論理ルーター: 42ac...ad24	Is1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	仮想マシン: nsx-mgr-147	Is1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	仮想マシン: vm1	Is1
<input type="checkbox"/>	vmnic@n-vds-1@94b323e6-1ee...	2021...4d76	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	VIF: abf2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	● 稼動中	● 稼動中	nsx-default-switch-security-vif...	仮想マシン: vm3	Is3

- j クラスタ内のすべての NSX Manager で上記の手順を繰り返します。

NSX-T とホスト プロファイルの統合

11

ESXi ホストから抽出したホスト プロファイルを NSX-T と統合し、ステートフル サーバとステートレス サーバに ESXi と NSX-T の VIB を展開します。

この章には、次のトピックが含まれています。

- [Auto Deploy ステートレス クラスタ](#)
- [ステートフル サーバ](#)

Auto Deploy ステートレス クラスタ

ステートレス ホストは設定を維持しません。このため、Auto Deploy サーバを用意して、ホストのパワーオン時に使用する起動ファイルを提供する必要があります。

このセクションでは、vSphere Auto Deploy と NSX-T トランスポート ノード プロファイルを使用してステートレス クラスタを設定し、異なるバージョンの ESXi と NSX-T を含む新しいイメージ プロファイルでホストを再プロビジョニングする方法について説明します。vSphere Auto Deploy 用に設定されたホストは、Auto Deploy サーバと vSphere ホスト プロファイルを使用してホストをカスタマイズします。これらのホストを NSX-T トランスポート ノード プロファイル用に設定し、ホストで NSX-T を構成することもできます。

ステートレス ホストを vSphere Auto Deploy と NSX-T トランスポート ノード プロファイルに設定して、カスタム ESXi と NSX-T バージョンのホストを再プロビジョニングできます。

ステートレス クラスタの Auto Deploy タスクの概要

ステートレス クラスタの Auto Deploy タスクの概要

Auto Deploy ステートレス クラスタの設定手順の概要は次のとおりです。

- 1 前提条件とサポートされるバージョン。 [前提条件とサポートされるバージョン](#) を参照してください。
- 2 (リファレンス ホスト) カスタム イメージ プロファイルを作成します。 [ステートレス ホスト用のカスタム イメージ プロファイルの作成](#) を参照してください。
- 3 (リファレンス ホストとターゲット ホスト) カスタム イメージ プロファイルを関連付けます。 [リファレンス ホストまたはターゲット ホストとカスタム イメージの関連付け](#) を参照してください。
- 4 (リファレンス ホスト) ESXi でネットワーク構成を行います。 [リファレンス ホストでのネットワークの構成](#) を参照してください。

- 5 (リファレンス ホスト) NSX でトランスポート ノードとしてを構成します。[NSX-T でのトランスポート ノードとしてのリファレンス ホストの設定](#) を参照してください。
- 6 (リファレンス ホスト) ホスト プロファイルを抽出して確認します。[ホスト プロファイルの抽出と確認](#) を参照してください。
- 7 (リファレンス ホストとターゲット ホスト) ステートレス クラスタとのホスト プロファイルの関連付けを確認します。[ステートレス クラスタとホスト プロファイルの関連付けの確認](#) を参照してください。
- 8 (リファレンス ホスト) ホストのカスタマイズを更新します。[ホストのカスタマイズの更新](#) を参照してください。
- 9 (ターゲット ホスト) 自動展開をトリガします。[ターゲット ホストでの自動展開のトリガ](#) を参照してください。
 - a トランスポート ノード プロファイルの適用前。[TNP 適用前のホストの再起動](#) を参照してください。
 - b トランスポート ノード プロファイルを適用します。[ステートレス クラスタへの TNP の適用](#) を参照してください。
 - c トランスポート ノード プロファイルの適用後。[TNP 適用後のホストの再起動](#) を参照してください。
- 10 ホスト プロファイルとトランスポート ノード プロファイルのトラブルシューティングを行います。[ホスト プロファイルとトランスポート ノード プロファイルのトラブルシューティング](#) を参照してください。

前提条件とサポートされるバージョン

前提条件、サポートされる ESXi と NSX-T のバージョンについて説明します。

サポートされるワークフロー

- イメージ プロファイルと HostProfile を使用

前提条件

- 同種のクラスタのみがサポートされます（クラスタ内のホストがすべてステートレスか、すべてステートフルである必要があります）。
- Image Builder サービスが有効になっている必要があります。
- Auto Deploy サービスを有効にする必要があります。

サポートされる NSX および ESXi のバージョン

サポートされる ESXi のバージョン	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 67ep15	ESXi 67ep17
NSX-T Data Center 2.4	○	○	×	×	×	×
NSX-T Data Center 2.4.1	○	○	×	×	×	×
NSX-T Data Center 2.4.2	○	○	×	×	×	×
NSX-T Data Center 2.4.3	○	○	×	×	×	×
NSX-T Data Center 2.5	○	○	○	○	×	×
NSX-T Data Center 2.5.1	○	○	○	○	○	○

ステートレス ホスト用のカスタム イメージ プロファイルの作成

データセンターで、リファレンス ホストとして準備するホストを特定します。

リファレンス ホストの最初の起動時に、ESXi はデフォルト ルールをリファレンス ホストに関連付けます。この手順で、カスタム イメージ プロファイル（ESXi と NSX VIB）を追加し、リファレンス ホストを新しいカスタム イメージに関連付けます。NSX-T イメージを含むイメージ プロファイルを使用することで、インストール時間が大幅に短縮されます。同じカスタム イメージがステートレス クラスタ内のターゲット ホストに関連付けられます。

注： リファレンスとターゲットのステートレス クラスタに、ESXi イメージ プロファイルのみを追加することもできます。ステートレス クラスタにトランスポート ノード プロファイルを適用すると、NSX-T VIB がダウンロードされます。[ソフトウェア デポの追加](#)を参照してください。

前提条件

Auto Deploy サービスと Image Builder サービスが有効になっていることを確認します。[vSphere Auto Deploy](#) を使用した、ホストの再プロビジョニングを参照してください。

手順

- 1 NSX-T パッケージをインポートするには、ソフトウェア デポを作成します。
- 2 nsx-lcp パッケージをダウンロードします。
 - a <https://my.vmware.com> にログインします。
 - b VMware NSX-T Data Center のダウンロード ページで、NSX-T のバージョンを選択します。
 - c 製品のダウンロード ページで、特定の VMware ESXi バージョンの NSX-T カーネル モジュールを検索します。
 - d [今すぐダウンロード] をクリックして、nsx-lcp パッケージのダウンロードを開始します。
 - e nsx-lcp パッケージをソフトウェア デポにインポートします。

NSX Kernel Module for VMware ESXi 6.7

ファイルサイズ: 37.64 MB

ファイルタイプ: zip

今すぐダウンロード

Name: nsx-lcp-2.5.0.0.14663975-esx67.zip

リリース日: 2019-09-19

ビルド番号: 14663974

NSX Kernel Module for VMware ESXi 6.7

This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxccli to install manually or include as part of an automated deployment system of the ESXi hosts.

MD5SUM: f224a0e12fc1722ae5b5259d279bfa1

SHA1SUM: a97d3125a26a47b94ec8408acd369d42681d3027

SHA256SUM:

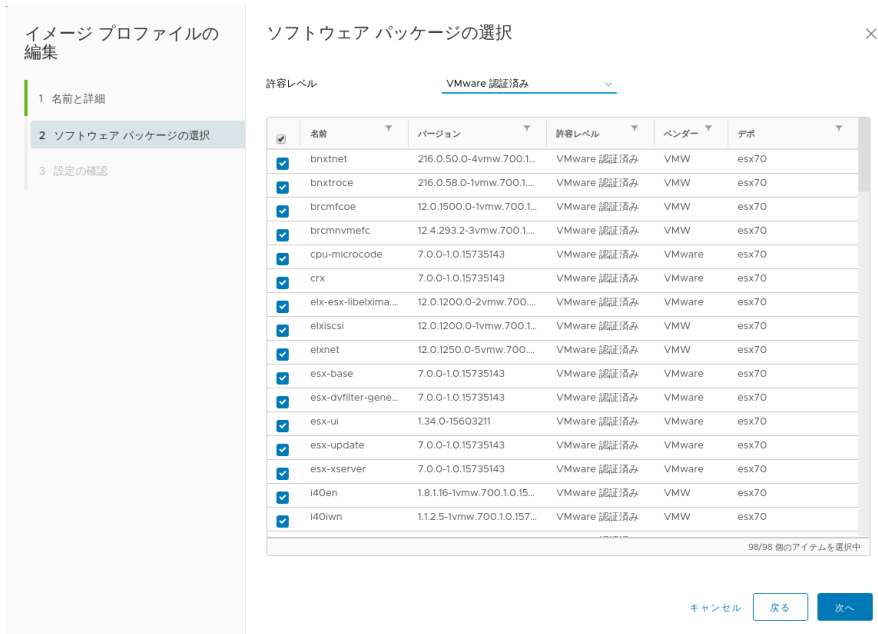
1ed76de6a7f22d227eb4be30a2e0aa91492a876b7b164814198de3

1eec77bc44

- 3 別のソフトウェア デポを作成し、ESXi パッケージをインポートします。

vSphere Web Client には、リファレンス ホストで作成された 2 つのデポが表示されます。

- 4 カスタム ソフトウェア デポを作成して、以前にインポートした ESXi イメージと nsx-lcp パッケージのクローンを作成します。
 - a 前の手順で作成した ESXi ソフトウェア デポから ESXi イメージ プロファイルを選択します。
 - b [クローン作成] をクリックします。
 - c [イメージ プロファイルのクローン作成] ウィザードで、作成するカスタム イメージの名前を入力します。
 - d クローン作成済みのイメージ (ESXi) を使用可能にするカスタム ソフトウェア デポを選択します。
 - e [ソフトウェア パッケージの選択] 画面で、[VMware 認定] の許容レベルを選択します。ESXi VIB が事前に選択されています。
 - f パッケージのリストから NSX-T パッケージを選択し、[次へ] をクリックします。
 - g [設定内容の確認] 画面で詳細を確認し、[終了] をクリックします。ESXi パッケージと NSX-T パッケージを含むクローン作成済みのイメージがカスタム ソフトウェア デポに作成されます。



次のステップ

リファレンス ホストとターゲット ホストをカスタム イメージに関連付けます。リファレンス ホストまたはターゲット ホストとカスタム イメージの関連付けを参照してください。

リファレンス ホストまたはターゲット ホストとカスタム イメージの関連付け

ESXi と NSX パッケージを含む新しいカスタム イメージを使用してリファレンス ホストとターゲット ホストを起動するには、カスタム イメージ プロファイルに関連付けます。

この時点では、カスタム イメージはリファレンス ホストとターゲット ホストに関連付けられますが、NSX のインストールまだ行われません。

重要： リファレンス ホストとターゲット ホストの両方で、このカスタム イメージの関連付けを行います。

前提条件

手順

- 1 ESXi ホストで、[メニュー] > [Auto Deploy] > [デプロイされたホスト] の順に移動します。
- 2 カスタム イメージ プロファイルをホストに関連付けるには、カスタム イメージを選択します。
- 3 [イメージ プロファイルの関連付けの編集] をクリックします。
- 4 [イメージ プロファイルの関連付けの編集] ウィザードで、[参照] をクリックし、カスタム デポを選択してカスタム イメージ プロファイルを選択します。
- 5 [イメージ プロファイルの署名チェックをスキップ] を有効にします。
- 6 [OK] をクリックします。



結果

次のステップ

リファレンス ホストでネットワーク構成を行います。[リファレンス ホストでのネットワークの構成](#) を参照してください。

リファレンス ホストでのネットワークの構成

ESXi でネットワークを構成するため、リファレンス ホストで VMkernel アダプタを含む標準スイッチが作成されます。

このネットワーク構成は、リファレンス ホストから抽出されたホスト プロファイルでキャプチャされます。ステートレス展開で、ホスト プロファイルはこのネットワーク構成を各ターゲット ホストに複製します。

手順

- 1 ESXi ホストで、VMkernel アダプタを追加して、vSphere 標準スイッチ (VSS) または分散仮想スイッチ (VDS) を構成します。

- 2 [VMkernel アダプタ] 画面に新しく追加された VSS/VDS スイッチが表示されていることを確認します。



次のステップ

リファレンス ホストを NSX-T のトランスポート ノードとして設定します。[NSX-T でのトランスポート ノードとしてのリファレンス ホストの設定](#) を参照してください。

NSX-T でのトランスポート ノードとしてのリファレンス ホストの設定

リファレンス ホストがカスタム イメージ プロファイルに関連付けられ、VSS スイッチで設定されたら、リファレンス ホストを NSX-T のトランスポート ノードとして設定します。

手順

- 1 ブラウザから NSX-T (https://<NSXManager_IPAddress>) にログインします。
- 2 リファレンス ホストを探すには、[システム] -> [ノード] -> [ホスト トランスポート ノード] の順に移動します。
- 3 VLAN トランスポート ゾーンを作成して、仮想ネットワークの範囲を定義します。この範囲は、N-VDS スイッチをトランスポート ゾーンに接続して定義されます。この接続に基づいて、N-VDS はトランスポート ゾーン内で定義されたセグメントにアクセスできます。[トランスポート ザーンの作成](#) を参照してください。
- 4 トランスポート ゾーンに VLAN セグメントを作成します。作成されたセグメントが論理スイッチとして表示されます。
 - a [ネットワーク] > [セグメント] の順に移動します。
 - b セグメントに接続するトランスポート ゾーンを選択します。
 - c VLAN ID を入力します。
 - d [保存] をクリックします。



- 5 N-VDS が物理ネットワークに接続する方法を定義するリファレンス ホストにアップリンク プロファイルを作成します。[アップリンク プロファイルの作成](#)を参照してください。

アップリンク プロファイル NIOC プロファイル Edge クラスター プロファイル Edge ブリッジ プロファイル 設定 トラnsポート ノード プロ

+ 追加 編集 削除 アクション

<input type="checkbox"/>	アップリンク プロファイル	ID	チーミングポリシー	アクティブアップリンク	スタンバイアップリンク	トラnsポート VLAN	MTU
<input checked="" type="checkbox"/>	Edgenodeprofile	d017...cf3b	フェイルオーバーの順序	activeuplinkedge		0	1600 (グローバル MTU)
<input type="checkbox"/>	hostnodeprofile	1219...46fb	フェイルオーバーの順序	activeuplinkhost	standbyuplink	0	1600 (グローバル MTU)

- 6 トラnsポート ノードとしてリファレンス ホストを設定します。[管理対象ホストのトラnsポート ノードの設定](#)を参照してください。
- [ホスト トラnsポート ノード] 画面で、リファレンス ホストを選択します。
 - [NSX の設定] をクリックし、以前に作成したトラnsポート ゾーン、N-VDS、アップリンク プロファイルを選択します。

1 ホストの詳細
2 NSX の設定

トラnsポート ゾーン
tz

トラnsポート ゾーンの新規作成

N-VDS の作成
NSX 作成
事前設定済み

+ N-VDS の追加

ノード スイッチの作成

N-VDS 名
vds-1

関連付けられたトラnsポート ゾーン
tz

NIOC プロファイル
nsx-default-nioc-hostswitch-profile

アップリンク プロファイル
nsx-default-uplink-hostswitch-profile

LLDP プロファイル
LLDP [Send Packet Enabled]

NIOC プロファイルの新規作成

アップリンク プロファイルの新規作成

キャンセル
前へ
終了

VMware, Inc.

205

- 7 [インストールするネットワーク マッピング] セクションで、[マッピングの追加] をクリックし、セグメント/論理スイッチのマッピングに VMkernel を追加します。

インストール用のネットワーク マッピング



vmnic0 と vmk0 を移行すると、ホストの接続が切断される可能性があります。

ステートフル ホスト (スタンドアローンまたはクラスタ) の論理スイッチを変更しても影響はありませんが、操作は失敗します。

+ 追加 削除

<input checked="" type="checkbox"/> VMkernel アダプタ *	VLAN セグメント/論理スイッチ *
<input checked="" type="checkbox"/> vmk0	segment-autodeploy

- 8 [終了] をクリックして、リファレンス ホストで NSX-T のインストールを開始します。

インストール時に、VMkernel アダプタと物理 NIC が VSS または DVS スイッチから N-VDS スイッチに移行されます。インストール後、リファレンス ホストの構成状態が Success と表示されます。

注： リファレンス ホストが [その他のホスト] に表示されます。

ホスト トランスポート ノード Edge トランスポート ノード Edge クラスタ ESXi ブリッジ クラスタ

管理元 vc ▼

NSX の設定 NSX の削除 アクション ▼

表示 すべて ▼

<input type="checkbox"/>	ノード	ID	IP アドレス	OS タイプ	NSX 設定	設定の状態	ノードの状態	トンネル	トランスポート	NSX バージョン	N-VDS
<input type="checkbox"/>	Other Hosts (2)	MoRef L...					● 1 台のホストで...				
<input type="checkbox"/>		42ea...8...		ESXi 6.7.0	設定済み	● 成功	● 劣化 ①	使用不可	tz	2.5.0.0.0.14...	1
<input checked="" type="checkbox"/>	hostnode	6d4c...f...		ESXi 6.7.0	設定済み	● 成功	● 稼働中 ①	↑1	tz	2.5.0.0.0.14...	1

- 9 vCenter Server で、VSS スイッチの物理 NIC アダプと VMkernel アダプタが移行され、N-VDS スイッチに接続していることを確認します。

VMkernel アダプタ

ネットワークの追加... 更新 編集... 削除

デバイス	ネットワーク ラベル	スイッチ	IP アドレス	TCP/IP スタック
vmk0	Management Network	vSwitch0		デフォルト
vmk1	Segment_autodeploy	vds-1		デフォルト

次のステップ

ホスト プロファイルを抽出して確認します。[ホスト プロファイルの抽出と確認](#) を参照してください。

ホスト プロファイルの抽出と確認

リファレンス ホストからホスト プロファイルを抽出したら、ホスト プロファイルで抽出された NSX-T 構成を確認します。これには、ターゲット ホストに適用される ESXi と NSX-T の構成が含まれます。

手順

- 1 ホスト プロファイルを抽出するには、[リファレンス ホストからホスト プロファイルを抽出して構成](#)します。
- 2 抽出されたホスト プロファイルの NSX 構成を確認します。

お気に入りに追加

すべて

フィルタ

その他

ストレージ設定

セキュリティおよびサービス

ネットワーク設定

標準スイッチ

仮想マシン ポートグループ

ホスト ポートグループ

物理 NIC 設定

vSphere Distributed Switch

ホスト仮想 NIC

NSX ホスト vNIC:

NSX ホスト vNIC : Segment_autodeploy

NetStack インスタンス

ネットワーク コアダンプの設定

一般システム設定

詳細設定

NSX ホスト vNIC : Segment_autodeploy

この仮想 NIC を接続する論理スイッチを決定

接続先の論理スイッチの選択

*論理スイッチの名前	Segment_autodeploy
------------	--------------------

どのような場合に論理スイッチ内の仮想 NIC を作成するかを決定

常にオブジェクトを作成

論理スイッチ内の仮想 NIC 用のステートレス ブート プロパティ

ステートレス ブート設定パラメータ (変更する前にドキュメントを参照してください)

*VLAN (変更する前にドキュメントを参照してください)	0
*チームング ポリシー (変更する前にドキュメントを参照してください)	first uplink
使用するアクティブ アップリンク (変更する前にドキュメントを参照してください)	vmnic1
使用するスタンバイ アップリンク (変更する前にドキュメントを参照してください)	--
*使用する不透明スイッチの名前 (変更する前にドキュメントを参照してください)	vds-1

ネットワーク設定

標準スイッチ

仮想マシン ポートグループ

ホスト ポートグループ

物理 NIC 設定

vSphere Distributed Switch

ホスト仮想 NIC

NSX ホスト vNIC:

NSX ホスト vNIC : Segment_autodeploy

NetStack インスタンス

ネットワーク コアダンプの設定

一般システム設定

詳細設定

vmknic の MAC アドレスを決定する方法を決定

デフォルトが利用不能の場合は、ユーザーに MAC アドレスの入力を求めるプロンプトを表示

VMkernel ネットワーク アダプタ名ポリシー

割り当てられたインターフェイス名

VMkernel ネットワーク アダプタ	vmk1
----------------------	------

MTU ポリシー

指定された MTU を割り当て

*MTU	1500
------	------

TCP/IP スタック:

vmknic が接続されている Netstack インスタンス

*名前	defaultTcpipStack
-----	-------------------

結果

ホストが両方の環境に準備されたとき場合、ホスト プロファイルには ESXi と NSX に関連する構成が含まれます。

次のステップ

ステートレス クラスタとホスト プロファイルの関連付けを確認します。[ステートレス クラスタとホスト プロファイルの関連付けの確認](#) を参照してください。

VMware, Inc.

207


ステートレス クラスタとホスト プロファイルの関連付けの確認

ESXi と NSX の構成を使用してターゲット ステートレス クラスタを準備するには、リファレンス ホストから抽出されたホスト プロファイルをターゲット ステートレス クラスタに関連付けます。

ステートレス クラスタに関連付けられたホスト プロファイルがないと、クラスタに参加する新しいノードを ESXi と NSX VIB と一緒に自動的に展開できません。

手順

- 1 ホスト プロファイルをステートレス クラスタに適用するか、分離します。[ホスト プロファイルからのエンティティの適用または分離](#)を参照してください。
- 2 [展開済みのホスト] タブで、既存のステートレス ホストが正しいイメージに関連付けられ、ホスト プロファイルに関連付けられていることを確認します。
- 3 ホスト プロファイルの関連付けがない場合は、ターゲット ホストを選択し、[ホストの関連付けの修正] をクリックして、ターゲット ホストのイメージとホスト プロファイルをに強制的に更新します。

ソフトウェア デポ デプロイ ルール デプロイされたホスト 検出されたホスト スクリプト バンドル 設定					
① Auto Deploy がホストに関連付けたイメージ プロファイル、ホスト プロファイル、および場所は次のとおりです。関連付けはホストの実際の状態と異なる場合があります。					
ホスト関連付けコンプライアンスの確認 ホストの関連付けの修正 イメージ プロファイルの関連付けの編集					
<input type="checkbox"/>	ホスト ▼	関連付けられたイメージ プロファイル ▼	関連付けられたホスト プロファイル ▼	関連付けられた場所 ▼	関連付けられたスクリプト バンドル ▼
<input type="checkbox"/>		CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>		CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

次のステップ

ホストのカスタマイズを更新します。[ホストのカスタマイズの更新](#)を参照してください。

ホストのカスタマイズの更新

ホスト プロファイルをターゲット クラスタに適用した後、ESXi パッケージと NSX-T パッケージの自動展開を行うために、ホストに追加のカスタム エントリが必要になることがあります。

手順

- 1 ターゲット クラスタにホスト プロファイルを適用した後、ホストがカスタム値で更新されない場合、次のメッセージが表示されます。

Host Profile | アクション ▼

サマリ 監視 設定 ホスト

名前: Host Profile
説明:
作成日: 2019/11/07 14:36
最終更新日: 2019/11/07 14:36
バージョン: 6.7.0

⚠ ホスト [redacted] では追加のカスタマイズが必要です。
⚠ ホスト [redacted] では追加のカスタマイズが必要です。

- 2 ホストのカスタマイズを更新するには、ホスト プロファイルに移動し、[アクション] -> [ホストのカスタマイズの編集] をクリックします。
- 3 ESXi バージョン 67ep6、67ep7、67u2 の場合、MUX ユーザーのパスワードを入力します。

Customize hosts

Enter host customizations.

