

# NSX アップグレードガイド

Update 5

変更日：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

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

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

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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

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

# 内容

NSX アップグレード ガイド	4
サポート ドキュメント	4
NSX のシステム要件	5
NSX で必要となるポートおよびプロトコル	6
1 vCloud Networking and Security から NSX へのアップグレード	10
NSX にアップグレードするための vCloud Networking and Security の準備	10
vCloud Networking and Security 5.5.x から NSX 6.2.x へのアップグレード	21
vCloud Director 環境での vCloud Networking and Security 5.5.x から NSX へのアップグレード	42
2 NSX アップグレード	61
NSX のアップグレードの準備	61
NSX 6.1.x または 6.2.x から NSX 6.2.x へのアップグレード	73
Cross-vCenter NSX での NSX 6.2.x へのアップグレード	88
3 NSX 環境での vSphere のアップグレード	106
NSX 環境での ESXi のアップグレード	106
ESXi アップグレード後のゲスト イントロスペクションの再デプロイ	108

# NSX アップグレード ガイド

『NSX アップグレード ガイド』では、vSphere Web Client を使用して VMware<sup>®</sup> NSX<sup>™</sup> システムをアップグレードする方法について説明します。また、詳細なアップグレード手順や推奨されるベスト プラクティスについても記載しています。

## 対象読者

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

## VMware の技術ドキュメントの用語集

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

## サポート ドキュメント

このアップグレード ガイドの他に、VMware はアップグレード プロセスをサポートするさまざまなドキュメントを公開しています。

### リリース ノート

アップグレードを開始する前に、リリース ノートを確認してください。アップグレードに関する既知の問題と回避策については、NSX のリリース ノートを参照してください。アップグレード プロセスを開始する前に問題を把握しておくことで、時間や労力を削減できます。<https://docs.vmware.com/jp/VMware-NSX-for-vSphere/index.html> を参照してください。

### 製品の相互運用性マトリックス

vCenter Server など、他の VMware 製品との相互運用性を確認できます。VMware 製品の相互運用性マトリックスは、[http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) の [Interoperability] タブを参照してください。

現在の NSX バージョンからのサポート対象のアップグレードパスを確認します。  
製品メニューの [アップグレード パス (Upgrade Path)] タブで [VMware NSX] を  
選択してください。

## 互換性ガイド

VMware 互換性ガイドでは、パートナー ソリューションと NSX の互換性を確認で  
きます。

<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security> を参照してください。

## NSX のシステム要件

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

## ハードウェア

表 1. ハードウェア要件

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

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

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

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

## ソフトウェア

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

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

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

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

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

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

## クライアントとユーザー アクセス

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

## NSX で必要となるポートおよびプロトコル

NSX が正常に機能するには、次のポートが開いている必要があります。

表 2. NSX で必要となるポートおよびプロトコル

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
クライアント PC	NSX Manager	443	TCP	NSX Manager 管理インターフェイス	×	○	PAM 認証
クライアント PC	NSX Manager	80	TCP	NSX Manager VIB アクセス	×	×	PAM 認証
ESXi ホスト	vCenter Server	443	TCP	ESXi ホストの準備	×	×	
vCenter Server	ESXi ホスト	443	TCP	ESXi ホストの準備	×	×	
ESXi ホスト	NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
ESXi ホスト	NSX Controller	1234	TCP	ユーザー ワールド エージェント接続	×	○	
NSX Controller	NSX Controller	2878、 2888、 3888	TCP	コントローラ クラスタ - 状態同期	×	○	IPsec
NSX Controller	NSX Controller	7777	TCP	内部コントローラ RPC ポート	×	○	IPsec
NSX Controller	NSX Controller	30865	TCP	コントローラ クラスタ - 状態同期	×	○	IPsec
NSX Manager	NSX Controller	443	TCP	コントローラと Manager の通信	×	○	ユーザー/パスワード
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	×	○	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	×	○	
NSX Manager	ESXi ホスト	443	TCP	管理とプロビジョニング接続	×	○	
NSX Manager	ESXi ホスト	902	TCP	管理とプロビジョニング接続	×	○	
NSX Manager	DNS サーバ	53	TCP	DNS クライアント接続	×	×	
NSX Manager	DNS サーバ	53	UDP	DNS クライアント接続	×	×	
NSX Manager	Syslog サーバ	514	TCP	Syslog 接続	×	×	
NSX Manager	Syslog サーバ	514	UDP	Syslog 接続	×	×	
NSX Manager	NTP タイム サーバ	123	TCP	NTP クライアント接続	×	○	
NSX Manager	NTP タイム サーバ	123	UDP	NTP クライアント接続	×	○	
vCenter Server	NSX Manager	80	TCP	ホストの準備	×	○	
REST Client	NSX Manager	443	TCP	NSX Manager REST API	×	○	ユーザー/パスワード

表 2. NSX で必要となるポートおよびプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (NSX 6.2.3 より前のデフォルト) または 4789 (NSX 6.2.3 以降の新規インスタールのデフォルト)	UDP	VTEP 間の転送ネットワークのカプセル化	×	○	
ESXi ホスト	ESXi ホスト	6999	UDP	VLAN LIF 上の ARP	×	○	
ESXi ホスト	NSX Manager	8301, 8302	UDP	分散仮想スイッチ同期	×	○	
NSX Manager	ESXi ホスト	8301, 8302	UDP	分散仮想スイッチ同期	×	○	
ゲストイントロスペクション仮想マシン	NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
プライマリ NSX Manager	セカンダリ NSX Manager	443	TCP	Cross-vCenter NSX ユニバーサル同期サービス	×	○	
プライマリ NSX Manager	vCenter Server	443	TCP	vSphere API	×	○	
セカンダリ NSX Manager	vCenter Server	443	TCP	vSphere API	×	○	
プライマリ NSX Manager	NSX ユニバーサルコントローラ クラスタ	443	TCP	NSX Controller REST API	×	○	ユーザー/パスワード
セカンダリ NSX Manager	NSX ユニバーサルコントローラ クラスタ	443	TCP	NSX Controller REST API	×	○	ユーザー/パスワード
ESXi ホスト	NSX ユニバーサルコントローラ クラスタ	1234	TCP	NSX 制御プレーン プロトコル	×	○	
ESXi ホスト	プライマリ NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
ESXi ホスト	セカンダリ NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード



## Cross-vCenter NSX と拡張リンク モードのポート

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

# vCloud Networking and Security から NSX へのアップグレード

# 1

この章には、次のトピックが含まれています。

- NSX にアップグレードするための vCloud Networking and Security の準備
- vCloud Networking and Security 5.5.x から NSX 6.2.x へのアップグレード
- vCloud Director 環境での vCloud Networking and Security 5.5.x から NSX へのアップグレード

## NSX にアップグレードするための vCloud Networking and Security の準備

NSX に正常にアップグレードするには、リリース ノートでアップグレードの問題を確認し、正しいアップグレード手順を実行していて、インフラストラクチャがアップグレードに適切に準備されていることを確認します。次のガイドラインは、アップグレード前のチェックリストとして使用できます。



**警告:** ダウングレードはサポートされない:

- アップグレードの前に、必ず NSX Manager をバックアップしてください。
- NSX Manager が正常にアップグレードされたあとは、NSX をダウングレードできません。