IMPORT HOST CUSTOMIZATIONS ⓘ

Required ▼	Property Name ▼	Path ▼	Value ▼
No	MAC Address	Networking configu...	02:00:0c:23:e9:9a
Yes	Adapter MA...	Storage configurati...	02:00:0c:23:e9:9a
Yes	Activate	Storage configurati...	false
Yes	Password	Security and	Security and Services > Security Settings > Security > User Configuration > mux_user > Pass

- 4 すべての必須フィールドが適切な値で更新されていることを確認します。

次のステップ

ターゲット ホストで自動展開をトリガします。ターゲット ホストでの自動展開のトリガを参照してください。

ターゲット ホストでの自動展開のトリガ

新しいノードがクラスタに追加された場合、手動で再起動を行い、ESXi および NSX-T VIB を設定する必要があります。

注： これは、ステートレス ホストにのみ適用されます。

ESXi の自動展開と NSX-T VIB の構成をトリガするようにホストを準備する場合、2 つの方法があります。

- TNP をステートレス クラスタに適用する前にホストを再起動します。
- TNP をステートレス クラスタに適用した後にホストを再起動します。

ホストに NSX-T をインストールするときに VMkernel アダプタを移行する場合は、次を参照してください。

- [ステートレス ホストがターゲット クラスタにある場合のシナリオ](#)
- [ステートレス ホストがターゲット クラスタの外部にある場合のシナリオ](#)

次のステップ

TNP をステートレス クラスタに適用する前にホストを再起動します。[TNP 適用前のホストの再起動](#) を参照してください。

TNP 適用前のホストの再起動

これは、ステートレス ホストにのみ適用されます。このシナリオでは、トランスポート ノード プロファイルはステートレス クラスタに適用されません。ターゲット ホストには NSX-T がインストールされず、設定されていません。

手順

- 1 ホストを再起動します。

ターゲット ホストが ESXi イメージで起動します。起動後、TNP プロファイルがターゲット ホストに適用され、NSX-T のインストールが完了するまで、ターゲット ホストはメンテナンス モードになります。次の順序でプロファイルがホストに適用されます。

次の順序でプロファイルがホストに適用されます。

- イメージ プロファイルがホストに適用されます。
- ホスト プロファイルの設定がホストに適用されます。
- NSX-T 構成がホストに適用されます。

- 2 ESXi ホストがトランスポート ノードではないため、ホストの VMkernel アダプタが <N-LogicalSegment> という名前の一時セグメントに接続します。NSX-T がインストールされると、一時スイッチが実際の N-VDS と 論理セグメントに置き換えられます。

サマリ 監視 設定 権限 仮想マシン データストア ネットワーク					
VMkernel アダプタ					
ネットワークの追加... 更新 編集... 削除					
デバイス	ネットワーク ラベル	スイッチ	IP アドレス	TCP/IP スタック	
vmk0	Management Network	vSwitch0		デフォルト	
vmk1	Segment_autodeploy	vds-1		デフォルト	

ESXi VIB は、再起動されたすべてのホストに適用されます。ESXi ホストの一時 NSX スイッチです。TNP がホストに適用されると、一時スイッチは実際の NSX-T スイッチに置き換えられます。

次のステップ

TNP をステートレス クラスタに適用します。[ステートレス クラスタへの TNP の適用](#) を参照してください。

ステートレス クラスタへの TNP の適用

TNP がクラスタに適用されている場合、ターゲット ホストでのみ NSX-T の構成とインストールが行われます。

手順

- リファレンス ホストからホスト プロファイルに抽出された設定をメモします。TNP プロファイルで対応するエンティティの値は同じにする必要があります。たとえば、ホスト プロファイルと TNP で使用される N-VDS 名は同じにする必要があります。
抽出されたホスト プロファイル設定の詳細については、[ホスト プロファイルの抽出と確認](#)を参照してください。
- TNP を追加します。[トランスポート ノード プロファイルの追加](#)を参照してください。
- 新しい TNP プロファイルと既存のホスト プロファイルの両方で、以下のパラメータに同じ値が設定されていることを確認します。
 - N-VDS 名：ホスト プロファイルの N-VDS 名と TNP が同じであることを確認します。
 - アップリンク プロファイル：ホスト プロファイルで参照されるアップリンク プロファイルと TNP が同じであることを確認します。
 - 物理 NIC：物理 NIC をアップリンク プロファイルにマッピングする場合は、まず、ホスト プロファイルで使用されている NIC を確認し、その物理 NIC をアップリンク プロファイルにマッピングします。
 - インストールのネットワーク マッピング：インストール中にネットワークをマッピングする場合は、まず、ホスト プロファイルで VMkernel とセグメントのマッピングを確認し、TNP に同じマッピングを追加します。
 - アンインストール時のネットワーク マッピング：アンインストール中にネットワークをマッピングする場合は、まず、ホスト プロファイルで VMkernel と VSS/DVS スイッチのマッピングを確認し、TNP に同じマッピングを追加します。

- 4 すべての必須フィールドを入力して、TNP を追加します。[トランスポート ノード プロファイルの追加](#)を参照してください。

新しい TNP プロファイルと既存のホスト プロファイルの両方で、以下のパラメータに同じ値が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：ホスト プロファイルで参照されるトランスポート ゾーンと TNP が同じであることを確認します。
- N-VDS 名：ホスト プロファイルで参照される N-VDS 名と TNP が同じであることを確認します。
- アップリンク プロファイル：ホスト プロファイルで参照されるアップリンク プロファイルと TNP が同じであることを確認します。
- 物理 NIC：物理 NIC をアップリンク プロファイルにマッピングする場合は、まず、ホスト プロファイルで使用されている NIC を確認し、その物理 NIC をアップリンク プロファイルにマッピングします。
- インストール時のネットワーク マッピング：インストール中にネットワークをマッピングする場合は、まず、ホスト プロファイルで VMkernel と論理スイッチのマッピングを確認し、TNP に同じマッピングを追加します。
- アンインストールのネットワーク マッピング：アンインストール中にネットワークをマッピングする場合は、まず、ホスト プロファイルで VMkernel と VSS/DVS スイッチのマッピングを確認し、TNP に同じマッピングを追加します。

N-VDS 名 *	vds-tzvian	▼
関連付けられたトランスポートゾーン	tz-33	
NIOC プロファイル *	nsx-default-nioc-hostswitch-profile	▼
NIOC プロファイルの新規作成		
アップリンク プロファイル *	nsx-default-uplink-hostswitch-profile	▼
アップリンク プロファイルの新規作成		
LLDP プロファイル *	LLDP [Send Packet Enabled]	▼
IP の割り当て *		▼
物理 NIC	vmnic1	▼
	uplink-1	▼
物理 NIC の追加		
物理 NIC のみの移行	<input type="checkbox"/> いいえ	
移行対象に選択した物理 NIC に vmk が存在しない場合は、このオプションを有効にします		
インストール用のネットワーク マッピング	1 個のマッピング	
アンインストール用のネットワーク マッピング	マッピングの追加	

ターゲット ノードに TNP を適用した後、TNP の構成がホスト プロファイルと一致しない場合、コンプライアンス エラーでノードが起動しないことがあります。

- 5 TNP プロファイルが正常に作成されたことを確認します。
- 6 TNP プロファイルをターゲット クラスタに適用し、[保存] をクリックします。

NSX の設定



トランスポート ノード プロファイルで定義されている展開設定を使用して、選択したクラスタに NSX がインストールされます

展開プロファイルの選択 *	TNP_StatelessCluster	▼
新しいトランスポート ノード プロファイルの作成		

キャンセル

保存

- 7 TNP プロファイルがターゲット クラスタに正常に適用されていることを確認します。正常に適用されていれば、クラスタのすべてのノードで NSX が正常に構成されています。
- 8 vSphere で、物理 NIC または VMkernel アダプタが N-VDS スイッチに接続されていることを確認します。

VMkernel アダプタ

 ネットワークの追加...
  更新
  編集...
  削除

デバイス	ネットワーク ラベル	スイッチ	IP アドレス	TCP/IP スタック
vmk0	Management Network	vSwitch0		デフォルト
vmk1	Segment_autodeploy	vds-1		デフォルト

- 9 NSX で、ESXi ホストがトランスポート ノードとして正常に構成されていることを確認します。

次のステップ

あるいは、クラスタに TNP を適用した後に、ターゲット ホストを再起動します。[TNP 適用後のホストの再起動](#) を参照してください。

TNP 適用後のホストの再起動

これは、ステートレス ホストにのみ適用されます。新しいノードがクラスタに追加されたら、ESXi パッケージと NSX-T パッケージが設定されるように、ノードを手動で再起動します。

手順

- 1 ホスト プロファイルで準備されているステートレス クラスタに TNP を適用します。[ステートレス クラスタでの TNP の作成と適用](#)を参照してください。
- 2 ホストを再起動します。

TNP プロファイルをステートレス クラスタに適用した後、クラスタに参加する新しいノードを再起動すると、そのノードにホストの NSX-T が自動的に設定されます。

次のステップ

再起動されたノードに ESXi と NSX-T が自動的に展開され、設定されるように、クラスタに参加するすべての新しいノードを再起動します。

自動展開の設定時にホスト プロファイルとトランスポート ノード プロファイルに関連する問題を解決する方法については、[ホスト プロファイルとトランスポート ノード プロファイルのトラブルシューティング](#)を参照してください。

ステートレス ホストがターゲット クラスタにある場合のシナリオ

このセクションでは、ターゲット クラスタにステートレス ホストが存在する場合の使用事例について説明します。

重要： ステートレス ターゲット ホストの場合：

- NSX-T 2.4 と NSX-T 2.4.1 では、VSS/DVS から N-VDS に vmk0 アダプタを移行できません。
- NSX-T 2.5 では、VSS/DVS から N-VDS への vmk0 アダプタの移行がサポートされています。

ターゲット ホスト	リファレンス ホストの構成	ターゲット ホストの Auto Deploy の手順
ターゲット ホストに vmkO アダプタが設定されています。	リファレンス ホストから抽出されたホスト プロファイルでは、N-VDS スイッチに vmkO が設定されています。 NSX-T では、TNP に vmkO 移行マッピングのみが設定されています。	<ol style="list-style-type: none"> 1 ホスト プロファイルをターゲット ホストに適用します。 vmkO アダプタが vSwitch に接続します。 2 必要に応じて、ホストのカスタマイズを更新します。 3 ホストを再起動します。ホスト プロファイルがホストに適用されます。vmkO が一時スイッチに接続されます。 4 TNP を適用します。 vmkO アダプタが N-VDS に移行されます。 ターゲット ホストが ESXi と NSX-T VIB で正常に展開されました。
ターゲット ホストに vmkO アダプタが設定されています。	リファレンス ホストから抽出されたホスト プロファイルでは、vSwitch に vmkO が設定され、N-VDS スイッチに vmk1 が設定されています。 NSX-T では、TNP に vmk1 移行マッピングのみが設定されています。	<ol style="list-style-type: none"> 1 ホスト プロファイルをターゲット ホストに適用します。 vmkO アダプタが vSwitch に接続されますが、vmk1 はどのスイッチにも認識されません。 2 必要に応じて、ホストのカスタマイズを更新します。 3 ホストを再起動します。 vmkO が vSwitch に接続され、vmk1 が一時 NSX スイッチに接続されます。 4 TNP を適用します。 vmk1 アダプタが N-VDS に移行されます。 5 (オプション) ホストがホスト プロファイルに準拠していない場合は、ホストを再起動してホストに準拠させます。 ターゲット ホストが ESXi と NSX-T VIB で正常に展開されました。
ターゲット ホストに vmkO アダプタが設定されています。	リファレンス ホストから抽出されたホスト プロファイルでは、vSwitch に vmkO が設定され、N-VDS スイッチに vmk1 が設定されています。 NSX-T では、TNP に vmkO と vmk1 の移行マッピングのみが設定されています。	<ol style="list-style-type: none"> 1 ホスト プロファイルをターゲット ホストに適用します。 vmkO アダプタが vSwitch に接続されますが、vmk1 はどのスイッチにも認識されません。 2 必要に応じて、ホストのカスタマイズを更新します。 3 ホストを再起動します。 vmkO アダプタが vSwitch に接続され、vmk1 が一時 NSX スイッチに接続されます。 4 TNP を適用します。 5 (オプション) ホストがホスト プロファイルに準拠していない場合は、ホストを再起動してホストに準拠させます。 ターゲット ホストが ESXi と NSX-T VIB で正常に展開されました。

ターゲット ホスト	リファレンス ホストの構成	ターゲット ホストの Auto Deploy の手順
ターゲット ホストに vmk0 アダプタと vmk1 アダプタが設定されています。	リファレンス ホストから抽出されたホスト プロファイルでは、vSwitch に vmk0 が設定され、N-VDS スイッチに vmk1 が設定されています。 NSX-T では、TNP に vmk1 移行マッピングが設定されています。	<ol style="list-style-type: none"> 1 ホスト プロファイルをターゲット ホストに適用します。 vmk0 アダプタと vmk1 アダプタが vSwitch に接続します。 2 必要に応じて、ホストのカスタマイズを更新します。 3 ホストを再起動します。 4 TNP を適用します。 vmk0 アダプタが vSwitch に接続され、vmk1 が N-VDS スイッチに接続されます。 5 (オプション) ホストがホスト プロファイルに準拠していない場合は、ホストを再起動してホストに準拠させます。 ターゲット ホストが ESXi と NSX-T VIB で正常に展開されました。
ターゲット ホストに vmk0 アダプタと vmk1 アダプタが設定されています。	リファレンス ホストから抽出されたホスト プロファイルでは、N-VDS に vmk0 と vmk1 が設定されています。 NSX-T では、TNP に vmk0 と vmk1 の移行マッピングが設定されています。	<ol style="list-style-type: none"> 1 ホスト プロファイルをターゲット ホストに適用します。 vmk0 アダプタと vmk1 アダプタが vSwitch に接続します。 2 必要に応じて、ホストのカスタマイズを更新します。 3 ホストを再起動します。 4 TNP を適用します。 vmk0 と vmk1 が N-VDS スイッチに移行されます。 ターゲット ホストが ESXi と NSX-T VIB で正常に展開されました。

ステートレス ホストがターゲット クラスタの外部にある場合のシナリオ

このセクションでは、ターゲット クラスタにステートレス ホストの外部に存在する場合の使用事例について説明します。

重要： ステートレス ホストでは、次の点に注意してください。

- NSX-T 2.4 と NSX-T 2.4.1 では、VSS/DVS から N-VDS に vmk0 アダプタを移行できません。
- NSX-T 2.5 では、VSS/DVS から N-VDS への vmk0 アダプタの移行がサポートされています。

ターゲット ホストの状態	リファレンス ホストの構成	ターゲット ホストの Auto Deploy の手順
<p>ホストはパワーオフ状態です（初回開始時）。その後、クラスタに追加されています。</p> <p>ターゲット クラスタにデフォルトの Auto Deploy ルールが設定され、ホスト プロファイルに関連付けられています。</p> <p>TNP はクラスタに適用されています。</p>	<p>リファレンス ホストから抽出されたホスト プロファイルでは、vSwitch に VMkernel アダプタ 0 (vmk0) が設定され、N-VDS スイッチに VMkernel アダプタ 1 (vmk1) が設定されています。</p> <p>NSX-T では、TNP に vmk1 移行マッピングのみが設定されています。</p>	<ol style="list-style-type: none"> ホストをパワーオンします。 <p>ホストがパワーオンされた後：</p> <ul style="list-style-type: none"> ■ ホストがクラスタに追加されます。 ■ ホスト プロファイルがターゲット ホストに適用されます。 ■ vmk0 アダプタは vSwitch 上にあり、vmk1 アダプタは一時スイッチ上にあります。 ■ TNP がトリガします。 ■ TNP がクラスタに適用された後、vmk0 アダプタが vSwitch 上にあり、vmk1 が N-VDS スイッチに移行されます。 <ol style="list-style-type: none"> （オプション）ホストがホスト プロファイルに準拠していない場合は、ホストを再起動してホストに準拠させます。 <p>ホストが ESXi と NSX-T VIB で正常に展開されました。</p>
<p>ホストはパワーオフ状態です（初回開始時）。その後、クラスタに追加されています。</p> <p>ターゲット クラスタにデフォルトの Auto Deploy ルールが設定され、ホスト プロファイルに関連付けられています。</p> <p>TNP はクラスタに適用されています。</p>	<p>リファレンス ホストから抽出されたホスト プロファイルでは、N-VDS スイッチに VMkernel アダプタ 0 (vmk0) と VMkernel アダプタ 1 (vmk1) が設定されています。</p> <p>NSX-T では、TNP に vmk0 と vmk1 の移行のみが設定されています。</p>	<ol style="list-style-type: none"> ホストをパワーオンします。 <p>ホストがパワーオンされた後：</p> <ul style="list-style-type: none"> ■ ホストがクラスタに追加されます。 ■ ホスト プロファイルがターゲット ホストに適用されます。 ■ vmk0 アダプタと vmk1 アダプタは一時スイッチ上にあります。 ■ TNP がトリガーされます。 ■ TNP がクラスタに適用された後、vmk0 と vmk1 が N-VDS スイッチに移行されます。 <p>ホストが ESXi と NSX-T VIB で正常に展開されました。</p>
<p>ホストはパワーオン状態です。その後、クラスタに追加されています。</p> <p>ターゲット クラスタにデフォルトの Auto Deploy ルールが設定され、ホスト プロファイルに関連付けられています。</p> <p>ターゲット ホストに vmk0 アダプタのみが設定されています。</p>	<p>リファレンス ホストから抽出されたホスト プロファイルでは、vSwitch に VMkernel アダプタ 0 (vmk0) が設定され、N-VDS スイッチに VMkernel アダプタ 1 (vmk1) が設定されています。</p> <p>NSX-T では、TNP に vmk1 移行マッピングが設定されています。</p>	<ol style="list-style-type: none"> ホストをクラスタの一部にします。 ホストを再起動します。 <p>ホストが再起動すると、ホスト プロファイルがターゲット ホストに適用されます。</p> <ul style="list-style-type: none"> ■ vmk0 アダプタが vSwitch に接続され、vmk1 アダプタが一時 NSX スイッチに接続されます。 ■ TNP がトリガーされます。 ■ vmk1 が N-VDS スイッチに移行されます。 <ol style="list-style-type: none"> （オプション）ホストがホスト プロファイルに準拠していない場合は、ホストを再起動してホストに準拠させます。 <p>ホストが ESXi と NSX-T VIB で正常に展開されました。</p>

ターゲット ホストの状態	リファレンス ホストの構成	ターゲット ホストの Auto Deploy の手順
<p>ホストはパワーオン状態です。その後、クラスタに追加されています。</p> <p>ターゲット クラスタにデフォルトの Auto Deploy ルールが設定され、ホスト プロファイルに関連付けられています。</p> <p>ターゲット ホストに vmk0 アダプタのみが設定されています。</p>	<p>リファレンス ホストから抽出されたホスト プロファイルでは、N-VDS に VMkernel アダプタ 0 (vmk0) と VMkernel アダプタ 1 (vmk1) が設定されています。</p> <p>NSX-T では、TNP に vmk0 と vmk1 の移行のみが設定されています。</p>	<ol style="list-style-type: none"> 1 ホストをクラスタの一部にします。 2 ホストを再起動します。 <p>ホストが再起動すると、ホスト プロファイルがターゲット ホストに適用されます。</p> <ul style="list-style-type: none"> ■ vmk0 アダプタと vmk1 アダプタが一時 NSX スイッチに接続します。 ■ TNP がトリガーされます。 ■ vmk0 と vmk1 が N-VDS スイッチに接続します。 <p>ホストが ESXi と NSX-T VIB で正常に展開されました。</p>
<p>ホストはパワーオン状態です。その後、クラスタに追加されています。</p> <p>ターゲット クラスタにデフォルトの Auto Deploy ルールが設定され、ホスト プロファイルに関連付けられています。</p> <p>ターゲット ホストに vmk0 と vmk1 のネットワーク マッピングが設定されています。</p>	<p>リファレンス ホストから抽出されたホスト プロファイルでは、vSwitch に VMkernel アダプタ 0 (vmk0) が設定され、N-VDS スイッチに VMkernel アダプタ 1 (vmk1) が設定されています。</p> <p>NSX-T では、TNP に vmk1 の移行が設定されています。</p>	<ol style="list-style-type: none"> 1 ホストをクラスタの一部にします。 2 ホストを再起動します。 <p>ホストが再起動すると、ホスト プロファイルがターゲット ホストに適用されます。</p> <ul style="list-style-type: none"> ■ vmk0 アダプタが vSwitch に接続され、vmk1 アダプタが一時 NSX スイッチに接続されます。 ■ TNP がトリガーします。 ■ vmk1 が N-VDS スイッチに移行されます。 <ol style="list-style-type: none"> 3 (オプション) ホストがホスト プロファイルに準拠していない場合は、ホストを再起動してホストに準拠させます。 <p>ホストが ESXi と NSX-T VIB で正常に展開されました。</p>
<p>ホストはパワーオン状態です。その後、クラスタに追加されています。</p> <p>ターゲット クラスタにデフォルトの Auto Deploy ルールが設定され、ホスト プロファイルに関連付けられています。</p> <p>ホストに vmk0 と vmk1 のネットワーク マッピングが設定されています。</p>	<p>リファレンス ホストのホスト プロファイルで、VMkernel アダプタ 0 (vmk0) と VMkernel アダプタ 1 (vmk1) が N-VDS スイッチに設定されています。</p> <p>NSX-T では、TNP に vmk0 と vmk1 の移行のみが設定されています。</p>	<ol style="list-style-type: none"> 1 ホストをクラスタの一部にします。 2 ホストを再起動します。 <p>ホストが再起動すると、ホスト プロファイルがターゲット ホストに適用されます。</p> <ul style="list-style-type: none"> ■ vmk0 アダプタと vmk1 アダプタが一時 NSX スイッチに接続します。 ■ TNP がトリガーします。 ■ vmk0 アダプタと vmk1 アダプタが N-VDS スイッチに移行されます。 <p>ホストが ESXi と NSX-T VIB で正常に展開されました。</p>