アップグレードは、企業で定められているメンテナンス期間中に実施することをお勧めします。

次のガイドラインは、アップグレード前のチェックリストとして使用できます。

- 1 vCloud Networking and Security のバージョンが 5.5 であることを確認します。このバージョンでない場合は、『vShield インストールとアップグレード ガイド』バージョン 5.5 を参照して、アップグレードの手順を確認してください。
- 2 必要なポートがすべて開いていることを確認します。[NSX で必要となるポートおよびプロトコル] を参照してください。
- 3 vSphere Distributed Switch のアップリンク ポート名情報を取得できることを確認します。  
<https://kb.vmware.com/kb/2129200> を参照してください。
- 4 vShield Endpoint パートナーのサービスを展開している場合は、アップグレードを行う前に互換性を確認します。
  - ほとんどの場合、パートナー ソリューションに影響を与えることなく、vCloud Networking and Security を NSX にアップグレードできます。ただし、アップグレードする NSX のバージョンと、パートナー ソリューションとの間に互換性がない場合、NSX をアップグレードする前に、パートナー ソリューションを互換性のあるバージョンにアップグレードする必要があります。

- VMware 互換性ガイドでネットワークとセキュリティについて確認します。  
<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security> を参照してください。
  - パートナーのドキュメントで、互換性とアップグレードの詳細について確認します。
- 5 環境内に Data Security がある場合は、vShield Manager のアップグレード前にアンインストールしておきます。[\[vShield Data Security のアンインストール\]](#) を参照してください。
  - 6 外部スイッチ プロバイダとして Cisco Nexus 1000V を使用している場合は、NSX にアップグレードする前に、これらのネットワークを vSphere Distributed Switch に移行する必要があります。NSX をインストールしたら、vSphere Distributed Switches を論理スイッチに移行できます。
  - 7 vShield Manager、vCenter Server、およびその他の vCloud Networking and Security コンポーネントの最新のバックアップが作成済みであることを確認します。[\[vCloud Networking and Security のバックアップとリストア\]](#) を参照してください。
  - 8 テクニカル サポート バンドルを作成します。
  - 9 nslookup コマンドを使用して、正引き/逆引きのドメイン名解決が動作していることを確認します。
  - 10 環境で vSphere Update Manager (VUM) を使用している場合は、vCenter Server で bypassVumEnabled フラグが True に設定されていることを確認します。この設定によって、VUM がインストールされているときや使用できないときでも、VIB を ESXi ホストに直接インストールするように ESX Agent Manager (EAM) が設定されます。<http://kb.vmware.com/kb/2053782> を参照してください。
  - 11 アップグレード バンドルをダウンロードしてステージングし、md5sum を使用して検証します。[\[vShield Manager から NSX へのアップグレード バンドルのダウンロードと MD5 の確認\]](#) を参照してください。
  - 12 ベスト プラクティスとして、アップグレードのすべてのセクションが完了するまでの間、環境内ですべての運用を停止することをお勧めします。
  - 13 指示があるまでは、vCloud Networking and Security のコンポーネントとアプライアンスのパワーオフや削除を行わないでください。

## vCloud Networking and Security から NSX へのアップグレードに必要なライセンスの確認

vCloud Networking and Security を NSX にアップグレードする場合、既存のライセンスは NSX for vShield Endpoint ライセンスに変換されます。

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

準備されたホスト、仮想ワイヤー、vShield App、または vShield Edge など、すでに vCloud Networking and Security の機能をデプロイしている場合、引き続きこれらの機能を使用できますが、これらの機能を NSX にアップグレードすることはできません。また、これらの機能を変更することもできません。

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

NSX ライセンスに関する FAQ (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>) を参照してください。

## vCloud Networking and Security のアップグレードによる動作上の影響

vCloud Networking and Security のアップグレード、特にホストの再起動が必要になる ESXi ホストのアップグレードには時間がかかります。ホストがすべてではなく一部だけアップグレードされている場合や、NSX Edge がまだアップグレードされていない場合など、アップグレード中の vCloud Networking and Security コンポーネントの動作状態を理解することは重要です。

vCloud Networking and Security から NSX 6.2.x にアップグレードするには、NSX コンポーネントを次の順番でアップグレードする必要があります。

- vShield Manager
- ホスト クラスと仮想ワイヤー
- vShield App
- vShield Edge
- vShield Endpoint

1 回の停止期間でアップグレードを実行することをお勧めします。この理由は、ダウンタイムを最小に抑えること、またアップグレード中に一部の vCloud Networking and Security 管理機能を利用できなくなるため、vCloud Networking and Security ユーザーの混乱を回避することです。しかし、サイトの要件により 1 回の停止期間でアップグレードを完了できない場合、以下の情報を参照することで、vCloud Networking and Security ユーザーはアップグレード中にどの機能が利用可能かを把握できます。

## vCenter Server のアップグレード

vCenter Server に組み込みの SSO を使用していて、vCenter Server 5.5 を vCenter Server 6.0 にアップグレードする場合、vCenter Server で vShield Manager との接続が失われることがあります。この状態は、vCenter Server 5.5 が root ユーザー名で vShield に登録されていた場合に発生します。NSX 6.2 以降では、root ユーザー名を使用した vCenter Server の登録は廃止されました。回避策として、root の代わりに administrator@vsphere.local のユーザー名を使用して、vCenter Server を vShield に登録します。

外部の SSO を使用している場合、変更は必要ありません。今までと同じユーザー名 (admin@mybusiness.mydomain など) をそのまま使用することができ、vCenter Server との接続は失われません。

## vShield Manager のアップグレード

アップグレード中：

- vShield Manager の設定はブロックされます。vShield API サービスは利用できません。vShield の設定は変更できません。既存の仮想マシンの接続は引き続き機能します。新しい仮想マシンのプロビジョニングは引き続き vSphere で機能しますが、vShield Manager のアップグレード中は、新しい仮想マシンは vShield 仮想ワイヤーに接続できません。

アップグレード後：

- vShield の設定の変更はすべて許可されます。

## ホスト クラスタのアップグレードと仮想ワイヤー

ホスト クラスタをアップグレードすると、新しい VIB がホストにインストールされます。

NSX では、仮想ワイヤーという名称は、論理スイッチに変更されました。

アップグレード中：

- NSX Manager では設定の変更はブロックされません。
- アップグレードはクラスタごとに実行されます。クラスタで DRS が有効な場合、DRS によってホストのアップグレード順序が管理されます。

クラスタ内の NSX ホストの一部がアップグレードされ、一部がアップグレードされていない場合：

- NSX Manager の設定の変更はブロックされません。論理ネットワークへの追加と変更は許可されます。新しい仮想マシンのプロビジョニングは、アップグレードが実行中でないホスト上で引き続き機能します。アップグレードが進行中のホストはメンテナンス モードになるため、仮想マシンはパワーオフするか、別のホストに退避させる必要があります。これは、DRS を使用するか、手動で実行できます。

## NSX Distributed Firewall への vShield App の移行

ホスト クラスタをアップグレードすると、vShield App の設定は Distributed Firewall に移行されます。

アップグレード中：

- 移行中は、既存のフィルタが引き続き動作します。
- 移行中は、フィルタの追加や変更をしないでください。

アップグレード後：

- 移行した各セクションおよびルールが正常に機能していることを確認します。
- 移行後は、NSX の [サービス デプロイ] ページから vShield App を削除します。

## vShield Edge のアップグレード

ホストをアップグレードしているかどうかに関係なく、vShield Edge をアップグレードできます。ホストをアップグレードしていなくても、vShield Edge をアップグレードすることは可能です。



**警告:** vCloud Director 8.10 より前のバージョンを使用している場合は、NSX Edge をアップグレードしないでください。[\[vCloud Director 環境での vShield Edge アップグレードの決定\]](#) を参照してください。

アップグレード中：

- アップグレード中の vShield Edge デバイスでは、設定の変更はブロックされます。
- パケット転送は一時的に中断されます。
- 論理スイッチへの追加と変更は許可されます。
- 新しい仮想マシンのプロビジョニングは引き続き機能します。