ホスト プロファイルとトランスポート ノード プロファイルのトラブルシューティング

ホスト プロファイルと TNP がステートレス クラスタの自動展開に使用されている場合に発生した問題のトラブルシューティングを行います。

シナリオ	説明
ホスト プロファイルを移動できません。	<p>問題：どの vCenter Server も、NSX-T 構成を含むホスト プロファイルを使用できません。</p> <p>回避策：なし。</p>
Auto Deploy ルール エンジン	<p>問題：新しいクラスタを展開するときに、ホスト プロファイルを Auto Deploy ルールで使用できません。新しいクラスタを展開すると、ホストは基本ネットワークで展開され、メンテナンス モードのままになります。</p> <p>回避策：NSX-T の GUI からクラスタを準備します。ステートレス クラスタへの TNP の適用を参照してください。</p>
コンプライアンス エラーを確認してください。	<p>問題：ホスト プロファイルの修正で、NSX-T 構成のコンプライアンス エラーを修正できない。</p> <ul style="list-style-type: none"> ■ ホスト プロファイルと TNP で構成されている物理 NIC が異なります。 ■ vNIC と LS のマッピング。論理スイッチと vNIC のマッピングの設定が、ホスト プロファイルと TNP プロファイルとで一致していません。 ■ N-VDS に接続する VMkernel の設定が、ホスト プロファイルと TNP とで一致していません。 ■ ホスト プロファイルと TNP とで不透明スイッチが一致していません。 <p>回避策：NSX-T 構成がホスト プロファイルと TNP で一致していることを確認します。ホストを再起動して、構成の変更を認識させます。ホストが起動します。</p>
修正方法	<p>問題：NSX-T 固有のコンプライアンス エラーが発生すると、そのクラスタでのホスト プロファイルの修正がブロックされる。</p> <p>設定が無効です。</p> <ul style="list-style-type: none"> ■ vNIC と LS のマッピング ■ 物理 NIC のマッピング <p>回避策：NSX-T 構成がホスト プロファイルと TNP で一致していることを確認します。ホストを再起動して、構成の変更を認識させます。ホストが起動します。</p>
接続	<p>問題：NSX-T で設定されているクラスタで、ホスト プロファイルをホスト レベルで適用できない。</p> <p>回避策：なし。</p>
接続解除	<p>問題：NSX-T で設定されたクラスタでホスト プロファイルの分離と追加を行っても、NSX-T 構成が削除されない。クラスタが新しく適用されたホスト プロファイルに準拠していても、以前のプロファイルの NSX-T 構成が残ったままになります。</p> <p>回避策：なし。</p>
更新	<p>問題：ユーザーがクラスタ内の NSX-T 構成を変更した場合、新しいホスト プロファイルを抽出する必要がある。失われたすべての設定について、ホスト プロファイルを手動で更新します。</p> <p>回避策：なし。</p>
ホスト レベルのトランスポート ノードの設定	<p>問題：anportsport ノードが自動展開され RU、個別のエンティティとして機能する。このトランスポート ノードに対する更新が TNP と一致しない場合があります。</p> <p>回避策：クラスタを更新します。スタンドアローンのトランスポート ノードの更新で、移行の設定が維持されません。移行で再起動を延期できないことがあります。</p>
mux_user パスワード ポリシーとパスワードがリセットされなかったため、ホスト プロファイルを適用できません。	<p>問題：vSphere 6.7 U3 より前のバージョンを実行しているホストでのみ発生する。mux_user のパスワードがリセットされていないと、ホストの修正とホスト プロファイル アプリケーションが失敗することがあります。</p> <p>回避策：[ポリシーとプロファイル] でホスト プロファイルを編集し、mux_user パスワード ポリシーを変更して、mux_user のパスワードをリセットします。</p>

シナリオ	説明
NVDS スイッチへの移行で選択した VMkernel アダプタで、ピア DNS 構成がサポートされません。	<p>問題: NVDS への移行で選択した VMkernel アダプタでピア DNS が有効になっていると、ホスト プロファイル アプリケーションが失敗する。</p> <p>回避策: 抽出されたホスト プロファイルを編集し、NVDS スイッチに移行する VMkernel アダプタのピア DNS 設定を無効にします。または、ピア DNS が有効になっている VMkernel アダプタを NVDS スイッチに移行しないようにします。</p>
VMkernel NIC アドレスの DHCP アドレスが保持されていません。	<p>問題: リファレンス ホストがステートフルの場合、ステートフル リファレンス ホストから抽出されたプロファイルを使用するステートレス ホストが、PXE 起動の MAC から派生した VMkernel 管理の MAC アドレスを保持できない。その結果、DHCP のアドレス割り当てで問題が発生します。</p> <p>回避策: ステートフル ホストから抽出されたホスト プロファイルを編集して、[vmknic の MAC アドレスを決定する方法を確認] を [システムが PXE 起動されたときの MAC アドレスを使用] に変更します。</p>
vCenter Server でホスト プロファイルのアプリケーション エラーが発生すると、ホストで NSX 構成エラーが発生する可能性があります。	<p>問題: vCenter Server でホスト プロファイル アプリケーションが失敗すると、NSX の構成も失敗することがある。</p> <p>回避策: vCenter Server で、ホスト プロファイルが正常に適用されていることを確認します。エラーを修正して再試行します。</p>
ステートレス ESXi ホストで LAG がサポートされません。	<p>問題: NSX で LAG として設定されたアップリンク プロファイルが、vCenter Server または NSX で管理されているステートレス ESXi ホストでサポートされない。</p> <p>回避策: なし。</p>

ステートフル サーバ

ESXi ホストのホスト プロファイルをステートフル サーバの NSX-T に統合します。

ステートフル ホストは、再起動後もすべての構成とインストールされた VIB を保持するホストです。ステートレス ホストの起動に必要な起動ファイルは Auto Deploy サーバに保存されるため、ステートレス ホストには Auto Deploy サーバが必要です。ただし、ステートフル ホストは同様のインフラストラクチャを必要としません。ステートフル ホストの起動に必要な起動ファイルは、そのハード ドライブに保存されます。

この手順では、リファレンス ホストがステートフル クラスタの外部にあり、ターゲット ホストがクラスタ内に存在します。ターゲット ホストはクラスタ内に配置することも、クラスタ外部のスタンドアローン ホストとして配置することもできます。ホスト プロファイルとトランスポート ノード プロファイル (TN プロファイル) を適用してクラスタを準備し、クラスタに参加する新しいターゲット ホストが NSX-T VIB で自動的に準備されるようにします。トランスポート ノードとしてターゲット ホストを構成します。スタンドアローン ホストの場合は、ホスト プロファイルを適用して、NSX-T VIB をインストールするように NSX-T を設定します。NSX-T の設定が完了すると、これがトランスポート ノードになります。

注: NSX-T VIB は TN プロファイルからインストールされます。ESXi ホストの構成はホスト プロファイルによって適用されます。

ターゲット ホストをトランスポート ノードに設定するときに、VMkernel アダプタと vmnic、または VSS または VDS スイッチに接続している物理ネットワーク インターフェイスが移行され、NSX-T 仮想分散スイッチ (N-VDS スイッチ) に接続します。

サポートされる NSX-T と ESXi のバージョン

ステートフル サーバでサポートされる NSX-T と ESXi のバージョン。

バージョン名	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03
NSX-T 2.4	○	×	×	×	×	×	○
NSX-T 2.4.1	○	○	×	×	×	×	○
NSX-T 2.4.2	○	○	×	×	×	×	○
NSX-T 2.4.3	○	○	×	×	×	×	○
NSX-T 2.5	○	○	○	○	○	○	○
NSX-T 2.5.1	○	○	○	○	○	○	○

ステートフル ターゲット クラスタの準備

ステートフル ターゲット クラスタを準備して、クラスタに参加する新しいホストが ESXi と NSX-T VIB で自動的に展開されるようにします。

クラスタ内またはクラスタ外のいずれかのホストをリファレンス ホストとして選択できます。リファレンス ホストのホスト プロファイルが抽出され、ターゲット ホストに適用されるため、リファレンス ホストを作成する必要があります。ここでは、vmk0（管理トラフィック）と vmk1（vMotion トラフィック）を N-VDS スイッチに移行する手順について説明します。

前提条件

手順

- 1 リファレンス ホストで、サポートされる ESXi ビルドを展開します。
 - a vSphere で、vmk1 アダプタを追加します。vmk0 はすでに存在し、管理トラフィックを処理しています。
- 2 トランSPORT ノードとしてリファレンス ノードを設定します。
 - a vmk0 と vmk1 を移行する前に、vSphere Web Client を使用して、NSX-T に論理スイッチが作成されていることを確認します。
 - b （オプション）NSX-T のインストール後に論理スイッチにマッピングされた vmk1 アダプタが N-VDS スイッチに移行されるように、NSX-T Manager UI で NSX を設定します。
 - c （オプション）NSX-T のインストール後に論理スイッチにマッピングされた vmk0 アダプタが N-VDS スイッチに移行されるように、NSX-T Manager UI で NSX-T を設定します。

注： vmk0 と vmk1 は異なる VSS または DVS スイッチに接続できます。

- d vSphere Web Client で、vmk0 と vmk1 が N-VDS スイッチ上の論理スイッチに接続されていることを確認します。
- 3 リファレンス ホストからホスト プロファイルを抽出します。

- 4 環境によっては、N-VDS スイッチへの移行が必要な vmkernel アダプタが数多く存在していることがあります。ただし、vmk アダプタを VSS/DVS から N-VDS スイッチに移行する前に、ターゲット ホスト上の設定パラメータがリファレンス ホストの設定パラメータと一致するようにしてください。
- 5 ターゲット ホストがスタンドアローン ホストの場合：
 - a ホスト プロファイルをターゲット ホストに適用します。
 - b ホストの NSX-T を手動で設定します。ESXi のホスト プロファイルが原因でホストをトランスポート ノードとして設定する場合は、次の条件を満たしていることを確認します。
 - c ホストが、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。
 - d vmk1 アダプタが、リファレンス ホストと同じ論理スイッチに接続している必要があります。
 - e ターゲット ホストが、リファレンス ホストと同じ IP プールを使用している必要があります。
 - f アップリンク プロファイル、LLDP、NIOC、インストールのネットワーク マッピング、ターゲット ホストで設定された N-VDS がリファレンス ホストの設定と一致している必要があります。
 - g VMkernel アダプタの vmk1 と vmnic1 を手動で追加し、VSS/DVS スイッチから N-VDS スイッチに移行します。vmk1 の移行シナリオを参照してください。
 - h 管理アダプタの vmk0 と vmnic0 を手動で追加します。
- 6 ターゲット ホストがクラスタの一部である場合：
 - a ホスト プロファイルをステートフル ターゲット クラスタに適用します。
 - b TN プロファイルを作成して、クラスタに適用します。
 - c 移行する vmk1 と vmnic1 を設定する方法については、vmk1 の移行シナリオを参照してください。
 - d 移行する vmk0 と vmnic0 を設定する方法については、vmk0 の移行シナリオを参照してください。
 - e TN プロファイルをクラスタに適用する方法

次のステップ

VMkernel アダプタの移行で NSX-T に適用されたホスト プロファイルを使用する場合と使用しない場合のシナリオ

ホスト プロファイルを適用する VMkernel の移行

このセクションで説明するシナリオでは、NSX-T で適用されているホスト プロファイルを使用して、VMkernel 1 (vmk1) アダプタを N-VDS スイッチに移行します。vmk1 アダプタは、vMotion、Fault Tolerance、その他のインフラストラクチャ サービスのトラフィックをサポートします。

シナリオ	エラー	回避策
<p>リファレンス ホストのプロファイルを適用して、スタンドアローンのターゲット ホストで vmk1 を移行する。</p>	<p>ターゲット ホストがトランスポート ノードとして設定されません。ターゲット ホストが NSX-T オブジェクトを認識していないため、ホスト プロファイルのアプリケーションでエラーが発生します。ターゲット ホストのホスト プロファイルの修正に失敗します。</p> <pre>Error: Received SOAP response fault : generate HostConfigTask Spec..</pre>	<ol style="list-style-type: none"> 1 リファレンス ホストのプロファイルを適用して vmk1 をターゲット ホストの論理スイッチに移行する前に、ターゲット ホストをトランスポート ノードとして設定します。これにより、NSX-T VIB がインストールされ、N-VDS スイッチが作成されて、vmk1 アダプタが VSS スイッチから N-VDS スイッチに移行されます。 <p>ESXi のホスト プロファイルが原因でホストをトランスポート ノードとして設定する場合は、次の条件を満たしていることを確認します。</p> <ul style="list-style-type: none"> ■ ホストが、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。 ■ vmk1 アダプタが、リファレンス ホストと同じ論理スイッチに接続している必要があります。 ■ ターゲット ホストが、リファレンス ホストと同じ IP ブールを使用している必要があります。 ■ アップリンク プロファイル、LLDP、NIOC、インストールのネットワーク マッピング、ターゲット ホストで設定された N-VDS がリファレンス ホストの設定と一致している必要があります。 <p>ターゲット ホストが、ホスト プロファイルと同じ論理スイッチ名で構成されている場合、ホスト プロファイルの修正が成功します。</p>
<p>ステートフル クラスタ内のターゲット ホストで vmk1 を移行する。</p>	<p>ターゲット ホストにホスト プロファイルを適用する前に、論理スイッチにマッピングされた vmk1 の TN プロファイルを適用してクラスタを準備すると、vmk1 の移行に失敗します。</p> <pre>Error: vmk1 missing on the host.</pre>	<ol style="list-style-type: none"> 1 クラスタに参加しているターゲット ホストにリファレンス ホストのプロファイルを適用します。 2 ターゲット ホストのホスト プロファイルを修正して、ターゲット ホストに vmk1 アダプタを作成します。 3 TN プロファイルをクラスタに再度適用し、vmk1 をターゲット クラスタに移行します。

シナリオ	エラー	回避策
スタンドアローン ホストで vmk0 と vmk1 を移行する。	スタンドアローン ホストで NSX-T を設定する場合、[インストールのネットワーク マッピング] フィールドに vmk0 または vmk1 マッピングが指定されていないと、移行が失敗します。	ターゲット ホストで NSX-T を設定する場合は、[インストールのネットワーク マッピング] フィールドに、N-VDS の同じ論理スイッチにマッピングされている vmk0 と vmk1 が指定されていることを確認します。
クラスタ ホストで vmk0 と vmk1 を移行する。	TN プロファイルをクラスタに適用する場合、[インストールのネットワーク マッピング] フィールドに vmk0 または vmk1 マッピングが指定されていないと、移行が失敗します。	TN プロファイルをクラスタに適用します。TN プロファイルをクラスタに設定する場合は、[インストールのネットワーク マッピング] フィールドに、N-VDS の論理スイッチにマッピングされている vmk0 と vmk1 が指定されていることを確認します。

ホスト プロファイルを適用しない VMkernel の移行

このセクションで説明するシナリオでは、NSX-T で適用されているホスト プロファイルを使用せずに、VMkernel 0 (vmk0) アダプタを N-VDS スイッチに移行します。vmk0 アダプタは、NSX-T の管理トラフィックをサポートします。

vmk0 がすでに存在するため、ホスト プロファイルをターゲット ホストに適用する必要はありません。vmk0 アダプタは、ESXi ホストの管理トラフィックをサポートします。

シナリオ	手順	結果
スタンドアローン ホストで vmk0 を移行する。	ターゲット ホストで NSX-T を設定する場合は、[インストールのネットワーク マッピング] フィールドに、N-VDS の論理スイッチにマッピングされている vmk0 が指定されていることを確認します。	vmk0 がターゲット ホストの論理スイッチに移行されます。
クラスタ ホストで vmk0 を移行する。	TN プロファイルをクラスタに適用します。TN プロファイルをクラスタに設定する場合は、[インストールのネットワーク マッピング] フィールドに、N-VDS の論理スイッチにマッピングされている vmk0 が指定されていることを確認します。	vmk0 がターゲット ホストの論理スイッチに移行されます。

ホスト トランスポート ノードからの NSX-T Data Center のアンインストール

12

ホスト トランスポート ノードから NSX-T Data Center をアンインストールする手順は、ホストのタイプと設定方法によって異なります。

- アンインストールのためのホスト ネットワーク マッピングの確認

ESXi ホストから NSX-T Data Center をアンインストールする前に、アンインストールのための適切なネットワーク マッピングが設定されていることを確認します。マッピングは、ESXi ホストで VMkernel インターフェイスが N-VDS に接続されている場合に必要です。

- vSphere クラスタからの NSX-T Data Center のアンインストール

トランスポート ノード プロファイルを使用して vSphere クラスタに NSX-T Data Center をインストールしている場合は、次の手順に従って、クラスタ内のすべてのホストから NSX-T Data Center をアンインストールできます。

- vSphere クラスタ内のホストからの NSX-T Data Center のアンインストール

NSX-T Data Center は、vCenter Server によって管理されている単一のホストからアンインストールできます。クラスタ内の他のホストは影響を受けません。

- スタンドアローン ホストからの NSX-T Data Center のアンインストール

スタンドアローン ホストから NSX-T Data Center をアンインストールできます。スタンドアローン ホストには、ESXi または KVM があります。

アンインストールのためのホスト ネットワーク マッピングの確認

ESXi ホストから NSX-T Data Center をアンインストールする前に、アンインストールのための適切なネットワーク マッピングが設定されていることを確認します。マッピングは、ESXi ホストで VMkernel インターフェイスが N-VDS に接続されている場合に必要です。

アンインストール マッピングは、アンインストール後にインターフェイスが接続される場所を決定します。物理インターフェイス (vmnicX) と VMkernel インターフェイス (vmkX) のアンインストール マッピングがあります。アンインストールを実行すると、VMkernel インターフェイスは、現在の接続から、アンインストール マッピングで指定されたポート グループに移動されます。物理インターフェイスがアンインストール マッピングに含まれている場合、物理インターフェイスは、VMkernel インターフェイスのターゲットのポート グループに基づいて、適切な vSphere Distributed Switch または vSphere 標準スイッチに接続されます。

注意： 物理インターフェイスまたは VMkernel インターフェイスが N-VDS に接続されている場合、ESXi ホストから NSX-T Data Center をアンインストールする影響が出る場合があります。ホストまたはクラスタが vSAN などの他のアプリケーションに参加している場合、それらのアプリケーションはアンインストールの影響を受ける可能性があります。

アンインストールのためのネットワーク マッピングを設定できる場所は 2 つあります。

- トランスポート ノード設定。これはそのホストに適用されます。
- トランスポート ノード プロファイル設定。これはクラスタに適用されます。

注： トランスポート ノード プロファイルをクラスタに適用するには、コンピュート マネージャが設定されている必要があります。

コンピュート マネージャが設定されている場合、ホストはトランスポート ノード設定とトランスポート ノード プロファイル設定の両方を持つことができます。最後に適用された設定がアクティブになります。アンインストールのためのネットワーク マッピングがアクティブ設定で正しく設定されていることを確認します。

この例では、クラスタ cluster-1 には、トランスポート ノード プロファイル TNP-1 が適用されています。ホスト tn-1 に「設定が一致しません」と表示されます。この不一致メッセージは、トランスポート ノード プロファイルが適用された後に、別の設定が tn-1 に適用されたことを示しています。トランスポート ノード tn-2 はトランスポート ノード プロファイルのネットワーク マッピングを使用し、トランスポート ノード tn-1 は独自の設定を使用します。

⚙️ NSX の設定
🗑️ NSX の削除
⚙️ アクション ▾

<input type="checkbox"/>	ノード	ID	IP アドレス	OS タイプ	NSX 設定
<input type="checkbox"/>	▲ New Cluster (2)	MoR...			⚠️ TNP-1
<input type="checkbox"/>	tn-1	926...	10....	ESXi ...	⚠️ 設定が一致しません
<input type="checkbox"/>	tn-2	901f....	10....	ESXi ...	設定済み

前提条件

- アンインストール マッピングで使用するための適切なポート グループが設定されていることを確認します。vSphere Distributed Switch の短期ポート グループまたは vSphere 標準スイッチのポート グループを使用する必要があります。

- スタンドアローン ESXi ホストのアンインストール マッピングで vSphere Distributed Switch のポート グループを使用する場合は、コンピュート マネージャを設定します。[コンピュート マネージャの追加](#) を参照してください。コンピュート マネージャが設定されていない場合は、vSphere 標準スイッチのポート グループを使用する必要があります。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 アンインストールする各ホストについて、アンインストールのためのネットワーク マッピングに、N-VDS 上の各 VMkernel インターフェイスのポート グループが含まれていることを確認します。不足しているマッピングを追加します。

重要： アンインストールのためのネットワーク マッピング内のポート グループは、vSphere Distributed Switch の短期ポート グループまたは vSphere 標準スイッチのポート グループである必要があります。

- a VMkernel インターフェイスを表示するには、vCenter Server にログインし、ホストを選択して [設定] - [VMkernel アダプタ] をクリックします。
- b トランスポート ノード構成がアクティブ構成の場合は、ホストを選択して [編集]（スタンドアローン ホストの場合）または [NSX の設定]（管理対象ホストの場合）をクリックします。[次へ] をクリックして、[アンインストール用のネットワーク マッピング] をクリックします。[vmknics のマッピング] タブと [物理 NIC のマッピング] タブでマッピングを確認します。
- c トランスポート ノード プロファイルがアクティブ構成の場合は、[NSX 設定] 列でクラスタのトランスポート ノード プロファイルの名前をクリックして、[編集] をクリックします。[N-VDS] タブで、[アンインストール用のネットワーク マッピング] をクリックします。[vmknics のマッピング] タブと [物理 NIC のマッピング] タブでマッピングを確認します。

vSphere クラスタからの NSX-T Data Center のアンインストール

トランスポート ノード プロファイルを使用して vSphere クラスタに NSX-T Data Center をインストールしている場合は、次の手順に従って、クラスタ内のすべてのホストから NSX-T Data Center をアンインストールできます。

トランスポート ノード プロファイルの詳細については、[トランスポート ノード プロファイルの追加](#) を参照してください。

注意： 物理インターフェイスまたは VMkernel インターフェイスが N-VDS に接続されている場合、ESXi ホストから NSX-T Data Center をアンインストールする影響が出る場合があります。ホストまたはクラスタが vSAN などの他のアプリケーションに参加している場合、それらのアプリケーションはアンインストールの影響を受ける可能性があります。

トランスポート ノード プロファイルを使用して NSX-T Data Center をインストールしていない場合、またはクラスタ内のホストのサブセットから NSX-T Data Center を削除する場合は、[vSphere クラスタ内のホストからの NSX-T Data Center のアンインストール](#)を参照してください。

注： クラスタからホストを削除しても、NSX-T Data Center はアンインストールされません。クラスタ内のホストから NSX-T Data Center をアンインストールする場合は、[vSphere クラスタ内のホストからの NSX-T Data Center のアンインストール](#)を参照してください。

前提条件

- アンインストールするホストで、ネットワーク アンインストール マッピングが設定されていることを確認します。[アンインストールのためのホスト ネットワーク マッピングの確認](#) を参照してください。
- vSphere で、アンインストールするホストがメンテナンス モードになっていることを確認します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 [管理元] ドロップダウン メニューから vCenter Server を選択します。
- 4 アンインストールするクラスタを選択し、[NSX の削除] をクリックします。
- 5 NSX-T Data Center ソフトウェアがホストから削除されていることを確認します。
 - a ホストのコマンドライン インターフェイスに root としてログインします。
 - b 次のコマンドを実行して、NSX-T Data Center VIB を確認します。

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

NSX-T Data Center ソフトウェアが正常に削除されている場合、VIB は表示されません。いずれかの NSX VIB がホストに残っている場合は、VMware サポートにお問い合わせください。

- 6 ホストに NSX Intelligence が展開されている場合、すべてのトランスポート ノードがデフォルトのネットワーク セキュリティ グループに含まれるため、NSX-T Data Center のアンインストールは失敗します。アンインストールするには：
 - a クラスタを選択して、[NSX の削除] をクリックします。
 - b 確認のポップアップ ウィンドウで、[強制的に削除] を選択します。
 クラスタ内のすべてのホストから NSX-T がアンインストールされます。

vSphere クラスタ内のホストからの NSX-T Data Center のアンインストール

NSX-T Data Center は、vCenter Server によって管理されている単一のホストからアンインストールできます。クラスタ内の他のホストは影響を受けません。