アップグレード後：

- 設定の変更はブロックされません。NSX へのアップグレードで導入された新機能は、NSX Controller がインストールされ、すべてのホスト クラスタが NSX バージョン 6.2.x にアップグレードされるまで設定できません。
- L2 VPN は、アップグレード後に再設定する必要があります。
- SSL VPN クライアントは、アップグレード後に再インストールする必要があります。

## ゲスト イントロスペクションへの vShield Endpoint の移行

NSX 6.x では、vShield Endpoint の名称はゲスト イントロスペクションに変更されました。NSX Manager をアップグレードした後に、[Networking and Security] - [インストール手順] - [サービス デプロイ] の順に移動すると、ゲストイントロスペクションサービスに[アップグレード]リンクが表示されます。vCloud Networking and Security を NSX にアップグレードする場合、ゲスト イントロスペクション仮想アプライアンスとホスト エージェントが、ゲスト イントロスペクションが有効なクラスタの各ホストに展開されます。

アップグレード中：

- 仮想マシンの追加や vMotion による移行または削除など、仮想マシンが変更される場合、NSX クラスタの仮想マシンは保護されなくなります。

アップグレード後：

- 仮想マシンの追加、削除、また vMotion の実行中、仮想マシンは保護されます。

## vCloud Networking and Security の動作状態の確認

アップグレードを開始する前に、vCloud Networking and Security の動作状態をテストすることが重要です。このテストを実施しないと、アップグレード後に問題が発生した場合に、それがアップグレード プロセスによるものなのか、アップグレード プロセス以前から存在していたのかを判断することができなくなります。

vCloud Networking and Security のアップグレードを開始する前に、環境内のすべてに問題がないか確認する必要があります。必ず最初に確認を行います。

アップグレード前のチェックリストとして次の手順を実行します。

## 手順

- 1 管理者ユーザーの ID とパスワードを特定します。
- 2 正引きと逆引きの名前解決が、すべてのコンポーネントで動作していることを確認します。
- 3 すべての vSphere と vShield コンポーネントにログインできることを確認します。
- 4 vShield Manager、vCenter Server、ESXi および vShield Edge の現在のバージョンを記録します。
- 5 VXLAN セグメントが機能することを確認します。

パケット サイズを正しく設定し、DF ビットを含めるようにします。

- 異なるホストの同じ仮想ワイヤー上にある 2 台の仮想マシン間で ping を実行します。
  - Windows 仮想マシンから : `ping -l 1472 -f <dest VM>`
  - Linux 仮想マシンから : `ping -s 1472 -M do <dest VM>`
- 2 つのホストの VTEP インターフェイス間で ping を実行します。
  - `ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>`

---

**注:** ホストの VTEP IP を取得するには、ホストの [管理 (Manage)] > [ネットワーク (Networking)] > [仮想スイッチ (Virtual Switches)] ページで、vmknics IP アドレスを探します。

---

- 6 仮想マシンから ping を実行して、外部ネットワークとの接続性を確認します。
- 7 NSX Edge デバイスの BGP と OSPF の状態を記録します。
- 8 vShield 環境を視覚的に確認して、すべてのステータス インジケータが緑、正常、デプロイ済みの状態であることを確認します。
- 9 Syslog が設定されていることを確認します。
- 10 可能な場合は、アップグレード前の環境で、新しいコンポーネントをいくつか作成して機能をテストします。
- 11 netcpad および vsfwd の user-world agent (UWA) の接続を検証します。
  - ESXi ホストで `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` を実行して、コントローラの接続状態を確認します。
  - vShield Manager で `show tech-support save session` コマンドを実行し、5671 を検索して、すべてのホストが vShield Manager に接続されていることを確認します。
- 12 (オプション) テスト環境がある場合は、本番環境をアップグレードする前に、アップグレードとアップグレード後の機能をテストします。