注意： 物理インターフェイスまたは VMkernel インターフェイスが N-VDS に接続されている場合、ESXi ホストから NSX-T Data Center をアンインストールする影響が出る場合があります。ホストまたはクラスタが vSAN などの他のアプリケーションに参加している場合、それらのアプリケーションはアンインストールの影響を受ける可能性があります。

前提条件

- アンインストールするホストで、ネットワーク アンインストール マッピングが設定されていることを確認します。[アンインストールのためのホスト ネットワーク マッピングの確認](#) を参照してください。
- vSphere で、アンインストールするホストがメンテナンス モードになっていることを確認します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 [管理元] ドロップダウン メニューから vCenter Server を選択します。

- 4 クラスタにトランスポート ノード プロファイルが適用されている場合は、クラスタを選択し、[アクション] - [トランスポート ノード プロファイルを切断] の順にクリックします。

クラスタにトランスポート ノード プロファイルが適用されている場合、クラスタの [NSX 設定] 列にプロファイル名が表示されます。

- 5 ホストを選択し、[NSX の削除] をクリックします。
- 6 NSX-T Data Center ソフトウェアがホストから削除されていることを確認します。
 - a ホストのコマンドライン インターフェイスに root としてログインします。
 - b 次のコマンドを実行して、NSX-T Data Center VIB を確認します。

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

NSX-T Data Center ソフトウェアが正常に削除されている場合、VIB は表示されません。いずれかの NSX VIB がホストに残っている場合は、VMware サポートにお問い合わせください。

- 7 クラスタに適用されていたトランスポート ノード プロファイルを再適用する場合は、クラスタを選択し、[NSX の設定] をクリックして、[展開プロファイルの選択] ドロップダウン メニューからプロファイルを選択します。

スタンドアローン ホストからの NSX-T Data Center のアンインストール

スタンドアローン ホストから NSX-T Data Center をアンインストールできます。スタンドアローン ホストには、ESXi または KVM があります。

注意： 物理インターフェイスまたは VMkernel インターフェイスが N-VDS に接続されている場合、ESXi ホストから NSX-T Data Center をアンインストールする影響が出る場合があります。ホストまたはクラスタが vSAN などの他のアプリケーションに参加している場合、それらのアプリケーションはアンインストールの影響を受ける可能性があります。

前提条件

スタンドアローン ESXi ホストから NSX-T Data Center をアンインストールする場合は、次の設定を確認します。

- アンインストールするホストで、ネットワーク アンインストール マッピングが設定されていることを確認します。[アンインストールのためのホスト ネットワーク マッピングの確認](#) を参照してください。
- vSphere で、アンインストールするホストがメンテナンス モードになっていることを確認します。

手順

- 1 ブラウザから、NSX Manager (<https://<nsx-manager-ip-address>>) に管理者権限でログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] を選択します。
- 3 [管理元] ドロップダウン メニューから [なし: スタンドアローン ホスト] を選択します。
- 4 ホストを選択し、[削除] をクリックします。表示された確認ダイアログ ボックスで、[NSX コンポーネントのアンインストール] が選択され、[強制的に削除] が選択解除されていることを確認します。[削除] をクリックします。

NSX-T Data Center ソフトウェアがホストから削除されます。すべての NSX-T Data Center ソフトウェアが削除されるまで、最大で 5 分程度かかる場合があります。

- 5 アンインストールに失敗した場合は、ホストを選択して [削除] を再度クリックします。確認ダイアログ ボックスで、[NSX コンポーネントのアンインストール] を選択解除し、[強制的に削除] を選択します。

ホスト トランスポート ノードは管理プレーンから削除されますが、ホストにはまだ NSX-T Data Center ソフトウェアがインストールされている可能性があります。

- 6 NSX-T Data Center ソフトウェアがホストから削除されていることを確認します。
- ホストのコマンドライン インターフェイスに root としてログインします。
 - 適切なコマンドを実行して、NSX-T Data Center ソフトウェア パッケージを確認します。

表 12-1. パッケージ リスト コマンド

ホスト OS	コマンド
ESXi	<pre>esxcli software vib list grep -E 'nsx vsipfwlib'</pre>
Red Hat Enterprise Linux と CentOS Linux	<pre>rpm -qa grep -E 'nsx vsipfwlib'</pre>
Ubuntu	<pre>dpkg -l grep -E 'nsx vsipfwlib'</pre>
SUSE Linux Enterprise Server	<pre>zypper packages --installed-only grep -E 'nsx vsipfwlib'</pre>

NSX-T Data Center ソフトウェアが正常に削除されている場合、パッケージは表示されません。いずれかの NSX ソフトウェア パッケージがホストに残っている場合は、VMware のサポートにお問い合わせください。

NSX Cloud コンポーネントのインストール

13

NSX Cloud には、複数のパブリック クラウド ネットワークを 1 つの画面で管理するための機能を提供します。

NSX Cloud は、プロバイダ固有のネットワークに依存せず、パブリック クラウドでのハイパーバイザーへのアクセスを必要としません。

また、次のようなメリットがあります。

- 本番環境で使用するものと同じネットワーク プロファイルやセキュリティ プロファイルを使用して、アプリケーションの開発およびテストを実施できます。
- 開発者は、開発中のアプリケーションを開発が終わるまで管理できます。
- ディザスタ リカバリによって、計画外の停止や、パブリック クラウドで発生したセキュリティの脅威からリカバリできます。
- パブリック クラウド間でワークロードを移行する場合、NSX Cloud では、移行先がどこであっても、ワークロード仮想マシンに類似のセキュリティ ポリシーを確実に適用できます。

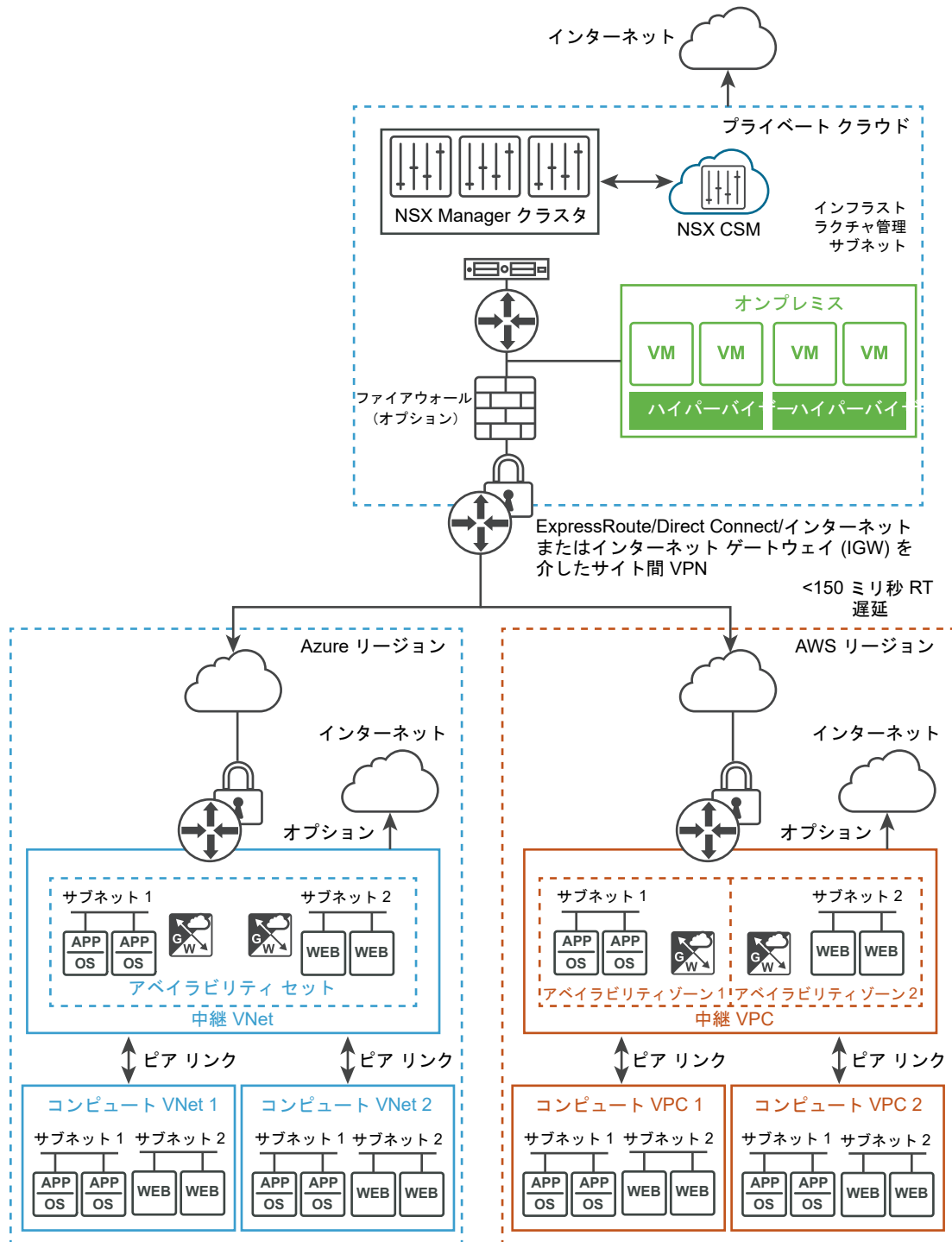
この章には、次のトピックが含まれています。

- [NSX Cloud のアーキテクチャとコンポーネント](#)
- [NSX Cloud の展開の概要](#)
- [NSX-T Data Center オンプレミス コンポーネントの展開](#)
- [パブリック クラウド アカウントの追加](#)
- [NSX Public Cloud Gateway の展開](#)
- [（オプション）ワークロード仮想マシンへの NSX Tools のインストール](#)
- [PCG の展開解除またはリンク解除](#)

NSX Cloud のアーキテクチャとコンポーネント

NSX Cloud は、NSX-T Data Center コア コンポーネントをパブリック クラウドに統合することで、実装環境全体にネットワークとセキュリティを提供します。

図 13-1. NSX Cloud アーキテクチャ



コア コンポーネント

NSX Cloud の主要なコンポーネントは次のとおりです。

- **[NSX Manager] :** ポリシー ベースのルーティングを使用する管理プレーン、ロール ベースのアクセス コントロール (RBAC)、制御プレーンおよびランタイム状態の定義に使用。

- [Cloud Service Manager (CSM)] : NSX Manager に組み込み、管理プレーンにパブリック クラウドに固有の情報を提供。
- [Public Cloud Gateway (PCG)] : NSX の管理プレーンと制御プレーン、NSX Edge Gateway Service との接続、およびパブリック クラウド エンティティとの API ベースの通信を提供。
- [NSX Tools] : ワークロード仮想マシンに NSX が管理するデータベースを提供。

NSX Cloud の展開の概要

NSX Cloud コンポーネントをインストールして設定し、NSX-T Data Center がパブリック クラウド ワークロード仮想マシンを管理できるようにするプロセスについては、この概要を参照してください。



注： 展開の計画中に、オンプレミスの NSX-T Data Center アプライアンスがパブリック クラウドに展開された PCG との接続され、トランジット VPC/VNet がコンピュータ VPC/VNet と同じリージョンにあることを確認します。

表 13-1. NSX Cloud の展開ワークフロー

タスク	方法
<input type="checkbox"/> CSM をインストールして NSX Manager と接続します。	NSX-T Data Center オンプレミス コンポーネントの展開 を参照してください。
<input type="checkbox"/> CSM で 1 つ以上のパブリック クラウド アカウントを追加します。	パブリック クラウド アカウントの追加 を参照してください。
<input type="checkbox"/> トランジット VPC または VNet 内で PCG を展開し、コンピュータ VPC または VNet にリンクします。	NSX Public Cloud Gateway の展開 を参照してください。
次の手順	『NSX-T Data Center 管理ガイド』の NSX Cloud の使用の手順 に沿って操作します。

NSX-T Data Center オンプレミス コンポーネントの展開

CSM のインストールを続行するには、NSX Manager がインストールされている必要があります。

CSM のインストール

Cloud Service Manager (CSM) は、NSX Cloud のコア コンポーネントです。

NSX Manager をインストールした後、NSX Manager のインストールと同じ手順を行い、仮想マシン ロールとして [nsx-cloud-service-manager] を選択して、CSM をインストールします。手順については、[NSX Manager および利用可能なアプライアンスのインストール](#)を参照してください。

必要に応じて、極小規模以上の仮想マシンに CSM を展開できます。詳細については、[NSX Manager 仮想マシンとホスト トランスポート ノードのシステム要件](#)を参照してください。

NSX Manager への CSM の追加

CSM アプライアンスと NSX Manager を接続して、これらのコンポーネントが相互通信できるようにする必要があります。

前提条件

- NSX Manager がインストールされていて、NSX Manager に管理者アカウントでログインするためのユーザー名とパスワードが必要です。
- CSM がインストール済みで、エンタープライズ管理者ロールが CSM に割り当てられている必要があります。

手順

- 1 ブラウザから CSM にログインします。
- 2 セットアップ ウィザードでプロンプトが表示されたら、[設定の開始] をクリックします。
- 3 [NSX Manager の認証情報] 画面で、次の詳細を入力します。

オプション	説明
NSX Manager のホスト名	NSX Manager の完全修飾ドメイン名 (FQDN) を入力します (分かっている場合)。NSX Manager の IP アドレスを入力することもできます。
管理者認証情報	NSX Manager のエンタープライズ管理者のユーザー名とパスワードを入力します。
NSX Manager のサムプリント	オプションで NSX Manager のサムプリント値を入力します。このフィールドを空白のままにすると、システムはサムプリントを識別し、次の画面に表示します。

- 4 (オプション) NSX Manager にサムプリント値を指定しなかった場合、または値が正しくない場合は、[サムプリントの確認] 画面が表示されます。チェック ボックスを選択し、システムによって検出されたサムプリントを受け入れます。
- 5 [接続] をクリックします。

注： セットアップ ウィザードでこの設定をしなかった場合、または関連付けられた NSX Manager を変更する場合は、CSM にログインし、[システム] - [設定] の順にクリックし、[関連付けられた NSX ノード] というパネルで [構成] をクリックします。

CSM は、NSX Manager のサムプリントを確認して、接続を確立します。

- 6 (オプション) プロキシ サーバを設定します。[\(オプション\) プロキシ サーバの設定](#)の手順を参照してください。

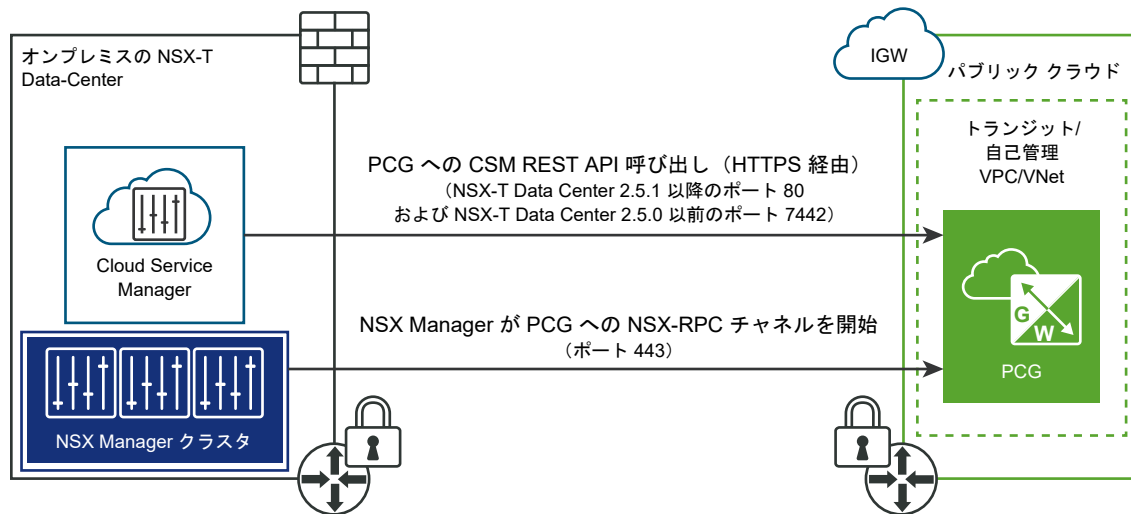
ポートとプロトコルへのアクセスの有効化

パブリック クラウド接続を有効にするために、NSX-T Data Center のオンプレミス環境で受信ポートを開く必要はありません。

次の送信ポートが必要です。

表 13-2. NSX-T Data Center とのパブリック クラウド接続に必要なポートとプロトコル

送信元	宛先	ポート	プロトコル	目的:
CSM	PCG	80 <small>注: NSX-T Data Center バージョン 2.5.0 を使用している場合は、代わりに非標準ポート 7442 を開き、SSL トラフィックがファイアウォールを通過するようにする必要があります。</small>	TCP	HTTPS を介した、アップグレード ワークフローなどの CSM の設定。
NSX Manager	PCG	443	TCP	NSX RPC チャネル。
CSM	NSX Manager	443	TCP	CSM からの NSX Manager へのアクセス。オンプレミスの展開の詳細については、 ポートとプロトコル を参照してください。



(オプション) プロキシ サーバの設定

信頼性の高い HTTP プロキシを介してインターネットに向かうすべての HTTP/HTTPS トラフィックをルーティングして監視する場合は、CSM で最大 5 台のプロキシ サーバを構成できます。

PCG および CSM からのすべてのパブリック クラウド通信は、選択したプロキシ サーバを介してルーティングされます。

PCG のプロキシ設定は CSM のプロキシ設定とは独立しています。PCG にプロキシ サーバを設定しないか、または異なるプロキシ サーバを設定することができます。

次のレベルの認証を選択できます。

- 認証情報ベースの認証。
- HTTPS インターセプトの証明書ベースの認証。
- 認証なし。

手順

- 1 [システム] - [設定] の順にクリックします。次に、[プロキシ サーバ] パネルの [設定] をクリックします。

注： これらの詳細は、CSM セットアップ ウィザードを使用する際にも指定できます。セットアップ ウィザードは CSM の初回インストール時に使用できます。

- 2 プロキシ サーバの設定画面で、次の詳細を入力します。

オプション	説明
デフォルト	このラジオ ボタンは、デフォルトのプロキシ サーバを指定する場合に使用します。
プロファイル名	プロキシ サーバ プロファイルの名前を指定します。このオプションは必須です。
プロキシ サーバ	プロキシ サーバの IP アドレスを入力します。このオプションは必須です。
ポート	プロキシ サーバのポートを入力します。このオプションは必須です。
認証	任意。追加認証を設定する場合は、このチェック ボックスを選択して、有効なユーザー名とパスワードを入力します。
ユーザー名	[認証] チェック ボックスを選択した場合は、必須です。
パスワード	[認証] チェック ボックスを選択した場合は、必須です。
証明書	任意。HTTPS インターセプトの認証証明書を指定する場合は、このチェックボックスを選択して、表示されたテキスト ボックスに証明書をコピーして貼り付けします。
プロキシなし	設定されているプロキシ サーバのいずれも使用しない場合は、このオプションを選択します。

(オプション) Cloud Service Manager の vIDM の設定

VMware Identity Manager を使用する場合は、NSX Manager 内から CSM にアクセスするように設定できます。

手順

- 1 NSX Manager と CSM に vIDM を構成します。手順については、『NSX-T Data Center 管理ガイド』の [VMware Identity Manager Integration の設定](#) を参照してください。
- 2 NSX Manager と CSM の vIDM ユーザーに同じロールを割り当てます。たとえば、**vIDM_admin** というユーザーに [エンタープライズ管理者] ロールを割り当てます。NSX Manager と CSM にそれぞれログインして、同じユーザー名に同じロールを割り当てる必要があります。詳細な手順については、『NSX-T Data Center 管理ガイド』の [ロールの割り当てまたはプリンシパル ID の追加](#) を参照してください。
- 3 NSX Manager にログインします。vIDM ログインにリダイレクトされます。

- 4 vIDM ユーザーの認証情報を入力します。ログインすると、アプリケーションのアイコンをクリックして NSX Manager と CSM を切り替えることができます。



パブリック クラウド アカウントの追加

パブリック クラウド インベントリを追加するには、パブリック クラウド アカウントをオンプレミス環境の NSX-T Data Center に接続し、VPC/VNet 内に必要なサブネットを作成して、NSX Cloud へのアクセスを許可するルールをパブリック クラウドに作成する必要があります。

これらの手順に決められた順番はありません。個別に行うこともできます。

注：

- 適切な方法で VPC/VNet をオンプレミスに接続します。たとえば、AWS の場合は Direct Connect、Microsoft Azure の場合は ExpressRoute を使用します。また、オンプレミスの VPN エンドポイントとパブリック クラウドで VPN エンドポイントとして機能する PCG を使用して、サイト間 VPN を確立することもできます。
- トランジット/コンピューティング トポロジを選択した場合は、トランジットとコンピューティング VPC/VNet 間にピアリング接続が確立されていることを確認します。1つの PCG で複数のコンピューティング VPC/VNet を管理できます。各 VPC/VNet に PCG ペアがインストールされているフラットなコンピューティング VPC/VNet アーキテクチャを選択することもできます。

Microsoft Azure ネットワークとオンプレミス NSX-T Data Center 環境の接続

Microsoft Azure ネットワークとオンプレミスの NSX-T Data Center アプライアンス間に接続を確立する必要があります。

注： NSX Manager がインストールされ、オンプレミス環境内の CSM と接続されている必要があります。

概要

- Microsoft Azure サブスクリプションとオンプレミス NSX-T Data Center を接続します。
- VNet を、NSX Cloud で必要な CIDR ブロックおよびサブネットで構成します。
- CSM アプライアンスの時刻を、Microsoft Azure Storage サーバまたは NTP と同期させます。

Microsoft Azure サブスクリプションとオンプレミス NSX-T Data Center との接続

すべてのパブリック クラウドに、オンプレミス環境に接続するためのオプションが提供されています。要件に合わせて、使用可能な接続オプションのいずれかを選択できます。詳細については、Microsoft Azure のリファレンス ドキュメントを参照してください。

注： Microsoft Azure によるセキュリティ上の考慮事項とベスト プラクティスを確認して実装する必要があります。たとえば、Microsoft Azure ポータルまたは API へのアクセス権を持つすべてのユーザー アカウントには、多要素認証 (MFA) を有効にする必要があります。多要素認証によって認証されたユーザーのみがポータルにアクセスできるようになると、認証情報が盗まれたり漏洩した場合でも、不正にアクセスされる可能性が低減します。詳細な情報および推奨事項については、Microsoft Azure Security Center のドキュメントを参照してください。

VNet の構成

Microsoft Azure で、ルーティング可能な CIDR ブロックを作成し、必要なサブネットを設定します。

- 1つの管理サブネット。推奨範囲は /28 以上で次のトラフィックに使用します。
 - オンプレミス アプライアンスへの制御トラフィック
 - クラウド プロバイダ API エンドポイントへの API トラフィック
- 1つのダウンリンク サブネット。推奨範囲は /24 で、ワークロードワークロード仮想マシンに使用します。
- 1つのアップリンク サブネット (HA の場合は 2 つ)。推奨範囲は /24 で、VNet で送受信される North-South トラフィックのルーティングに使用します。

これらのサブネットの使用方法の詳細については、[NSX Public Cloud Gateway の展開](#) を参照してください。

Microsoft Azure インベントリへの安全なアクセスの設定

NSX Cloud をサブスクリプションで運用するには、Azure リソースの ID を管理するための Microsoft Azure 機能に基づいて、必要な権限および CSM と PCG のロールを付与するサービス プリンシパルを作成します。