## ローカル管理者ユーザーの CLI 管理者ユーザーへの移行

NSX 6.x より前のシリーズでは、ユーザー admin はローカル データベース ユーザーでした。NSX 6.0 から、ユーザー admin は CLI ユーザーになりました。後方互換性を保つため、管理者ユーザーを移行するための手順があります。

vCloud Networking and Security 5.x シリーズでは、CLI の管理者ユーザーとユーザー インターフェイス (VSM) の管理者ユーザーは異なっていました。CLI のユーザー admin のパスワードは OS で管理され、VSM ユーザーのパスワードは、ユーザーのローカル データベースで管理されていました。CLI 管理者ユーザーのパスワードを変更しても、この変更は VSM 管理者ユーザーのパスワードには影響しませんでした。同様に、VSM 管理者ユーザーのパスワードを変更しても、この変更は CLI 管理者パスワードには影響しませんでした。

NSX 6.x シリーズでは、VSM ユーザー データベースの使用は現在推奨されていません。CLI ユーザーは NSX Manager に直接ログインできます。

アップグレードシナリオでは、後方互換のため、管理者ユーザーが CLI データベースと Web ユーザー インターフェイス データベースの両方に存在します。この場合、CLI ユーザーのパスワードが変更されても、変更はユーザー インターフェイスまたは REST API の呼び出しには反映されません。NSX 6.x より前のシリーズでは、CLI ユーザーはユーザー インターフェイスまたは REST API にはログインできませんでした。

NSX 6.x シリーズの新規 (グリーン フィールド) デプロイの場合、CLI ユーザーと NSX Manager (ユーザー インターフェイスまたは REST) は同じであり、認証情報も同じです。

アップグレードした NSX デプロイを、NSX 6.x の新規デプロイと同じように動作させるには、2 つのオプションがあります。

- オプション 1 --- データベースの管理者ユーザーのパスワードを変更します。

次の REST API を使用してパスワードを変更できます。このオプションでは、古いパスワードを知っている必要があります。

PUT URI /api/2.0/services/usermgmt/user/local/<userId>

```
<userInfo>
  <userId></userId>
  <password></password>
  <fullname></fullname>
  <email></email>
  <accessControlEntry>
    <role></role>
    <resource>
      <resourceId></resourceId>
      ...
    </resource>
  </accessControlEntry>
</userInfo>
```

たとえば、curl を使用して、次のように指定します。

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml'
-X PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d
'<userInfo><userId>admin</userId><password>123</password><fullname>admin</fullname><email>
admin@company.com</email><accessControlEntry><role>security_admin</role><resource><resourceId>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
```

この API は、パスワードを含むローカル ユーザー アカウントの更新に使用できます。パスワードが提供されない場合は、既存のパスワードが保持されます。URI の userId 変数は、XML に指定されたものと同じにする必要があります。



- オプション 2 --- Web ユーザー インターフェイス管理者ユーザーを維持せずに削除し、CLI 管理者ユーザーにロールを追加できます。この変更を行うと、CLI ユーザーの認証情報を使用して NSX Manager にログインすることができ、CLI 管理者ユーザーのパスワード変更は NSX Manager の管理者ユーザーに反映されます。

Web ユーザー インターフェイスの管理者ユーザーは `super_user` であるため、Web ユーザー インターフェイス管理者ユーザーを削除する前に、`super_user` 権限を持つ別のユーザーを追加する必要があります。

- `super_user` ロールを持つ新しいユーザー `tempadmin` を追加します。

たとえば、`curl` を使用して、次のように指定します。

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d '<userInfo><userId>tempadmin</userId><password>123</password><fullname>tempadmin</fullname><email>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resource><resourceId>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
```

- `tempadmin` を使用して Web ユーザー インターフェイスのユーザー `admin` を削除します。

たとえば、`curl` を使用して、次のように指定します。

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X DELETE https://<vsm-ip>/api/2.0/services/usermgmt/user/admin
```

- CLI ユーザー `admin` に `super_user` ロールを追加します。

たとえば、`curl` を使用して、次のように指定します。

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X POST https://<nsx-ip>/api/2.0/services/usermgmt/role/admin?isCli=true -d '<accessControlEntry><role>super_user</role></accessControlEntry>'
```