[概要]：

- Microsoft Azure サブスクリプションには、NSX-T Data Center の管理下に置くことができる 1 つ以上の VNet が含まれています。VNet はトランジット モードの場合またはコンピューティング モードの場合があります。トランジット VNet は PCG を展開する場所です。他の VNet をトランジット VNet にリンクして、ホストされているワークロード仮想マシンをオンボーディングできます。トランジット VNet にリンクされた VNet は コンピューティング VNet と呼ばれます。
- NSX Cloud が提供する PowerShell スクリプトにより、サービス プリンシパルとロールを作成できます。これらは、Microsoft Azure の認証情報のセキュリティを確保すると同時に、Microsoft Azure の管理 ID 機能を使用して認証を管理します。このスクリプトを使用して、1 つのサービス プリンシパルに複数のサブスクリプションを含めることもできます。
- 必要に応じて、すべてのサブスクリプションでサービス プリンシパルを再利用するか、新しいサービス プリンシパルを作成するかを選択できます。追加したサブスクリプションで、異なるサービス プリンシパルを作成する場合は、別のスクリプトを使用します。
- サブスクリプションが複数の場合、サブスクリプションで使用するサービス プリンシパルが 1 つであっても、複数であっても、CSM ロールと PCG ロールの JSON ファイルを更新して、セクション *AssignableScopes* に各サブスクリプション名を追加する必要があります。

- VNet にすでに NSX Cloud サービス プリンシパルがある場合は、スクリプトを再度実行してパラメータから サービス プリンシパル名を除外することで更新できます。
- サービス プリンシパル名は、Microsoft Azure Active Directory に対して一意である必要があります。同一の Active Directory ドメイン内の異なるサブスクリプションに同じサービス プリンシパルを使用することも、サブスクリプションごとに異なるサービス プリンシパルを使用することもできます。ただし、同じ名前のサービス プリンシパルを 2 つ作成することはできません。
- Microsoft Azure サブスクリプションの所有者であるか、すべての Microsoft Azure サブスクリプションで ロールを作成し割り当てる権限を持っている必要があります。
- 次のシナリオがサポートされます。
 - [シナリオ 1:] 1 つの Microsoft Azure サブスクリプションを NSX Cloud で有効にする。
 - [シナリオ 2:] 同じ Microsoft Azure Directory に、NSX Cloud で有効にする複数の Microsoft Azure サブスクリプションがあり、すべてのサブスクリプションで 1 つの NSX Cloud サービス プリンシパルを使用する。
 - [シナリオ 3:] 同じ Microsoft Azure Directory に、NSX Cloud で有効にする複数の Microsoft Azure サブスクリプションがあり、それぞれのサブスクリプションで異なる NSX Cloud サービス プリンシパルを使用する。

プロセスの概要は、以下の通りです。

- 1 NSX Cloud PowerShell スクリプトを使用して以下を実行します。
 - NSX Cloud のサービス プリンシパル アカウントを作成します。
 - CSM のロールを作成します。
 - PCG のロールを作成します。
- 2 (オプション) リンクする他のサブスクリプションのサービス プリンシパルを作成します。
- 3 CSM で Microsoft Azure サブスクリプションを追加します。

注： 複数のサブスクリプションを使用している場合は、サービス プリンシパルが同一か異なるかにかかわらず、CSM に各サブスクリプションを個別に追加する必要があります。

サービス プリンシパルとロールの生成

NSX Cloud は、1 つ以上の複数のサブスクリプションに必要なサービス プリンシパルとロールを生成するのに役立つ PowerShell スクリプトを提供します。

前提条件

- AzureRM モジュールがインストールされた PowerShell 5.0 以上が必要です。
- Microsoft Azure サブスクリプションの所有者であるか、すべての Microsoft Azure サブスクリプションで ロールを作成し割り当てる権限を持っている必要があります。

注： Microsoft Azure からの応答時間によって、スクリプトの初回実行時にスクリプトが失敗する可能性があります。スクリプトが失敗した場合は、再度実行してください。

手順

- 1 Windows デスクトップまたはサーバで、NSX-T Data Center の [ダウンロード] ページ > [ドライバとツール] > [NSX Cloud スクリプト] > [Microsoft Azure] の順に移動して、CreateNSXCloudCredentials.zip という名前の ZIP ファイルをダウンロードします。
- 2 Windows システムで、ZIP ファイルの次の内容を展開します。

スクリプト/ファイル	説明
CreateNSXRoles.ps1	<p>CSM および PCG の NSX Cloud サービス プリンシパルおよび管理対象 ID ロールを生成するための PowerShell スクリプトです。このスクリプトには次のパラメータを使用します。</p> <ul style="list-style-type: none"> ■ -subscriptionId <the Transit_VNet's_Azure_subscription_ID> ■ (オプション) -servicePrincipalName <Service_Principal_Name> ■ (オプション) -useOneServicePrincipal
AddServicePrincipal.ps1	<p>複数のサブスクリプションを追加し、各サブスクリプションに異なるサービス プリンシパルを割り当てる場合に必要となる、オプションのスクリプトです。次の手順の、[シナリオ 3] を参照してください。このスクリプトには次のパラメータを使用します。</p> <ul style="list-style-type: none"> ■ -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID> ■ -transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID> ■ -csmRoleName <CSM_Role_Name> ■ -servicePrincipalName <Service_Principal_Name>
nsx_csm_role.json	<p>CSM のロール名と権限の JSON テンプレートです。このファイルは、PowerShell スクリプトに入力され、スクリプトと同じフォルダに配置されている必要があります。</p>
nsx_pcg_role.json	<p>PCG のロール名と権限の JSON テンプレートです。このファイルは、PowerShell スクリプトに入力され、スクリプトと同じフォルダに配置されている必要があります。</p> <p>注： デフォルト PCG (ゲートウェイ) ロール名は nsx-pcg-role です。CSM でサブスクリプションを追加する場合は、この値を指定する必要があります。</p>

- 3 [シナリオ 1:] 1 つの Microsoft Azure サブスクリプションを NSX Cloud で有効にする。
 - a PowerShell インスタンスから、Microsoft Azure スクリプトと JSON ファイルをダウンロードしたディレクトリに移動します。
 - b CreateNSXRoles.ps1 という名前のスクリプトを、パラメータ -SubscriptionId を使用して、次のように指定して実行します。

```
.\CreateNSXRoles.ps1 -subscriptionId <the_single_Azure_subscription_ID>
```

注： デフォルトのサービス プリンシパル名 nsx-service-admin を上書きする場合は、パラメータ -servicePrincipalName を使用することもできます。サービス プリンシパル名は、Microsoft Azure Active Directory 内で一意である必要があります。

- 4 [シナリオ 2:] 同じ Microsoft Azure Directory に、NSX Cloud で有効にする複数の Microsoft Azure サブスクリプションがあり、すべてのサブスクリプションで 1 つの NSX Cloud サービス プリンシパルを使用する。

- a PowerShell インスタンスから、Microsoft Azure スクリプトと JSON ファイルをダウンロードしたディレクトリに移動します。
- b 各 JSON ファイルを編集して、*"AssignableScopes"* というセクションの下に他のサブスクリプション ID のリストを追加します。以下に例を示します。

```
"AssignableScopes": [

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

注： サブスクリプション ID を追加するには、例に示す形式を使用する必要があります： `"/subscriptions/<Subscription_ID>"`

- c CreateNSXRoles.ps1 という名前のスクリプトをパラメータ `-subscriptionID` および `-useOneServicePrincipal` を指定して実行します。

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID>
-useOneServicePrincipal
```

注： デフォルト名 `nsx-service-admin` を使用する場合は、ここでサービス プリンシパル名を省略します。サービス プリンシパル名が Microsoft Azure Active Directory にすでにある場合は、サービス プリンシパル名なしでこのスクリプトを実行します。これにより、サービス プリンシパルが更新されます。

- 5 [シナリオ 3:] 同じ Microsoft Azure Directory に、NSX Cloud で有効にする複数の Microsoft Azure サブスクリプションがあり、それぞれのサブスクリプションで異なる NSX Cloud サービス プリンシパルを使用する。

- a PowerShell インスタンスから、Microsoft Azure スクリプトと JSON ファイルをダウンロードしたディレクトリに移動します。
- b 2 番目のシナリオの手順 [b] と [c] に沿って、各 JSON ファイルの *AssignableScopes* セクションに複数のサブスクリプションを追加します。

- c CreateNSXRoles.ps1 という名前のスクリプトをパラメータ -subscriptionID を指定して実行します。

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

注： デフォルト名 nsx-service-admin を使用する場合は、ここでサービス プリンシパル名を省略します。サービス プリンシパル名が Microsoft Azure Active Directory にある場合は、サービス プリンシパル名なしでこのスクリプトを実行します。これにより、サービス プリンシパルが更新されます。

- d AddServicePrincipal.ps1 という名前のスクリプトを次のパラメータを指定して実行します。

パラメータ	値
-computeSubscriptionId	Compute_VNet の Azure サブスクリプション ID
-transitSubscriptionId	トランジット VNet の Azure サブスクリプション ID
-csmRoleName	ファイル nsx_csm_role.JSON からこの値を取得します
-servicePrincipalName	新しいサービス プリンシパル名

```
./AddServicePrincipal.ps1 -computeSubscriptionId
<the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>
```

- 6 PowerShell スクリプトを実行したディレクトリでファイルを探します。名前は次のようになります：
NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>。このファイルには、CSM で Microsoft Azure サブスクリプションを追加するために必要な情報が含まれています。

- クライアント ID
- クライアント キー
- テナント ID
- サブスクリプション ID

結果

次の構成で作成されます。

- NSX Cloud 用の Azure Active Directory アプリケーション。
- NSX Cloud アプリケーションの Azure Resource Manager サービス プリンシパル。
- サービス プリンシパル アカウントに設定された CSM のロール。
- パブリック クラウド インベントリで機能できるようにする PCG のロール。

- NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name> のような名前のファイルが、PowerShell スクリプトを実行したディレクトリに作成されます。このファイルには、CSM で Microsoft Azure サブスクリプションを追加するために必要な情報が含まれています。

注： CSM ロールと PCG ロールの作成後に使用可能な権限のリストについては、それらのロールの作成に使用される JSON ファイルを参照してください。

次のステップ

CSM での Microsoft Azure サブスクリプションの追加

注： 複数のサブスクリプションに対して NSX Cloud を有効にする場合は、CSM に個別のサブスクリプションを追加する必要があります。たとえば、合計 5 つのサブスクリプションがある場合、CSM に 5 つの Microsoft Azure アカウントを追加する必要があります。サブスクリプション ID 以外はすべて同じ値を設定してください。

CSM での Microsoft Azure サブスクリプションの追加

NSX Cloud のサービス プリンシパルおよび CSM と Public Cloud Gateway (PCG) のロールの詳細情報を入力したら、CSM に Microsoft Azure サブスクリプションを追加できます。

前提条件

- NSX-T Data Center のエンタープライズ管理者ロールが必要です。
- NSX Cloud のサービス プリンシパルの詳細情報が含まれる PowerShell スクリプトの出力が必要です。
- ロールとサービス プリンシパルを作成する際に PowerShell スクリプトを実行したときに提供した PCG ロールの値が必要です。デフォルト値は `nsx-pcg-role` です。

手順

- 1 エンタープライズ管理者ロールを持つアカウントを使用して、CSM にログインします。
- 2 [CSM] - [クラウド] - [Azure] の順に移動します。
- 3 [+ (追加)] マークをクリックし、次の詳細を入力します。

オプション	説明
名前	CSM で、アカウントを識別するための適切な名前を指定します。1 つの Microsoft Azure テナント ID に、複数の Microsoft Azure サブスクリプションが関連付けられている場合があります。アカウント名に「Account」を含めると、CSM 内で分かりやすい名前になります。たとえば、Azure-DevOps-Account や Azure-Finance-Account などにします。
クライアント ID	PowerShell スクリプトの出力からこの値をコピーして、貼り付けます。
キー	PowerShell スクリプトの出力からこの値をコピーして、貼り付けます。
サブスクリプション ID	PowerShell スクリプトの出力からこの値をコピーして、貼り付けます。
テナント ID	PowerShell スクリプトの出力からこの値をコピーして、貼り付けます。

オプション	説明
ゲートウェイ ロール名	デフォルト値は <code>nsx-pcg-role</code> です。デフォルトを変更した場合、この値は <code>nsx_pcg_role.json</code> ファイルから取得できます。
クラウド タグ	デフォルトではこのオプションが有効になっており、Microsoft Azure タグを NSX Manager に表示することができます。

4 [保存] をクリックします。

CSM でアカウントが追加されて、3 分以内に [アカウント] セクションに表示されます。

- 5 仮想マシンを管理する VNet 内のすべての仮想マシンをホワイトリストに追加します。これは必須ではありません。ただし、既存環境に展開する場合、検疫ポリシーを無効から有効にすると影響が生じるため、このように設定することをおすすめします。

次のステップ

VNet での PCG の展開

Amazon Web Services (AWS) ネットワークとオンプレミス NSX-T Data Center 環境の接続

Amazon Web Services (AWS) ネットワークとオンプレミスの NSX-T Data Center アプライアンス間に接続を確立する必要があります。

注： NSX Manager がインストールされ、オンプレミス環境内の CSM と接続されている必要があります。

概要

- 要件に合わせて使用可能なオプションのいずれかを使用して、AWS アカウントとオンプレミスの NSX Manager アプライアンスを接続します。
- Virtual Private Cloud (VPC) をサブネットおよび NSX Cloud の他の要件とともに構成します。

AWS アカウントのオンプレミスの NSX-T Data Center 環境への接続

すべてのパブリック クラウドに、オンプレミス環境に接続するためのオプションが提供されています。要件に合わせて、使用可能な接続オプションのいずれかを選択できます。詳細については、AWS のリファレンス ドキュメントを参照してください。

注： AWS によるセキュリティ上の考慮事項とベスト プラクティスを確認して実装する必要があります。AWS セキュリティのベスト プラクティスを参照してください。

Virtual Private Cloud (VPC) の構成

次の構成が必要です。

- 高可用性を備えた PCG をサポートするための 6 つのサブネット
- インターネット ゲートウェイ (IGW)

- プライベート ルート テーブルおよびパブリック ルート テーブル
- サブネットとルート テーブルの関連付け
- 有効な DNS 解決と DNS ホスト名

次のガイドラインの指示のとおり VPC を構成してください。

- 1 VPC は /16 ネットワークを使用し、展開する必要があるゲートウェイごとに 3 つのサブネットを設定します。

重要： 高可用性を使用する場合は、別のアベイラビリティ ゾーンで、追加の 3 つのサブネットを設定します。

- [管理サブネット]: このサブネットは、オンプレミス NSX-T Data Center と PCG 間の管理トラフィックに使用されます。推奨レンジは、/28 です。
- [アップリンク サブネット]: このサブネットは、North-South のインターネット トラフィックに使用されます。推奨レンジは、/24 です。
- [ダウンリンク サブネット]: このサブネットは、ワークロード仮想マシンの IP アドレス範囲を含んでおり、それに応じてサイズ調整する必要があります。デバッグのため、ワークロード仮想マシンに追加のインターフェイスを組み込む必要がある点に留意してください。

注： この VPC に PCG を展開する際にサブネットを選択する必要があるため、サブネットに適宜ラベルを付けます。たとえば、**management-subnet**、**uplink-subnet**、**downlink-subnet** などとします。

詳細については、[NSX Public Cloud Gateway の展開](#) を参照してください。

- 2 この VPC にインターネット ゲートウェイ (IGW) が接続されていることを確認します。
- 3 VPC のルーティング テーブルで [宛先] が **0.0.0.0/0** に設定され、[ターゲット] は VPC に接続されているインターネット ゲートウェイであることを確認します。
- 4 この VPC で DNS 解決が使用され、DNS ホスト名が有効であることを確認します。

AWS インベントリへの安全なアクセスの設定

VPC とワークロード仮想マシンを持つ 1 つ以上の AWS アカウントを NSX-T Data Center で管理することができます。

[概要]:

- トランジット/コンピューティング VPC トポロジを使用すると、1 つの VPC に PCG を展開してそれをトランジット VPC にし、他の VPC をそれにリンクしてコンピューティング VPC にすることができます。
- NSX Cloud は、AWS アカウントの AWS CLI から実行できるシェル スクリプトを提供します。これにより、IAM プロファイルとロールを作成し、トランジット VPC と コンピューティング VPC の信頼関係を作成します。
- 次のシナリオがサポートされます。
 - [シナリオ 1:] NSX Cloud で 1 つの AWS アカウントを使用する。
 - [シナリオ 2:] 1 つのマスター AWS アカウントで管理されている複数のサブアカウントを AWS で使用する。

- [シナリオ 3:] NSX Cloud で複数の AWS アカウントを使用する。

プロセスの概要は、以下の通りです。

1 AWS CLI から、NSX Cloud シェル スクリプトを使用して、次の手順を実行します。

- IAM プロファイルを作成します。
- PCG のロールを作成します。
- (オプション) トランジット VPC をホストする AWS アカウントとコンピューティング VPC をホストする AWS アカウントの間に信頼関係を作成します。

2 CSM で AWS アカウントを追加します。

IAM プロファイルと PCG ロールの生成

NSX Cloud は、1 つ以上の AWS アカウントを設定するのに役立つ SHELL スクリプトを提供します。これにより、AWS アカウントに必要な権限を提供するプロファイルに添付された PCG の IAM プロファイルとロールを生成します。

2 つの異なる AWS アカウントで複数のコンピューティング VPC にリンクされたトランジット VPC をホストする場合は、スクリプトを使用してアカウント間の信頼関係を作成できます。

注： PCG (ゲートウェイ) ロール名は、デフォルトで `nsx_pcg_service` です。ゲートウェイ ロール名に別の値を設定する場合はスクリプトで変更できます。ただし、CSM に AWS アカウントを追加するときに必要となるため、このデフォルト名はメモしておいてください。

前提条件

スクリプトを実行する前に、Linux またはその互換システムに以下をインストールして設定しておく必要があります。

- AWS CLI
- jq (JSON パーサー)
- openssl

注： 複数の AWS アカウントを使用している場合は、適切な方法を使用してアカウントをピアリングする必要があります。

手順

1 Linux または互換性のあるデスクトップまたはサーバで、NSX-T Data Center の [ダウンロード] 画面 > [ドライバとツール] > [NSX Cloud スクリプト] > [AWS] の順に移動して、`nsx_csm_iam_script.sh` という名前のシェル スクリプトをダウンロードします。

2 [シナリオ 1:] NSX Cloud で 1 つの AWS アカウントを使用する。

- a たとえば、次のスクリプトを実行します。

```
bash nsx_csm_iam_script.sh
```

- b 「Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no] 」という質問が表示されたら、「yes」と入力します。
- c 「What do you want to name the IAM User?」という質問が表示されたら、IAM ユーザーの名前を入力します。

注： IAM ユーザー名は、AWS アカウント内で一意である必要があります。

- d 「Do you want to add trust relationship for any Transit VPC account? [yes/no] 」という質問が表示されたら、「no」と入力します。

スクリプトが正常に実行されると、PCG の IAM プロファイルとロールが AWS アカウントに作成されます。値は、スクリプトが実行されたのと同じディレクトリの出力ファイル `aws_details.txt` に保存されます。次に、[CSM での AWS アカウントの追加](#)の手順を実行してから、[VPC での PCG の展開](#)の手順を実行し、トランジットまたは自己管理 VPC を設定します。

3 [シナリオ 2:] 1 つのマスター AWS アカウントで管理されている複数のサブアカウントを AWS で使用する。

- a AWS マスター アカウントからスクリプトを実行します。

```
bash nsx_csm_iam_script.sh
```

- b 「Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no] 」という質問が表示されたら、「yes」と入力します。
- c 「What do you want to name the IAM User?」という質問が表示されたら、IAM ユーザーの名前を入力します。

注： IAM ユーザー名は、AWS アカウント内で一意である必要があります。

- d 「Do you want to add trust relationship for any Transit VPC account? [yes/no] 」という質問が表示されたら、「no」と入力します。

注： マスター AWS アカウントでは、トランジット VPC にサブアカウントのコンピュート VPC を表示する権限がある場合、サブアカウントとの信頼関係を確立する必要はありません。権限がない場合は、[シナリオ 3] の手順に沿って複数のアカウントを設定します。

スクリプトが正常に実行されると、PCG の IAM プロファイルとロールが AWS マスター アカウントに作成されます。値は、スクリプトが実行されたディレクトリの出力ファイルに保存されます。ファイル名は `aws_details.txt` です。次に、[CSM での AWS アカウントの追加](#)の手順を実行してから、[VPC での PCG の展開](#)の手順を実行し、トランジットまたは自己管理 VPC を設定します。

4 [シナリオ 3:] NSX Cloud で複数の AWS アカウントを使用する。

注： 続行する前に、AWS アカウントがピアリングされていることを確認します。

- a トランジット VPC をホストする場合の 12 桁の AWS アカウント番号をメモしておきます。
- b シナリオ 1 の a から d の手順に沿って AWS アカウントにトランジット VPC を設定し、CSM へのアカウントの追加を終了します。
- c コンピュート VPC をホストする他の AWS アカウントで、Linux またはその互換システムから NSX Cloud スクリプトをダウンロードして実行します。

注： あるいは、異なるアカウント認証情報の AWS プロファイルを使用し、同じシステムを使用して他の AWS アカウントに対してスクリプトを再実行することもできます。

- d 「Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no] 」という質問が表示されたら、「yes」と入力します。

注： この AWS アカウントをすでに CSM に追加していて、スクリプトを再利用して別の AWS アカウントに接続する場合は、「no」と入力して IAM ユーザーの作成をスキップできます。

- e 「What do you want to name the IAM User?」という質問が表示されたら、IAM ユーザーの名前を入力します。

注： IAM ユーザー名は、AWS アカウント内で一意である必要があります。

- f 「Do you want to add trust relationship for any Transit VPC account? [yes/no]」という質問が表示されたら、「yes」と入力します。
- g 「What is the Transit VPC account number?」という質問に対して、手順 1 でメモした 12 桁の AWS アカウント番号を入力するか、コピーして貼り付けます。

2 つの AWS アカウント間で IAM 信頼関係が確立され、スクリプトによって外部 ID が生成されます。

スクリプトが正常に実行されると、PCG の IAM プロファイルとロールが AWS マスター アカウントに作成されます。値は、スクリプトが実行されたディレクトリの出力ファイルに保存されます。ファイル名は `aws_details.txt` です。次に、[CSM での AWS アカウントの追加](#)の手順を実行してから、[トランジット VPC または VNet へのリンク](#)の手順を実行し、トランジット VPC へのリンクのプロセスを終了します。

CSM での AWS アカウントの追加

スクリプトによって生成される値を使用して、AWS アカウントを追加します。

手順

- 1 エンタープライズ管理者ロールで CSM にログインします。
- 2 [CSM] - [クラウド] - [AWS] の順に移動します。

- 3 [+ (追加)] をクリックし、NSX Cloud スクリプトから生成された出力ファイル `aws_details.txt` を使用して、次の詳細を入力します。

オプション	説明
名前	この AWS アカウントのわかりやすい名前を入力します。
アクセス キー	アカウントのアクセス キーを入力します。
プライベート キー	アカウントのプライベート キーを入力します。
クラウド タグの検出	デフォルトではこのオプションが有効になっており、AWS タグを NSX Manager に表示することができます。
ゲートウェイ ロール名	デフォルト値は <code>nsx_pcg_service</code> です。 <code>aws_details.txt</code> ファイル内のスクリプトの出力で、この値を確認できます。

AWS アカウントが CSM に追加されます。

CSM の [VPC] タブで、AWS アカウントのすべての Virtual Private Cloud (VPC) を表示できます。

CSM の [インスタンス] タブで、この VPC 内の EC2 インスタンスを表示できます。

- 4 仮想マシンを管理する VPC 内のすべての仮想マシンをホワイトリストに追加します。これは必須ではありません。ただし、既存環境に展開する場合、検疫ポリシーを無効から有効にすると影響が生じるため、このように設定することをおすすめします。

次のステップ

VPC での PCG の展開

NSX Public Cloud Gateway の展開

NSX Public Cloud Gateway (PCG) は、パブリック クラウドと NSX-T Data Center のオンプレミス管理コンポーネント間の North-South 接続を可能にします。

PCG のアーキテクチャとワークロード仮想マシン管理の展開モードに関する次の用語について理解しておく必要があります。

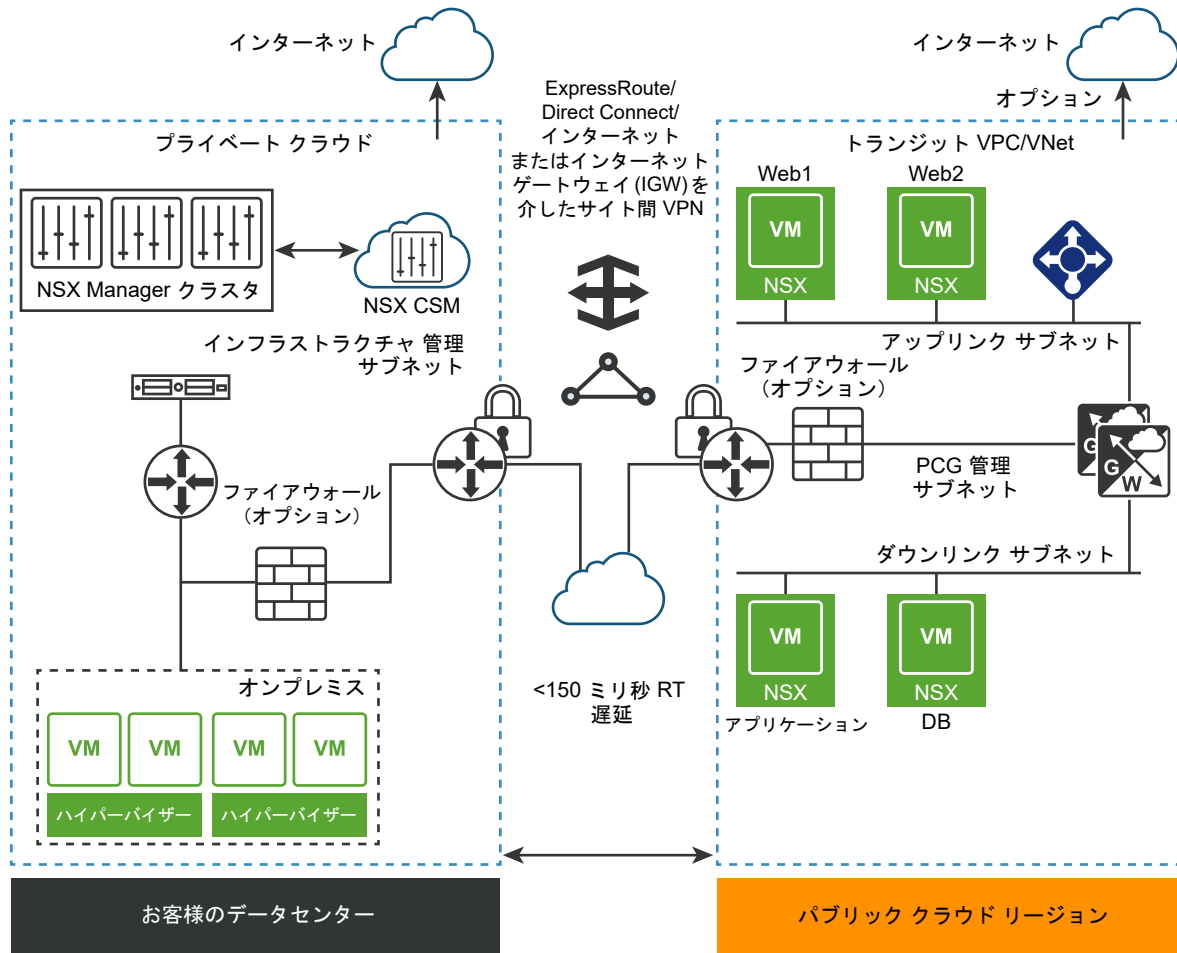
注： PCG は、サポートされているパブリック クラウドごとに 1 つのデフォルトサイズで展開されます。

パブリック クラウド	PCG インスタンス タイプ
AWS	C4.xlarge 注： 一部のリージョンでは、C4.xlarge インスタンス タイプをサポートしていない場合があります。詳細については、AWS のドキュメントを参照してください。
Microsoft Azure	標準 DS3 v.2

アーキテクチャ

PCG は、スタンドアローンのゲートウェイ アプライアンスにすることも、パブリック クラウド VPC または VNet 間で共有してハブ アンド スポーク トポロジを実現することもできます。

図 13-2. NSX Public Cloud Gateway アーキテクチャ



展開のモード

[自己管理 VPC/VNet] : PCG を VPC または VNet に展開すると、VPC または VNet は自己管理として見なされます。したがって、この VPC または VNet でホストされている仮想マシンは、NSX で管理することができます。

[トランジット VPC/VNet] : コンピュート VPC/VNet をリンクすると、自己管理 VPC/VNet がトランジット VPC/VNet になります。

[コンピューティング VPC/VNet] : PCG が展開されておらず、トランジット VPC/VNet にリンクされている VPC/VNet は、コンピューティング VPC/VNet と呼ばれます。

PCG を展開するために VPC/VNet で必要なサブネット

PCG は、VPC または VNet に設定される次のサブネットを利用します。Microsoft Azure ネットワークとオンプレミス NSX-T Data Center 環境の接続または Amazon Web Services (AWS) ネットワークとオンプレミス NSX-T Data Center 環境の接続を参照してください。

- [管理サブネット] : このサブネットは、オンプレミス NSX-T Data Center と PCG 間の管理トラフィックに使用されます。推奨レンジは、/28 です。

- [アップリンク サブネット]：このサブネットは、North-South のインターネット トラフィックに使用されます。推奨レンジは、/24 です。
- [ダウンリンク サブネット]：このサブネットは、ワークロード仮想マシンの IP アドレス範囲を含んでおり、それに応じてサイズ調整する必要があります。デバッグのため、ワークロード仮想マシンに追加のインターフェイスを組み込む必要があることがある点に留意してください。

PCG 環境は、NSX-T Data Center コンポーネントの完全修飾ドメイン名 (FQDN) と、これらの FQDN を解決できる DNS サーバを使用した、既存のネットワーク アドレス プランに適応します。

注： PCG を使用する場合、パブリック クラウドと NSX-T Data Center との接続に IP アドレスを使用することは推奨されませんが、この方法を選択した場合は、IP アドレスを変更しないでください。

仮想マシン管理のモード

NSX 強制モード：このモードの場合、ワークロード仮想マシンは NSX Tools を使用して NSX で管理されます。AWS または Microsoft Azure で `nsx.network=default` タグが適用された後に、各ワークロード仮想マシンに NSX Tools をインストールする必要があります。

Native Cloud 強制モード：このモードの場合、ワークロード仮想マシンは、NSX Tools を使用せずに NSX で管理されます。

検疫ポリシー

検疫ポリシー：これは、パブリック クラウドのセキュリティ グループと連動する NSX Cloud の脅威検出機能です。

- NSX 強制モード では、検疫ポリシーを有効または無効にすることができます。ワークロード仮想マシンをオンボーディングするときに、検疫ポリシーを無効にし、すべての仮想マシンをホワイトリストに追加することをおすすめします。
- Native Cloud 強制モード では、検疫ポリシーは常に有効で、無効にすることはできません。

使用可能な設計オプション

PCG の展開モードに関係なく、どちらのモードでもコンピュート VPC/VNet をリンクできます。

表 13-3. PCG 展開モードで使用可能な設計オプション

トランジット VPC/VNet での PCG 展開モード	このトランジット VPC/VNet にコンピュート VPC/VNet をリンクするときに使用可能なモード
NSX 強制モード	<ul style="list-style-type: none"> ■ NSX 強制モード ■ Native Cloud 強制モード
Native Cloud 強制モード	<ul style="list-style-type: none"> ■ NSX 強制モード ■ Native Cloud 強制モード

注： トランジットまたはコンピュート VPC/VNet にモードを選択した後で、そのモードを変更することはできません。モードを切り替える場合は、PCG の展開を解除し、目的のモードで再展開する必要があります。

VNet での PCG の展開

PCG を Microsoft Azure VNet に展開するには、次の手順を実行します。

PCG を展開する VNet は、他の VNet が接続できるトランジット VNet（コンピューティング VNet と呼ばれる）として機能できます。この VNet は仮想マシンを管理し自己管理 VNet として機能することもできます。

PCG を展開するには次の手順を実行します。既存のトランジット VNet にリンクする場合は、[トランジット VPC または VNet へのリンク](#) を参照してください。

前提条件

- パブリック クラウド アカウントは、すでに CSM に追加されている必要があります。
- PCG の展開先の VNet には、高可用性に合わせて適宜調整された必須のサブネット（アップリンク、ダウンリンク、管理）が配置されている必要があります。

手順

- 1 エンタープライズ管理者ロールを持つアカウントを使用して、CSM にログインします。
- 2 [クラウド] - [Azure] をクリックし、[VNet] タブに移動します。
- 3 PCG を展開する VNet をクリックします。
- 4 [ゲートウェイの展開] をクリックします。[ゲートウェイの展開] ウィザードが開きます。
- 5 一般的なプロパティについては、次のガイドラインを考慮します。

オプション	説明
SSH パブリック キー	PCG の展開で検証するための SSH パブリック キーを指定します。これは、PCG の展開ごとに必要です。
関連付けられている VNet の検疫ポリシー	<p>NSX Tools (NSX 強制モード) を使用してワークロード仮想マシンを管理する場合にのみ、検疫ポリシーの設定を変更できます。検疫ポリシーは、Native Cloud 強制モード で常に有効になっています。</p> <p>PCG を初めて展開する場合は、デフォルトの[無効]モードのままにします。この値は、仮想マシンのオンボーディング後に変更できます。詳細については、『NSX-T Data Center 管理ガイド』の「[検疫ポリシーの管理]」を参照してください。</p>
NSX Tools による管理	Native Cloud 強制モード にワークロード仮想マシンをオンボーディングするには、デフォルトの無効状態のままにします。ワークロード仮想マシンに NSX Tools をインストールして NSX 強制モード を使用する場合は、このオプションを有効にします。
NSX Tools の自動インストール	これは、NSX Tools で管理を有効にした場合にのみ使用できます。選択すると、トランジット/自己管理/リンク コンピュート VNet 内で、 <code>nsx.network=default</code> タグが適用されているすべてのワークロード仮想マシンに NSX Tools が自動的にインストールされます。
ローカル ストレージ アカウント	<p>CSM に Microsoft Azure サブスクリプションを追加すると、Microsoft Azure ストレージ アカウントのリストが CSM で使用できるようになります。ドロップダウン メニューからストレージ アカウントを選択します。PCG の展開で CSM は、パブリックに使用可能な PCG の仮想ハードディスク (VHD) を、選択したリージョンのストレージ アカウントにコピーします。</p> <p>注： 前回の PCG の展開で、仮想ハードディスク イメージをリージョン内の該当のストレージ アカウントにコピーしている場合、以降の展開では、この場所のイメージが使用して展開時間を短縮します。</p>

オプション	説明
仮想ハードディスクの URL	<p>公開されている VMware のリポジトリで提供されない別の PCG イメージを使用する場合は、PCG の仮想ハードディスクの URL をここに入力できます。仮想ハードディスクは、この VNet が作成された同じアカウントと同じリージョンに配置されている必要があります。</p> <p>注： VHD は、正しい URL 形式にする必要があります。Microsoft Azure で [クリックしてコピー] オプションを使用することをお勧めします。</p>
プロキシ サーバ	<p>この PCG からインターネットに向かうトラフィックで使用するプロキシ サーバを選択します。プロキシ サーバは CSM で構成されます。CSM と同じプロキシ サーバがある場合はそれを選択するか、CSM とは異なるプロキシ サーバを選択するか、または [プロキシ サーバなし] を選択できます。</p> <p>CSM でプロキシ サーバを構成する方法の詳細については、(オプション) プロキシ サーバの設定 を参照してください。</p>
詳細	DNS の詳細設定を使用すると、NSX-T Data Center 管理コンポーネントを解決するための DNS サーバを柔軟に選択できます。
パブリック クラウド プロバイダを DHCP 経由で取得	Microsoft Azure の DNS 設定を使用する場合は、このオプションを選択します。DNS 設定を上書きするオプションを選択していない場合は、これがデフォルトの DNS 設定になります。
パブリック クラウド プロバイダの DNS サーバ情報の変更	1 台または複数の DNS サーバの IP アドレスを手動で指定して、NSX-T Data Center アプライアンスと、この VNet 内のワークロード仮想マシンを解決する場合は、このオプションを選択します。
NSX-T Data Center アプライアンスにのみパブリック クラウド プロバイダの DNS サーバを使用	Microsoft Azure の DNS サーバを使用して NSX-T Data Center 管理コンポーネントを解決するには、このオプションを選択します。この設定では、2 台の DNS サーバを使用できます。1 台は NSX-T Data Center アプライアンスを解決する PCG 用で、もう 1 台は、この VNet 内のワークロード仮想マシンを解決する VNet 用です。

6 [次へ] をクリックします。

7 [サブネット] では、次のガイドラインを考慮します。

オプション	説明
NSX クラウド ゲートウェイの HA の有効化	高可用性を有効にするには、このオプションを選択します。
サブネット	高可用性を有効にするには、このオプションを選択します。
管理 NIC のパブリック IP アドレス	[新しい IP アドレスの割り当て] を選択して、管理 NIC にパブリック IP アドレスを指定します。空いているパブリック IP アドレスを再利用する場合は、パブリック IP アドレスを手動で指定できます。
アップリンク NIC のパブリック IP アドレス	[新しい IP アドレスの割り当て] を選択して、アップリンク NIC にパブリック IP アドレスを指定します。空いているパブリック IP アドレスを再利用する場合は、パブリック IP アドレスを手動で指定できます。

次のステップ

『NSX-T Data Center 管理ガイド』の [NSX Cloud の使用](#) の手順に沿って操作します。

VPC での PCG の展開

PCG を Amazon VPC に展開するには次の手順を実行します。

PCG を展開する VPC は、他の VPC が接続できるトランジット VPC（コンピューティング VPC と呼ばれる）として機能できます。この VPC は、仮想マシンを管理し自己管理 VPC として機能することもできます。

PCG を展開するには次の手順を実行します。既存のトランジット VPC にリンクする場合は、[トランジット VPC または VNet へのリンク](#) を参照してください。

前提条件

- パブリック クラウド アカウントは、すでに CSM に追加されている必要があります。
- PCG の展開先の VPC には、高可用性に合わせて適宜調整された必須のサブネット（アップリンク、ダウンリンク、管理）が配置されている必要があります。
- VPC のネットワーク ACL の設定に、ALLOW 受信ルールを含める必要があります。

手順

- 1 エンタープライズ管理者ロールを持つアカウントを使用して、CSM にログインします。
- 2 [クラウド] - [AWS] - [<AWS_account_name>] の順にクリックし、[VPC] タブに移動します。
- 3 [VPC] タブで、AWS リージョン名（us-west など）を選択します。AWS のリージョンは、コンピューティング Virtual Private Cloud (VPC) を作成した場所と同じである必要があります。
- 4 NSX Cloud 用に構成されたコンピュート VPC を選択します。
- 5 ゲートウェイの展開 をクリックします。
- 6 一般的なゲートウェイの詳細を設定します。

オプション	説明
PEM ファイル	ドロップダウン メニューから PEM ファイルのいずれかを選択します。このファイルは、NSX Cloud が展開された場所およびコンピュート VPC を作成した場所と同じリージョンに含まれている必要があります。 これにより AWS アカウントが一意に識別されます。
関連付けられている VPC の検疫ポリシー	NSX Tools (NSX 強制モード) を使用してワークロード仮想マシンを管理する場合にのみ、検疫ポリシーの設定を変更できます。検疫ポリシーは、Native Cloud 強制モード で常に有効になっています。 PCG を初めて展開する場合は、デフォルトの[無効]モードのままにします。この値は、仮想マシンのオンボーディング後に変更できます。詳細については、『NSX-T Data Center 管理ガイド』の「[検疫ポリシーの管理]」を参照してください。
NSX Tools による管理	Native Cloud 強制モード にワークロード仮想マシンをオンボーディングするには、デフォルトの無効状態のままにします。ワークロード仮想マシンに NSX Tools をインストールして NSX 強制モード を使用する場合は、このオプションを有効にします。
プロキシ サーバ	この PCG からインターネットに向かうトラフィックで使用するプロキシ サーバを選択します。プロキシ サーバは CSM で構成されます。CSM と同じプロキシ サーバがある場合はそれを選択するか、CSM とは異なるプロキシ サーバを選択するか、または [プロキシ サーバなし] を選択できます。 CSM でプロキシ サーバを構成する方法の詳細については、 (オプション) プロキシ サーバの設定 を参照してください。
詳細	必要な場合は、詳細設定で追加オプションを指定できます。

オプション	説明
AMI ID のオーバーライド	AWS アカウントで使用可能な AMI ID のうち、PCG では異なる AMI ID を指定するには、高度な機能を使用します。
パブリック クラウド プロバイダを DHCP 経由で取得	AWS 設定を使用する場合は、このオプションを選択します。DNS 設定を上書きするオプションを選択していない場合は、これがデフォルトの DNS 設定になります。
パブリック クラウド プロバイダの DNS サーバ情報の変更	1 台または複数の DNS サーバの IP アドレスを手動で指定して、NSX-T Data Center アプライアンスと、この VPC 内のワークロード仮想マシンを解決する場合は、このオプションを選択します。
NSX-T Data Center アプライアンスにのみパブリック クラウド プロバイダの DNS サーバを使用	AWS の DNS サーバを使用して NSX-T Data Center 管理コンポーネントを解決するには、このオプションを選択します。この設定では、2 台の DNS サーバを使用できます。1 台は NSX-T Data Center アプライアンスを解決する PCG 用で、もう 1 台はこの VPC 内のワークロード仮想マシンを解決する VPC 用です。

7 次へ をクリックします。

8 サブネットの詳細をすべて設定します。

オプション	説明
Public Cloud Gateway の HA の有効化	推奨設定は [有効] です。予定外のダウンタイムを回避するために、高可用性 (HA) のアクティブ/スタンバイのペアを設定します。
プライマリ ゲートウェイの設定	ドロップダウン メニューから、HA のプライマリ ゲートウェイとして us-west-1a などのアベイラビリティ ゾーンを選択します。 ドロップダウン メニューから、アップリンク、ダウンリンク、および管理サブネットを割り当てます。
セカンダリ ゲートウェイの設定	ドロップダウン メニューから、HA のセカンダリ ゲートウェイとして us-west-1b などの別のアベイラビリティ ゾーンを選択します。 セカンダリ ゲートウェイは、プライマリ ゲートウェイが失敗したときに使用されます。 ドロップダウン メニューから、アップリンク、ダウンリンク、および管理サブネットを割り当てます。
管理 NIC のパブリック IP アドレス	[新しい IP アドレスの割り当て] を選択して、管理 NIC にパブリック IP アドレスを指定します。空いているパブリック IP アドレスを再利用する場合は、パブリック IP アドレスを手動で指定できます。
アップリンク NIC のパブリック IP アドレス	[新しい IP アドレスの割り当て] を選択して、アップリンク NIC にパブリック IP アドレスを指定します。空いているパブリック IP アドレスを再利用する場合は、パブリック IP アドレスを手動で指定できます。

展開 をクリックします。

9 プライマリ（および選択した場合はセカンダリ）PCG 環境の状態を監視します。この処理には 10 ～ 12 分かかります。

10 PCG が正常に展開されたら、終了 をクリックします。

次のステップ

『NSX-T Data Center 管理ガイド』の [NSX Cloud の使用](#) の手順に沿って操作します。

トランジット VPC または VNet へのリンク

1 つ以上のコンピュート VPC または VNet をトランジット VPC または VNet にリンクできます。

前提条件

- トランジット VPC または VNet に PCG があることを確認します。
- リンクする VPC/VNet が、VPN またはピアリングを介してトランジット VPC または VNet に接続していることを確認します。
- コンピュート VPC/VNet がトランジット VPC/VNet と同じリージョンに存在することを確認します。

注： ルートベースの IPsec VPN 構成では、仮想トンネル インターフェイス (VTI) ポートの IP アドレスを指定する必要があります。この IP アドレスは、ワークロード仮想マシンと異なるサブネット内にある必要があります。これにより、ワークロード仮想マシンの受信トラフィックが VTI ポートにリダイレクトされなくなり、切断されます。

注： パブリック クラウドでは、セキュリティ グループあたりの受信/送信ルール数にデフォルトの制限があり、NSX Cloud はデフォルトのセキュリティ グループを作成します。これは、トランジット VPC/VNet にリンクできるコンピュート VPC/VNet の数に影響します。VPC/VNet あたり 1 つの CIDR ブロックの場合、NSX Cloud は、トランジット VPC/VNet ごとに 10 個のコンピュート VPC/VNet をサポートします。任意のコンピュート VPC/VNet に複数の CIDR がある場合、1 つのトランジット VPC/VNet でサポートされるコンピュート VPC/VNet の数が少なくなります。デフォルトの制限を調整するには、パブリック クラウドのプロバイダに連絡してください。

手順

- 1 エンタープライズ管理者ロールを持つアカウントを使用して、CSM にログインします。
- 2 [クラウド] - [AWS/Azure] - [<public_cloud_account_name>] の順にクリックし、[VPC/VNet] タブに移動します。
- 3 [VPC] タブまたは [VNet] タブで、1 つ以上のコンピュート VPC または VNet をホストしているリージョン名を選択します。
- 4 NSX Cloud 用に設定されたコンピュート VPC/VNet を選択します。
- 5 [トランジット VPC へのリンク] または [トランジット VNet へのリンク] をクリックします

6 [トランジット VPC または VNet のリンク] ウィンドウでオプションを指定します。

オプション	説明
トランジット VPC または VNet	<p>ドロップダウン メニューで、トランジット VPC または VNet を選択します。選択するトランジット VPC または VNet は、VPN またはピアリングを介してこの VPC とリンクされている必要があります。</p> <p>注： トランジット VNet に接続する場合は、その VNet で DNS フォワーダを構成し、<code>nsx.dnsserver=<IP address of the DNS forwarder></code> タグをトランジット VNet に適用する必要があります。DNS フォワーダの設定の詳細については、Microsoft Azure のドキュメントを参照してください。</p>
デフォルトの検疫ポリシー	PCG を初めて展開する場合は、デフォルトの[無効]モードのままにします。この値は、仮想マシンのオンボーディング後に変更できます。詳細については、『NSX-T Data Center 管理ガイド』の「[検疫ポリシーの管理]」を参照してください。
NSX Tools による管理	Native Cloud 強制モード にワークロード仮想マシンをオンボーディングするには、デフォルトの無効な状態のままにしておきます。ワークロード仮想マシンに NSX Tools をインストールして NSX 強制モード を使用する場合は、このオプションを有効にします。
NSX Tools の自動インストール	これは、NSX Tools での管理を選択した場合、または Microsoft Azure VNet の場合にのみ使用できます。選択すると、トランジット/自己管理/リンク コンピュート VNet 内で、 <code>nsx.network=default</code> タグが適用されているすべてのワークロード仮想マシンに NSX Tools が自動的にインストールされます。