## vShield Data Security のアンインストール

環境内に Data Security がある場合は、NSX にアップグレード前にアンインストールしておきます。

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

### 手順

- 1 vShield Manager 5.5 のインベントリ パネルから、[Datacenters] フォルダを展開し、vShield Data Security がインストールされているホストに移動します。

- 2 vShield Data Security がインストールされている各ホストで、次の手順を完了して、アンインストールします。
  - a ホストをクリックして、[vShield ホスト準備] ペインの [サマリ (Summary)] タブで、vShield Data Security の [アンインストール (Uninstall)] リンクをクリックします。
  - b [アンインストールするサービスを選択します] ペインで、vShield Data Security が選択されていることを確認し、[アンインストール (Uninstall)] ボタンをクリックします。

vShield Data Security がアンインストールされ、[vShield ホスト準備] ペインに、**インストールされていません** という状態が表示されます。

## vCloud Networking and Security のバックアップとリストア

すべての vCloud Networking and Security コンポーネントを正しくバックアップすることは、障害が発生した場合にシステムを正常動作の状態にリストアするために重要です。

vShield Manager のバックアップには、仮想ワイヤ、ルーティング エンティティ、セキュリティ、vApp ルール、および vShield Manager ユーザー インターフェイスや API でユーザーが行ったその他のすべての設定含む、あらゆる vShield 設定が含まれます。vCenter データベースと仮想スイッチのような関連要素は、別々にバックアップする必要があります。

少なくとも、定期的に vShield Manager と vCenter Server のバックアップを作成することをお勧めします。バックアップの頻度とスケジュールは、ビジネス上のニーズと操作手順によって異なる場合があります。設定の変更を何度も行う場合は、頻繁に vCloud Networking and Security のバックアップを作成することをお勧めします。

vShield Manager のバックアップは、オンデマンドで作成することも、時間単位、日単位、または週単位で作成することもできます。

次の場合にバックアップを作成することをお勧めします。

- vCloud Networking and Security または vCenter Server をアップグレードする前。
- vCloud Networking and Security または vCenter Server をアップグレードした後。
- 仮想スイッチ、Edge、セキュリティ、ファイアウォール ポリシーを作成した後など、vCloud Networking and Security コンポーネントをデプロイした当日や初期設定の後。
- インフラストラクチャまたはトポロジを変更した後。
- 2 日目に大きな変更を行った後。

任意の時点でシステム全体をロールバックできるように、vCloud Networking and Security コンポーネントのバックアップを vCenter Server、クラウド管理システム、操作ツールなどの他の連携コンポーネントのバックアップと同時に実行することをお勧めします。

## vShield Manager データのオン デマンド バックアップ

オンデマンド バックアップにより、いつでも vShield Manager のデータをバックアップできます。

### 手順

- 1 vShield Manager インベントリ パネルから [設定とレポート (Settings & Reports)] をクリックします。
- 2 [構成 (Configuration)] タブをクリックします。

- 3 [バックアップ (Backups)] をクリックします。
- 4 (オプション) システム イベント テーブルをバックアップしない場合は、[システム イベントの除外 (Exclude System Events)] チェック ボックスをオンにします。
- 5 (オプション) 監査ログ テーブルをバックアップしない場合は、[監査ログの除外 (Exclude Audit Logs)] チェック ボックスをオンにします。
- 6 バックアップの保存先であるシステムの [ホスト IP アドレス (Host IP Address)] を入力します。
- 7 バックアップシステムの [ホスト名 (Host Name)] を入力します。
- 8 バックアップシステムにログインするために必要な [ユーザー名 (User Name)] を入力します。
- 9 [パスワード (Password)] フィールドに、バックアップシステムにログインするユーザー名に対応するパスワードを入力します。
- 10 [バックアップディレクトリ (Backup Directory)] フィールドに、バックアップの保存先の絶対パスを入力します。
- 11 [ファイル名の接頭辞 (Filename Prefix)] に文字列を入力します。