次のステップ

『NSX-T Data Center 管理ガイド』の [NSX Cloud の使用](#) の手順に沿って操作します。

自動作成された論理エンティティとクラウド ネイティブのセキュリティ グループ

トランジット VPC/VNet に PCG を展開してコンピューティング VPC/VNet をリンクすると、NSX-T Data Center およびパブリック クラウドで必要な設定がトリガされます。

自動作成された NSX-T の論理エンティティ

一連の論理エンティティが NSX Manager で自動的に作成されます。

NSX Manager にログインして、自動作成された論理エンティティを表示します。

重要： 手動で PCG を展開解除する場合を除き、これらの自動作成エンティティは削除しないでください。詳細については、[PCG の展開解除のトラブルシューティング](#)を参照してください。

システム エンティティ

[システム] タブには、次のエンティティが表示されます。

表 13-4. 自動作成されたシステム エンティティ

論理システム エンティティ	作成される数	名称	スコープ
[トランスポート ゾーン]	トランジット VPC/VNet ご とに 2 つのトランスポート ゾ ーンが作成されます。	<ul style="list-style-type: none"> ■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN 	スコープ：グローバル
[Edge トランスポート ノード]	展開される PCG ごとに 1 つ の Edge トランスポート ノード が作成されます。高可用性モ ードで展開された場合は 2 台 作成されます。	<ul style="list-style-type: none"> ■ PublicCloudGatewayT N-<VPC/VNET-ID> ■ PublicCloudGatewayT N-<VPC/VNET-ID>-preferred 	スコープ：グローバル
[Edge クラスタ]	1 つであるか高可用性ペアであ るかにかかわらず、展開される PCG ごとに 1 つの Edge ク ラスタが作成されます。	PCG-cluster-<VPC/VNet- ID>	スコープ：グローバル

インベントリ エンティティ

[インベントリ] タブに、次のエンティティが表示されます。

表 13-5. グループ

グループ	スコープ
次の 2 つのグループ： <ul style="list-style-type: none"> ■ cloud-default-route ■ cloud-metadata services 	スコープ：すべての PCG で共有
1 つのグループは、コンピューティング VPC/VNet レベルで作成され た各セグメントの親グループとして、トランジット VPC/VNet レベル で作成されます。cloud-<Transit VPC/VNet ID>-all- segments	範囲：すべてのコンピュート VPC/VNet 全体で共有

表 13-5. グループ（続き）

グループ	スコープ
各コンピューター VPC/VNet の 2 つのグループ： <ul style="list-style-type: none"> ■ コンピューティング VPC/VNet のすべての CIDR 用のネットワーク CIDR グループ：cloud-<Compute VPC/VNet ID>-cidr ■ コンピューティング VPC/VNet 内のすべての管理対象セグメントのローカル セグメント グループ：cloud-<Compute VPC/VNet ID>-local-segments 	範囲：すべてのコンピューティング VPC/VNet 全体で共有
現在サポートされているパブリック クラウド サービスに次のグループが作成されます。 <ul style="list-style-type: none"> ■ aws-dynamo-db-service-endpoint ■ aws-elb-service-endpoint ■ aws-rds-service-endpoint ■ aws-s3-service-endpoint ■ azure-cosmos-db-service-endpoint ■ azure-load-balancer-service-endpoint ■ azure-sql-service-endpoint ■ azure-storage-service-endpoint 	範囲：すべての PCG で共有

注： Native Cloud 強制モード で展開またはリンクされた PCG の場合、VPC/VNet のすべてのワークロード仮想マシンは、NSX Manager の仮想マシンで使用可能になります。

セキュリティ エンティティ

[セキュリティ] タブに、次のエンティティが表示されます。

表 13-6. 自動作成されたセキュリティ エンティティ

論理セキュリティ エンティティ	作成される数	名称	範囲
分散ファイアウォール (East-West)	トランジット VPC/VNet ごとに 2 つ： <ul style="list-style-type: none"> ■ ステートレス ■ ステートフル 	<ul style="list-style-type: none"> ■ cloud-stateless-<VPC/VNet ID> ■ cloud-stateful-<VPC/VNet ID> 	<ul style="list-style-type: none"> ■ ローカル管理対象セグメント内のトラフィックを許可するためのステートフル ルール ■ 管理対象外の仮想マシンからのトラフィックを拒否するためのステートフル ルール
ゲートウェイ ファイアウォール (North-South)	トランジット VPC/VNet ごとに 1 つ	cloud-<Transit VPC/VNet ID>	

ネットワーク エンティティ

オンボーディングの異なるステージで次のエンティティが作成されます。これらのエンティティは、[ネットワーク] タブに表示されます。

図 13-3. PCG の展開後に自動作成された NSX-T Data Center ネットワーク エンティティ

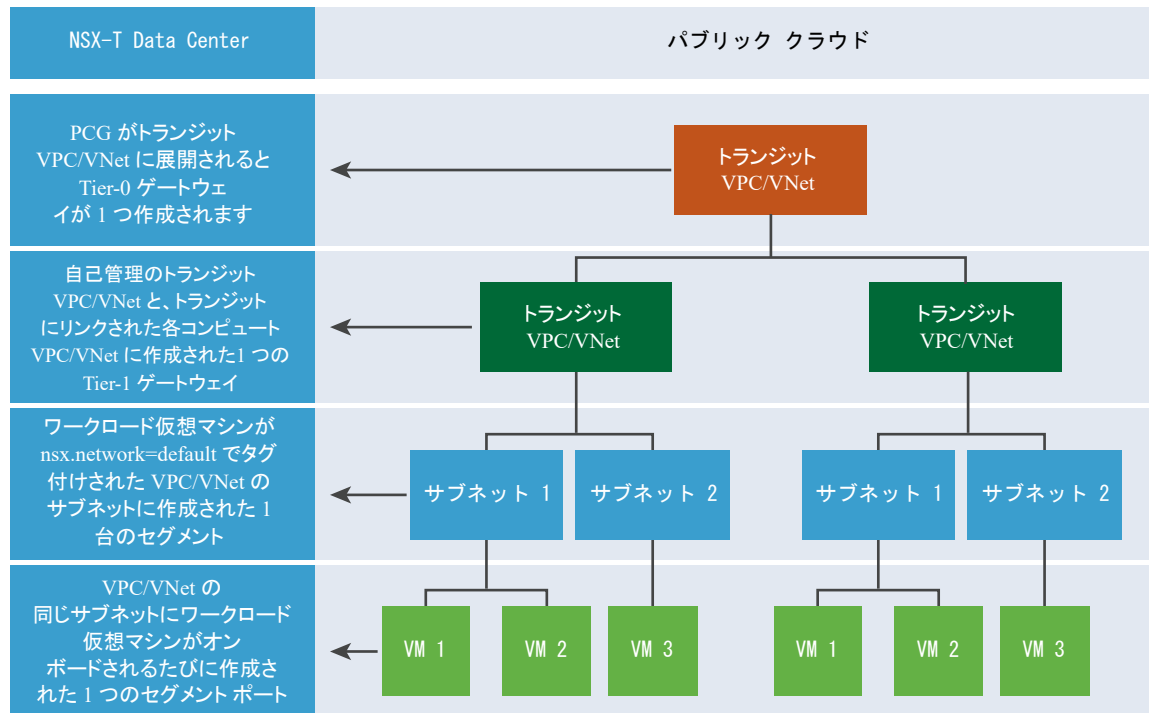


表 13-7. 自動作成されたネットワーク エンティティ

オンボーディング タスク	NSX-T Data Center で作成された論理エンティティ
トランジット VPC/VNet に展開された PCG	<ul style="list-style-type: none"> ■ Tier-0 ゲートウェイ ■ インフラストラクチャ セグメント (デフォルトの VLAN スイッチ) ■ Tier-1 ルーター
トランジット VPC/VNet にリンクされたコンピューティング VPC または VNet	<ul style="list-style-type: none"> ■ Tier-1 ルーター
NSX Agent がインストールされたワークロード仮想マシンには、コンピューティングまたは自己管理 VPC/VNet のサブネット内で「nsx.network:default」キー値のタグが付けられる	<ul style="list-style-type: none"> ■ セグメントは、このコンピューティングまたは自己管理 VPC または VNet の特定のサブネットに対して作成される ■ NSX Agent がインストールされているタグ付けされたワークロード仮想マシンごとにハイブリッド ポートが作成される
より多くのワークロード仮想マシンがコンピューティングまたは自己管理 VPC/VNet の同じサブネット内でタグ付けされる	<ul style="list-style-type: none"> ■ NSX Agent がインストールされているタグ付けされたワークロード仮想マシンごとにハイブリッド ポートが作成される

転送ポリシー

自己管理のトランジット VPC/VNet を含む、コンピューティング VPC/VNet には、次の 3 つの転送ルールが設定されています。

- 同じコンピューティング VPC の任意の CIDR にパブリック クラウドのネットワークを介してアクセスする（アンダーレイ）
- パブリック クラウド メタデータ サービスに関連するトラフィックをパブリック クラウドのネットワークを介してルーティングする（アンダーレイ）
- コンピューティング VPC/VNet の CIDR ブロック、および既知のサービスに含まれていないものすべてを NSX-T Data Center ネットワークを介してルーティングする（オーバーレイ）。

自動作成されるパブリック クラウドの構成

パブリック クラウドでは、PCG の展開後に一部の構成が自動的に行われます。

両方のモードでのパブリック クラウド構成：NSX 強制モード と Native Cloud 強制モード

[AWS の場合：]

- Amazon VPC では、新しい Type A レコード セットが `nsx-gw.vmware.local` という名前で Amazon Route 53 のプライベート ホスト ゾーンに追加されます。このレコードにマッピングされた IP アドレスは、PCG の管理 IP アドレスと一致します。これは DHCP を使用して AWS によって割り当てられ、VPC ごとに異なります。Amazon Route 53 のプライベート ホスト ゾーンにあるこの DNS エントリは、PCG の IP アドレスを解決するために NSX Cloud によって使用されます。

注： Amazon Route 53 のプライベート ホスト ゾーンで定義されているカスタム DNS ドメイン名を使用するときは、AWS の VPC 設定で [DNS 解決] および [DNS ホスト名] 属性を [はい] に設定する必要があります。

- PCG のアップリンク インターフェイス用のセカンダリ IP アドレスが作成されます。AWS 弾性 IP アドレスは、このセカンダリ IP アドレスに関連付けられます。この設定は SNAT 用です。

Native Cloud 強制モード：

PCG を展開すると、次のセキュリティ グループが作成されます。

ワークロード仮想マシンがグループと一致し、NSX Manager で対応するセキュリティ ポリシーと一致すると、それらのセキュリティ ポリシーごとに、`nsx-<GUID>` のような名前のセキュリティ グループがパブリック クラウドに作成されます。

注： AWS では、セキュリティ グループが作成されます。Microsoft Azure では、NSX Manager でアプリケーションセキュリティ グループに対応するグループが作成されます。また、NSX Manager で、ネットワーク セキュリティ グループに対応するセキュリティ ポリシーが作成されます。

セキュリティ グループ 名	Microsoft Azure での使用	AWS での使用	説明
vm-quarantine-sg	はい	いいえ	NSX Cloud が Microsoft Azure に作成したセキュリティ グループ。NSX-T のセキュリティ ポリシーに一致しない仮想マシンに割り当てられます。
デフォルト	いいえ	はい	AWS 内の既存のセキュリティ グループで、NSX Cloud が NSX-T のセキュリティ ポリシーに一致しない仮想マシンにこのグループを割り当てます。
vm-overlay-sg	はい	はい	仮想マシンのオーバーレイ セキュリティ グループ（本リリースでは使用されません）

NSX 強制モード を使用している場合、NSX Cloud が PCG インターフェイス用に作成するパブリック クラウド セキュリティ グループ。

[gw] セキュリティ グループが個別の PCG インターフェイスに割り当てられます。

表 13-8. NSX Cloud が PCG インターフェイス向けに作成するパブリック クラウド セキュリティ グループ

セキュリティ グループ 名	Microsoft Azure での使用	AWS での使用	説明
gw-mgmt-sg	はい	はい	ゲートウェイの管理セキュリティ グループ
gw-uplink-sg	はい	はい	ゲートウェイのアップリンク セキュリティ グループ
gw-vtep-sg	はい	はい	ゲートウェイのダウンリンク セキュリティ グループ

ワークロード仮想マシンに、次のセキュリティ グループが作成されます。

表 13-9. NSX Cloud が NSX 強制モード でワークロード仮想マシン用に作成するパブリック クラウド セキュリティ グループ

セキュリティ グループ 名	Microsoft Azure での使用	AWS での使用	説明
vm-quarantine-sg	はい	いいえ	NSX Cloud が Microsoft Azure に作成するセキュリティ グループ。NSX 強制モード の脅威検出ワークフローで使用されます。
デフォルト	いいえ	はい	AWS に存在する既存のセキュリティ グループ。NSX 強制モード が NSX Cloud で脅威検出ワークフローに使用します。

表 13-9. NSX Cloud が NSX 強制モード でワークロード仮想マシン用に作成するパブリック クラウド セキュリティ グループ (続き)

セキュリティ グループ 名	Microsoft Azure での使用	AWS での使用	説明
vm-underlay-sg	はい	はい	仮想マシン非オーバーレイ セキュリティ グループ
vm-overlay-sg	はい	はい	仮想マシンのオーバーレイ セキュリティ グループ (本リリースでは使用されません)

(オプション) ワークロード仮想マシンへの NSX Tools のインストール

NSX 強制モード を使用している場合は、ワークロード仮想マシンへの NSX Tools のインストールに進みます。

『NSX-T Data Center 管理ガイド』で [NSX 強制モードでの仮想マシンのオンボーディング](#)を参照してください。

PCG の展開解除またはリンク解除

PCG の展開解除またはリンク解除に関連する手順については、この概要を参照してください。

NSX 強制モード の場合

- NSX が管理するワークロード仮想マシンから `nsx.network=default` タグを削除します。
- NSX 強制モード で検疫ポリシーが有効になっている場合は、このポリシーを無効にします。
- NSX Cloud がフォールバック セキュリティ グループとして使用できるパブリック クラウドのセキュリティ グループを指定します。
- PCG に関連付けられている、ユーザーが作成したすべての論理エンティティを削除します。

Native Cloud 強制モード の場合

- NSX Cloud でフォールバック セキュリティ グループとして使用できるパブリック クラウドのセキュリティ グループを指定します。
- PCG に関連付けられている、ユーザーが作成したすべての論理エンティティを削除します。

手順

1 パブリック クラウドの `nsx.network` タグの削除

PCG を展開する前に、すべての仮想マシンを管理対象外にする必要があります。

2 検疫ポリシーの無効化とフォールバック セキュリティ グループの指定

PCG の展開解除または VPC/VNet のリンク解除を続行するには、NSX 強制モード と Native Cloud 強制モード のいずれのモードでも、パブリック クラウドに新規または既存のセキュリティ グループを準備し、そのセキュリティ グループを CSM のフォールバック セキュリティ グループに指定する必要があります。

3 ユーザー作成の論理エンティティの削除

PCG に関連付けられている、ユーザーが作成したすべての論理エンティティを削除する必要があります。

4 CSM からの [展開解除またはリンク解除]

前提条件をすべて完了したら、次の手順に従って、PCG の展開解除またはリンク解除を行います。

5 PCG の展開解除のトラブルシューティング

PCG の展開解除に失敗した場合は、NSX Cloud が作成したすべてのエンティティを NSX Manager とパブリック クラウドから手動で削除する必要があります。

パブリック クラウドの nsx.network タグの削除

PCG を展開する前に、すべての仮想マシンを管理対象外にする必要があります。

注： これは、NSX 強制モード でのみ適用されます。

パブリック クラウド内の VPC または VNet に移動し、管理対象仮想マシンから `nsx.network=default` タグを削除します。

検疫ポリシーの無効化とフォールバック セキュリティ グループの指定

PCG の展開解除または VPC/VNet のリンク解除を続行するには、NSX 強制モード と Native Cloud 強制モード のいずれのモードでも、パブリック クラウドに新規または既存のセキュリティ グループを準備し、そのセキュリティ グループを CSM のフォールバック セキュリティ グループに指定する必要があります。

NSX 強制モード を使用する場合、検疫ポリシーを無効にする必要があります（有効になっている場合）。

注： フォールバック セキュリティ グループは、パブリック クラウド内の既存のユーザー定義セキュリティ グループである必要があります。NSX Cloud セキュリティ グループをフォールバック セキュリティ グループとして使用することはできません。NSX Cloud セキュリティ グループのリストについては、[自動作成された論理エンティティとクラウド ネイティブのセキュリティ グループ](#) を参照してください。

AWS では、default セキュリティ グループは NSX Cloud によって作成されていないので、このグループをフォールバック セキュリティ グループとして設定できます。

フォールバック セキュリティ グループをすでに指定していて、コンピューティング VPC/VNet のリンクを解除し、後でトランジット VPC/VNet に再リンクする場合は、別のフォールバック セキュリティ グループを設定する必要があります。

NSX 強制モード で検疫ポリシーが有効になっている場合

検疫ポリシーが有効になっている場合、NSX Cloud によって定義されたパブリック クラウドのセキュリティ グループが仮想マシンに割り当てられます。PCG を展開解除する場合、検疫ポリシーを無効にして、仮想マシンが NSX Cloud セキュリティ グループから削除されるときに割り当てることができるフォールバック セキュリティ グループを指定する必要があります。

PCG の展開を解除する VPC または VNet の検疫ポリシーを無効にして、フォールバック セキュリティ グループの ID を指定します。

- CSM で VPC または VNet に移動します。

- [アクション] - [設定の編集] の順に進み、[デフォルトの検疫] の設定を無効にします。
- 仮想マシンが割り当てられるフォールバック セキュリティ グループの値を入力します。
- この VPC または VNet で管理対象外になっているかまたは隔離されているすべての仮想マシンに、フォールバック セキュリティ グループが割り当てられます。
- すべての仮想マシンが管理対象外の場合、フォールバック セキュリティ グループが割り当てられます。
- 検疫ポリシーを無効にしているときに管理対象仮想マシンが存在する場合、それらの仮想マシンは NSX Cloud が割り当てたセキュリティ グループのままになります。最初にそのような仮想マシンから `nsx.network=default` タグを削除して NSX 管理から仮想マシンを除外するときにも、フォールバック セキュリティ グループが割り当てられます。

Native Cloud 強制モード を使用している場合

フォールバック セキュリティ グループの ID を指定します。

- CSM で VPC または VNet に移動します。
- [アクション] - [設定の編集] の順にクリックします
- PCG の展開が解除された後、仮想マシンの割り当てが可能なフォールバック セキュリティ グループとして、セキュリティ グループ ID を入力するか（AWS の場合）、ネットワーク セキュリティ グループのリソース ID を入力します（Microsoft Azure の場合）。

注： ホワイトリストに追加された仮想マシンの場合、NSX Cloud は何も処理を行いません。仮想マシンはフォールバック セキュリティ グループに移動しません。NSX Cloud が割り当てたセキュリティ グループにホワイトリストの仮想マシンが存在する場合、指定したフォールバック セキュリティ グループに仮想マシンを手動で移動する必要があります。検疫ポリシーを有効および無効にする手順とその効果の詳細については、『NSX-T Data Center 管理ガイド』の [NSX Cloud 検疫ポリシーによる脅威の検出](#) を参照してください。

ユーザー作成の論理エンティティの削除

PCG に関連付けられている、ユーザーが作成したすべての論理エンティティを削除する必要があります。

PCG に関連付けられたエンティティを特定し、削除します。

注： 自動作成された論理エンティティは削除しないでください。CSM から [展開解除] または [トランジット VPC/VNet からのリンク解除] をクリックすると、これらは自動的に削除されます。詳細については、[自動作成された論理エンティティとクラウド ネイティブのセキュリティ グループ](#) を参照してください。

CSM からの [展開解除またはリンク解除]

前提条件をすべて完了したら、次の手順に従って、PCG の展開解除またはリンク解除を行います。

- 1 CSM にログインし、パブリック クラウドに移動します。
 - AWS を使用している場合は、[クラウド] - [AWS] - [VPC] の順に移動します。1 つまたはペアの PCG が展開され、実行されている VPC をクリックします。

- Microsoft Azure を使用している場合は、[クラウド] - [Azure] - [VNet] の順に移動します。1 つまたはペアの PCG が展開され、実行されている VNet をクリックします。

2 [展開解除] または [トランジット VPC/VNet からのリンク解除] をクリックします。

PCG の展開解除またはリンク解除が完了すると、NSX Cloud によって作成されたデフォルト エンティティは自動的に削除されます。

PCG の展開解除のトラブルシューティング

PCG の展開解除に失敗した場合は、NSX Cloud が作成したすべてのエンティティを NSX Manager とパブリック クラウドから手動で削除する必要があります。

- パブリック クラウドで次の操作を行います。
 - トランジット VPC/VNet 内のすべての PCG を終了します。
 - NSX Cloud で作成されていないセキュリティ グループにすべてのワークロード仮想マシンを移動します。
 - NSX Cloud によって作成されたセキュリティ グループをパブリック クラウドから削除します（[自動作成されるパブリック クラウドの構成](#) を参照）。
 - Microsoft Azure の場合は、**nsx-gw-<vnet ID>-rg** という名前で NSX Cloud が作成したリソースグループも削除します。
- CSM でパブリック クラウド インベントリを再同期します。
- NSX Manager で、VPC/VNet ID を含む自動作成エンティティを削除します（[自動作成された NSX-T の論理エンティティ](#) を参照）。

注： 自動作成されたグローバル エンティティは削除しないでください。VPC/VNet ID を含む名前だけを削除してください。

NSX Intelligence のインストールと構成

14

VMware NSX® Intelligence™ には、オンプレミスの NSX-T Data Center 環境のセキュリティ状態と、そこで発生したネットワーク トラフィック フローを視覚的に表示するためのグラフィカル ユーザー インターフェイスが用意されています。

NSX-T Data Center バージョン 2.5 以降では、ESXi ベースのホストで NSX Intelligence を使用できます。次の機能が提供されます。

- NSX-T Data Center のグループ、仮想マシン、ネットワーク フローなどの NSX-T コンポーネントの視覚的な表示。使用されるデータは、指定された期間に集計されたネットワーク フローに基づきます。
- セキュリティ ポリシー、ポリシー セキュリティ グループ、アプリケーションのサービスに関する推奨事項。推奨事項は、アプリケーション レベルでマイクロセグメンテーションを実装する際に役立ちます。これにより、NSX-T データセンター環境の仮想マシン間で発生する通信トラフィックのパターンを関連付け、より動的なセキュリティ ポリシーを適用できます。

NSX-T Data Center Enterprise Plus ライセンスを保有している場合、または NSX-T Data Center 評価版ライセンスを保有し、その評価期間中の場合は、NSX Intelligence を使用できます。

重要： NSX Intelligence のインストール、設定、使用権限が付与されているエンタープライズ管理者ロールが必要です。

NSX Intelligence アプライアンスは、2 つの異なる展開シナリオで使用できます。Small アプライアンスは、ラボまたは事前検証の展開、あるいは小規模な本番環境で使用できます。大規模な本番環境では、Large アプライアンスを使用できます。[NSX Intelligence のシステム要件](#) を参照してください。

NSX Intelligence 機能を有効にするには、NSX-T Data Center アプライアンスとは別に提供される NSX Intelligence アプライアンスをインストールする必要があります。NSX Intelligence アプライアンスをインストールするには、NSX Manager ユーザー インターフェイス (UI) を使用します。[NSX Intelligence アプライアンスのインストール](#) を参照してください。

NSX Intelligence アプライアンスを正常にインストールして構成した後は、NSX Manager の UI で [プランとトラブルシューティング] > [検出とプラン] タブに移動し、NSX Intelligence の機能にアクセスします。『NSX-T Data Center 管理ガイド』の「NSX Intelligence について」を参照してください。

この章には、次のトピックが含まれています。

- [NSX Intelligence のインストールと構成のワークフロー](#)
- [NSX Intelligence のインストールの準備](#)
- [NSX Intelligence インストーラ バンドルのダウンロードと解凍](#)

- [NSX Intelligence アプライアンスのインストール](#)
- [NSX Intelligence アプライアンスのインストールで発生した問題のトラブルシューティング](#)
- [NSX Intelligence アプライアンスのアンインストール](#)

NSX Intelligence のインストールと構成のワークフロー

次のチェックリストを使用して、NSX Intelligence のインストールの進行状況を確認してください。

表示されている順序で操作を行ってください。

- 1 ESXi ベースのホストに NSX-T Data Center 2.5 以降をインストールします。VMware NSX® Intelligence™ は、ESXi ベースのホストでのみサポートされます。[2 章 NSX-T Data Center インストールのワークフロー](#) を参照してください。
- 2 NSX Intelligence のシステム要件を満たしていることを確認します。[NSX Intelligence のシステム要件](#) を参照してください。
- 3 NSX Manager 仮想マシンと、NSX Intelligence アプライアンスを展開するコンピューティング クラスタの時刻を同期します。
- 4 NSX Intelligence インストーラの TAR ファイルをローカル Web サーバにダウンロードします。この TAR ファイルには、NSX Intelligence アプライアンスのインストールに使用する NSX Intelligence OVF ファイルが含まれています。[NSX Intelligence インストーラ バンドルのダウンロードと解凍](#) を参照してください。
- 5 NSX Intelligence アプライアンスをインストールします。[NSX Intelligence アプライアンスのインストール](#) を参照してください。
- 6 NSX Manager UI で NSX Intelligence UI を有効にするため、NSX Manager セッションに使用している Web ブラウザを更新します。
- 7 NSX Intelligence の機能を使用します。『NSX-T Data Center 管理ガイド』の「NSX Intelligence について」を参照してください。

NSX Intelligence のインストールの準備

NSX Intelligence のインストールに必要な最小システム要件を満たすように、展開環境を準備する必要があります。

次の表では、NSX Intelligence の展開、プラットフォーム、インストールの要件について詳しく説明します。

要件	説明
サポートされる展開方法	OVF VMware vCenter Server™ で、コンピュート マネージャとして追加された NSX Manager を使用してデプロイします。 重要： NSX Intelligence アプライアンスをインストールするには、NSX Manager を使用します。OVF が個別にインストールされている場合はアプライアンスをインストールできません。
サポート対象のプラットフォーム	ESXi ホスト vCenter Server による管理

要件	説明
IP アドレス	NSX Intelligence アプライアンスには固定 IP アドレスが必要です。インストール後に IP アドレスを変更することはできません。
NSX Intelligence アプライアンスのパスワード	<ul style="list-style-type: none"> ■ 12 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の大文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 5 文字以上の異なる文字 ■ 辞書に登録されている単語が使われていない ■ パリンドローム（回文）になっていない ■ 使用できるモノトニックな文字シーケンスは 4 つ以下です。
VMware Tools	ESXi ホストで実行される NSX Intelligence 仮想マシンには、VMware Tools がインストールされています。VMware Tools は削除しないでください。
システム	<ul style="list-style-type: none"> ■ システム要件を満たしていることを確認します。NSX Intelligence のシステム要件 を参照してください。 ■ 必要なポートが開いていることを確認します。NSX Intelligence が使用する TCP および UDP ポート を参照してください。 ■ 管理サブネットとゲートウェイの IP アドレス、DNS サーバの IP アドレス、使用する NSX Intelligence アプライアンスの NTP サーバの IP アドレスの情報を取得します。 ■ SSD ベースのデータストアが設定され、NSX Intelligence アプライアンスにアクセスできることを確認します。

NSX Intelligence のシステム要件

NSX Intelligence アプライアンスをインストールする前に、ご使用の環境がアプライアンスをインストールするサーバ ホストと仮想マシンを可視化するクライアントの両方の最小システム要件を満たしていることを確認します。

NSX Intelligence アプライアンス リソースの要件

次の表に、使用可能な NSX Intelligence アプライアンス サイズと、それぞれに必要な仮想マシン リソースを示します。NSX Intelligence の小規模な仮想マシンのアプライアンス サイズは、ラボおよび POC（事前検証）の環境に適しています。また、小規模な本番環境にも適しています。NSX Intelligence の大規模な仮想マシンのアプライアンス サイズは本番環境に適しています。

アプライアンスのサイズ	メモリ	vCPU	ディスク容量
NSX Intelligence（小規模）	64 GB	16	2 TB
NSX Intelligence（大規模）	128 GB	32	2 TB

注： NSX Manager クラスタあたり、1 つの NSX Intelligence アプライアンスがサポートされます。

NSX Intelligence Web クライアントのメモリ、CPU、およびブラウザの要件

最適なパフォーマンスを維持するため、クライアント システムには、少なくとも 2 つの 1.4 GHz CPU コアと 16 GB 以上の RAM が必要です。

次の表に、NSX Intelligence でサポートされている Web ブラウザのバージョンを示します。サポート対象のブラウザの最低解像度は、1280 X 800 ピクセルです。

ブラウザ	Windows 10	Mac OS X 10.14, 10.13	Ubuntu 18.4
Chrome 76	○	○	○
Firefox 68	○	○	○
Microsoft Edge 44	○	該当なし	該当なし

注： Microsoft Edge を使用する場合、パフォーマンスに関する既知の問題があります。詳細については、NSX-T Data Center リリース ノートを参照してください。

NSX Intelligence が使用する TCP および UDP ポート

NSX Intelligence は、特定の TCP および UDP ポートを使用して、他のコンポーネントおよび製品と通信します。物理およびホストの両方のハイパーバイザー ファイアウォールで、これらのポートが開いている必要があります。

重要： NSX Intelligence ノードにリモートからアクセスするには、このノードで SSH を有効にする必要があります。

表 14-1. NSX Intelligence が使用する TCP および UDP ポート

送信元	宛先	ポート	プロトコル	説明
NSX Intelligence	DNS サーバ	53	TCP	DNS
NSX Intelligence	DNS サーバ	53	UDP	DNS
NSX Intelligence	管理 SCP サーバ	22	TCP	SSH (サポート バンドル、バックアップなどのアップロード)
NSX Intelligence	NTP サーバ	123	UDP	NTP
NSX Intelligence	vCenter Server/NSX Unified Appliance	443	TCP	設定されている場合、NSX Intelligence からコンピュータ マネージャ (vCenter Server) への通信と NSX Unified Appliance。
NSX Intelligence	NSX Unified Appliance/NSX トランスポート ノード	9092	TCP	NSX Unified Appliance またはトランスポート ノードへの NSX Intelligence の発信通信
NTP サーバ	NSX Intelligence	123	UDP	NTP

表 14-1. NSX Intelligence が使用する TCP および UDP ポート（続き）

送信元	宛先	ポート	プロトコル	説明
管理クライアント	NSX Intelligence	22	TCP	SSH（デフォルトでは無効）
管理クライアント/NSX Unified Appliance	NSX Intelligence	443	TCP	NSX API サーバ
NSX Unified Appliance/トランスポート ノード	NSX Intelligence	9092	TCP	NSX Unified Appliance またはトランスポート ノードから NSX Intelligence アプライアンスへの着信メッセージ

NSX Intelligence インストーラ バンドルのダウンロードと解凍

NSX Intelligence アプライアンスをインストールするには、NSX Intelligence インストーラ バンドル ファイルをローカル Web サーバにダウンロードして解凍します。バンドル ファイルには、OVF と、NSX Intelligence アプライアンスのインストールに使用されるその他のサポート ファイルが含まれています。

前提条件

- NSX Intelligence の使用資格が付与されていることを確認します。NSX-T Data Center Enterprise Plus ライセンスを保有している場合、または NSX-T Data Center 評価版ライセンスを保有し、その評価期間中の場合は、NSX Intelligence を使用できます。
- NSX Intelligence のインストール、設定、使用権限が付与されているエンタープライズ管理者ロールが必要です。
- ダウンロードを実行するユーザーが、ローカル Web サーバに .tar ファイルをダウンロードして、内容を抽出できる権限を持っていることを確認します。
- NSX Intelligence インストーラ バンドル ファイルのダウンロードに使用する予定のローカル Web サーバが、HTTP のデフォルト ポート 80 を使用していることを確認します。

手順

- 1 VMware ダウンロード ポータルで NSX Intelligence インストーラ TAR ファイルを見つけます。
- 2 NSX Manager ユーザー インターフェイスからアクセスできるローカル Web サーバの場所に、NSX Intelligence インストーラ バンドル ファイルをダウンロードして保存します。

注： 現在サポートされている Web サーバは、IIS (Windows) と Apache (Linux、Mac OS) です。別の Web サーバも選択できますが、これらのオペレーティングシステムでテストされ、サポートされている Web サーバは IIS と Apache です。

インストーラ バンドルのファイル名は、VMware-NSX-Intelligence-appliance-<release-number>.<build-number>.tar の形式です。例：VMware-NSX-Intelligence-appliance-1.0.0.0.0.14303803.tar

3 同じローカル Web サーバ上に TAR ファイルの内容を解凍します。

- a サポートされているいずれかの Web サーバで TAR ファイルの内容を解凍するには、次の情報を使用します。

オペレーティング システム	Web サーバ	解凍ツール
Windows	IIS	<p>7-Zip アプリケーション</p> <p>7-Zip File Manager ユーザー インターフェイスを使用するか、コマンド プロンプト ウィンドウを使用します。たとえば、コマンド プロンプト ウィンドウを使用してサンプルの TAR ファイルを解凍するには、ダウンロードした NSX Intelligence TAR ファイルの場所に移動し、次のコマンドを入力します。</p> <pre>7z x VMware-NSX-Intelligence-appliance-1.0.0.0.0.14303803.tar</pre>
Linux	Apache	<p>tar コマンドライン ユーティリティ</p> <p>たとえば、サンプルの TAR ファイルを展開するには、コマンド プロンプトで次のように入力します。</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.0.14303803.tar</pre>
Mac OS	Apache	<p>tar コマンドライン ユーティリティ</p> <p>たとえば、サンプルの TAR ファイルを展開するには、Terminal コマンドラインで次のように入力します。</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.0.14303803.tar</pre>

前述のバンドル ファイル名の場合、次のファイルが解凍されます。

- nsx-intelligence-appliance-1.0.0.0.0.14303803.cert
- nsx-intelligence-appliance-1.0.0.0.0.14303803.mf
- nsx-intelligence-appliance-1.0.0.0.0.14303803.ovf
- nsx-intelligence-appliance.vmdk

- b インストールを続行する前に、解凍されたファイルのチェックサムがマニフェスト ファイルに記載されている情報と同じであることを確認します。

4 次の情報を使用して、使用している Web サーバで NSX Intelligence インストーラ ファイル タイプに MIME タイプが設定されていることを確認します。必要に応じて、Web サーバを手動で更新します。

NSX Intelligence インストーラファイル タイプ	MIME タイプ
.ovf	application/vmware
.vmdk	application/octet-stream
.mf	text/cache-manifest
.cert	application/x-x509-user-cert

- 5 NSX Intelligence OVF ファイルのファイルパスをコピーします。例: `http://local-web-server/nsx-intelligence-appliance-1.0.0.0.14303803.ovf` このパスを NSX Intelligence アプライアンスのインストール プロセスで指定します。

次のステップ

NSX Intelligence アプライアンスのインストールを続行します。NSX Intelligence アプライアンスのインストールを参照してください。

NSX Intelligence アプライアンスのインストール

NSX Intelligence アプライアンスをインストールして構成するには、NSX Manager UI を使用します。

NSX Intelligence 機能を使用する前に、NSX Intelligence アプライアンスをインストールして構成し、NSX Intelligence サービスとプラグインを NSX Manager に統合する必要があります。

前提条件

- NSX-T Data Center 2.5 以降がインストールされていることを確認します。2 章 NSX-T Data Center インストールのワークフロー を参照してください。
- NSX Intelligence のインストール、設定、使用権限が付与されているエンタープライズ管理者ロールが必要です。
- VMware ダウンロード ポータルで NSX Intelligence インストーラ バンドル ファイルを探して、ローカル Web サーバにダウンロードします。NSX Intelligence インストーラ バンドルのダウンロードと解凍 を参照してください。
- NSX Intelligence インストーラ バンドル ファイルを含むローカル Web サーバが、HTTP のデフォルト ポート 80 を使用していることを確認します。
- 構成する NSX Intelligence アプライアンスのサイズを決めます。小規模サイズは、ラボまたは事前検証の展開、あるいは小規模な本番環境で使用できます。大規模な本番環境の場合は、大規模サイズを使用します。
- インストールするアプライアンス サイズについて、NSX Intelligence のシステム要件を満たしていることを確認します。NSX Intelligence のシステム要件 を参照してください。
- NSX Intelligence アプライアンスを展開するコンピューティング クラスタの時間を NSX Manager サーバと同期します。
- NSX Intelligence アプライアンスの構成に必要な管理サブネット、ゲートウェイ、DNS サーバ、NTP サーバの IP アドレスを取得します。

手順

- 1 ブラウザから、エンタープライズ管理者の権限で NSX Manager (`https://<nsx-manager-ip-address>`) にログインします。
- 2 NSX Manager で [システム] - [アプライアンス] の順に選択します。
- 3 [アプライアンスの概要] ペインで下にスクロールして NSX Intelligence アプライアンス カードを探し、[NSX Intelligence アプライアンスの追加] をクリックします。

4 [アプライアンスを追加] ウィザードで、NSX Intelligence アプライアンスの詳細を入力します。

詳細項目	実行するアクション
[OVF ファイル]	ローカル Web サーバにダウンロードした NSX Intelligence OVF ファイルの URL を入力します。例: <code>http://localhost/nsx-intelligence-appliance-1.1.0.0.13912394.ovf</code>
[名前]	NSX Intelligence アプライアンスの名前を入力します。この値は、完全修飾ドメイン名にすることも、 mytest-lab などの簡易名を指定することもできます。
[管理サブネット]	NSX Intelligence アプライアンスで使用する IP アドレス（範囲を含む）を入力します。例: <code>10.11.22.33/24</code>
[ゲートウェイ IP]	使用する NSX Intelligence アプライアンスの 1 つのゲートウェイ IP アドレスを入力します。
[DNS サーバ]	1 台以上の DNS サーバの IP アドレスを入力します。
[NTP サーバ]	1 台以上の NTP サーバの IP アドレスを入力します。
[ノード サイズ]	構成する NSX Intelligence アプライアンスのサイズを選択します。Small アプライアンスは、ラボまたは事前検証環境、あるいは小規模な本番環境で使用できます。大規模な本番環境の場合は、Large アプライアンスを使用します。

5 [次へ] をクリックします。

6 NSX Intelligence アプライアンスの展開先の詳細を入力します。

詳細項目	実行するアクション
[コンピュート マネージャ]	ドロップダウン メニューから、NSX Intelligence アプライアンスをインストールするコンピュート マネージャを選択します。
[クラスタ]	ドロップダウン メニューから、使用するクラスタを選択します。
[リソース プール]	(オプション) ドロップダウン メニューからリソース プールを選択します。
[ホスト]	(オプション) ドロップダウン メニューからホストを選択します。複数のトランスポート ノードがあるクラスタを使用している場合は、使用するトランスポート ノードを決定します。 注: ホストを明示的に選択すると、vCPU カウント チェックが上書きされます。選択するホストに、インストールする NSX Intelligence アプライアンスのサイズに対応できる十分な vCPU 数があることを確認します。これがない場合、NSX Intelligence アプライアンスの設定が正しく行われない可能性があります。不明な場合は、テキスト ボックスを空のままにします。これにより、適切なホストが自動的に選択されます。
[データストア]	ドロップダウン メニューから、NSX Intelligence の構成とデータを保存するデータストアを選択します。
[ネットワーク]	ドロップダウン メニューから、使用するネットワークを選択します。
[SSH の有効化] と [root アクセスの有効化]	NSX Intelligence アプライアンス コマンドライン インターフェイス (CLI) への SSH アクセスまたは root アクセスを有効にするかどうかを指定します。 デフォルトで、これらのオプションはセキュリティ上の理由から無効になっています。CLI を使用して、バックアップ ファイル サーバを設定し、NSX Intelligence アプライアンス構成のバックアップとリストアを行います。

7 [次へ] をクリックします。

8 管理者認証情報と NSX Intelligence アプライアンスへのアクセス権を設定します。

- a root アクセスを有効にした場合は、root パスワードを設定します。UI に表示されるパスワード要件に従います。
- b CLI 認証情報と監査 CLI 認証情報を選択します。CLI パスワードまたは監査 CLI パスワードのいずれかに root パスワードを使用する場合は、[root パスワードと同じ] を選択します。それ以外の場合は、[CLI パスワード] と [監査 CLI パスワード] にパスワードを入力します。

9 [アプライアンスのインストール] をクリックします。

インストールの進行状況が [プランとトラブルシューティング] タブに表示されます。NSX Intelligence アプライアンスが必要とするすべてのサービスとプラグインを検出するため、インストールに 5 ～ 30 分かかることがあります。

注： エラーが報告された場合は、エラー メッセージの情報を使用して、報告された問題を解決します。問題が解決されたら、NSX Intelligence アプライアンスをアンインストールしてから、[システム] - [アプライアンス] タブから再インストールする必要があります。発生する可能性がある問題の解決方法については、[NSX Intelligence アプライアンスのアンインストール](#)または[NSX Intelligence アプライアンスのインストールで発生した問題のトラブルシューティング](#)を参照してください。

10 NSX Intelligence アプライアンスが正常にインストールされたら、[表示を更新] をクリックします。

NSX Manager UI が更新され、[プランとトラブルシューティング] - [検出とプラン] タブで NSX Intelligence 機能が有効になります。

次のステップ

NSX Intelligence の機能を使用します。『NSX-T Data Center 管理ガイド』の「NSX Intelligence の使用」を参照してください。

NSX Intelligence アプライアンスのインストールで発生した問題のトラブルシューティング

このセクションでは、NSX Intelligence アプライアンスのインストール時に発生する可能性のある問題の解決に役立つ情報を提供します。

認証情報が無効か、指定したアカウントがロックされている

NSX Intelligence アプライアンスを展開すると、「認証情報が正しくないか、指定されたアカウントがロックされています」というエラー メッセージが表示されます。

問題

NSX Intelligence アプライアンスのインストーラを実行した後、インストーラが NSX Intelligence サーバを NSX Manager に登録しようとしたときに、「認証情報が正しくないか、指定されたアカウントがロックされています」というエラーメッセージが表示されます

原因

次のいずれかの理由で登録手順が失敗した可能性があります。

- 管理プレーンのトークンが期限切れになっている可能性があります。トークンの有効期間は 30 分です。
- NSX Intelligence サーバ ホストと NSX Manager ホストでシステム時刻が同期されていません。

解決方法

- 1 NSX Intelligence サーバ ホストと NSX Manager ホストでシステム時刻が同期されていることを確認します。
- 2 システム時刻が同期されている場合は、ネットワークに遅延があるかどうかを確認します。
- 3 システム時刻を同期した後、またはネットワークの遅延が解決したときに、NSX Intelligence アプライアンスを削除してインストールを再試行してください。

アプライアンスの展開に失敗した状態がクリアされない

NSX Intelligence アプライアンスの展開に成功しても「アプライアンスの展開に失敗しました」という状態が表示されません。

問題

リソース不足などの問題で、NSX Intelligence アプライアンスの最初の展開に失敗すると、報告された問題が解決されても展開失敗の状態メッセージがクリアされません。

原因

問題の解決は NSX Intelligence アプライアンスの外部で行われているため、報告された展開の問題の根本原因が解決されても NSX Intelligence アプライアンスはこの状態を認識しません。

解決方法

- 1 以前のアプライアンスの展開時に報告された問題を解決したら、NSX Intelligence アプライアンスをアンインストールします。
- 2 [システム] - [アプライアンス] タブで NSX Intelligence アプライアンスを再インストールします。
- 3 (オプション) NSX Intelligence アプライアンスの更新された展開状態を取得するには、Web ブラウザの表示を更新します。

NSX Intelligence アプライアンスのアンインストール

NSX Intelligence を完全にアンインストールするには、次の手順を実行します。

手順

- 1 ブラウザから、エンタープライズ管理者の権限で NSX Manager (<https://<nsx-manager-ip-address>>) にログインします。
- 2 NSX Manager UI で、[システム] - [アプライアンス] を選択します。

- 3 NSX Intelligence アプライアンス カードを探します。
- 4 [削除] をクリックします。
- 5 [アプライアンスの削除を確認] ダイアログ ボックスで、[確認] をクリックします。

インストール問題のトラブルシューティング

15

NSX-T Data Center のインストールと構成に関連する問題のリスト

問題	解決方法
ホストまたはクラスタから NSX-T を削除した後に、vCenter Server または ESXi ホストに不透明ネットワークが表示される	https://ikb.vmware.com/s/article/75234
ESXi ホスト上の bootbank の容量が不足しているためインストールが失敗する	https://kb.vmware.com/s/article/74864

この章には、次のトピックが含まれています。

- ESXi ホスト上の bootbank の容量が不足しているためインストールが失敗する

ESXi ホスト上の bootbank の容量が不足しているためインストールが失敗する

ESXi ホスト上の bootbank または alt-bootbank に十分な容量がない場合、NSX-T Data Center のインストールが失敗することがあります。

問題

ESXi ホストで、次のようなログ (esxupdate.log) メッセージが表示されることがあります。

```
20**-**-**T13:37:50Z esxupdate: 5557508: BootBankInstaller.pyc:
ERROR: The pending transaction requires 245 MB free space,
however the maximum supported size is 239 MB.^@
```

原因

ESXi ホストの未使用 VIB は、サイズが比較的大きくなることがあります。これらの未使用の VIB によって、必要な VIB をインストールするときに、bootbank または alt-bootbank の容量が不足することがあります。

解決方法

- 不要になった VIB をアンインストールし、追加のディスク容量を解放します。

未使用の VIB の削除に関する詳細については、VMware ナレッジベースの記事 <https://kb.vmware.com/s/article/74864> を参照してください。