この文字列はバックアップ ファイル名の前に追加されるため、バックアップ システム上でファイルを容易に区別できるようになります。例えば **ppdb** と入力すると、バックアップ ファイル名は **ppdbHH\_MM\_SS\_DayDDMonYYYY** となります。

- 12 [パス フレーズ (Pass Phrase)] を入力してバックアップ ファイルを保護します。

vCloud Networking and Security では、パス フレーズの入力はオプションでした。NSX では、パス フレーズは必須です。

- 13 [転送プロトコル (Transfer Protocol)] ドロップダウン メニューで、[SFTP] または [FTP] を選択します。

- 14 [バックアップ (Backup)] をクリックします。

完了すると、バックアップはこのフォームの下テーブルに表示されます。

- 15 [設定の保存 (Save Settings)] をクリックして設定を保存します。

すべてのバックアップを 1 つのディレクトリに保存している場合、バックアップの表示に問題が発生することがあります。ベスト プラクティスとして、時折アーカイブフォルダにバックアップ ファイルを移動することをお勧めします。

## vSphere Distributed Switch のバックアップ

vSphere Distributed Switch (VDS) および分散ポート グループの設定をファイルにエクスポートできます。

有効なネットワーク設定がファイルに保存され、ほかのデプロイ環境で利用できるようになります。

この機能は、vSphere Web Client 5.1 以降でのみ使用できます。VDS 設定およびポートグループ設定は、インポートの一環としてインポートされます。

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

## vCenter Server のバックアップ

NSX デプロイを保護するには、vCenter Server データベースをバックアップして仮想マシンのスナップショットを作成することが重要です。

vCenter Server のバックアップとリストアの手順、およびベスト プラクティスについては、お使いのバージョンの vCenter Server ドキュメントを参照してください。

仮想マシンのスナップショットについては、<http://kb.vmware.com/kb/1015180> を参照してください。

vCenter Server 5.5 に役立つリンク：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

vCenter Server 6.0 に役立つリンク：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

## vShield Manager から NSX へのアップグレード バンドルのダウンロードと MD5 の確認

vShield Manager から NSX へのアップグレード バンドルには、NSX インフラストラクチャのアップグレードに必要なすべてのファイルが含まれています。vShield Manager をアップグレードする前に、まず、アップグレードするバージョンに対応したアップグレード バンドルをダウンロードする必要があります。

### 前提条件

MD5 チェックサム ツールを用意します。

### 手順

- 1 vShield Manager から NSX へのアップグレード バンドルを、vShield Manager から参照できる場所にダウンロードします。アップグレード バンドルのファイル名は、**VMware-vShield-Manager-upgrade-bundle-to-NSX-<releaseNumber>-<NSXbuildNumber>.tar.gz** のような形式になっています。
- 2 アップグレード バンドルのファイル名の最後が tar.gz になっていることを確認します。

一部のブラウザでファイル拡張子を変更される場合があります。たとえば、ダウンロード ファイルの名前が VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz の場合は、次のように名前を変更します。

VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.tar.gz

このように変更しないと、アップグレード バンドルのアップロード後に次のようなエラー メッセージが表示されます。「無効なアップグレードバンドルファイルVMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz です。アップグレード ファイル名の拡張子は tar.gz です。」

- 3 MD5 チェックサム ツールを使用して、VMware Web サイトに公開されているアップグレード バンドルの公式な MD5 サムと、チェックサム ツールで計算された MD5 サムを比較します。
  - a MD5 チェックサム ツールで、アップグレード バンドルを参照します。
  - b ツールを使用して、バンドルのチェックサムを計算します。
  - c VMware Web サイトにリストされているチェックサムをコピーアンドペーストします。
  - d ツールを使用して 2 つのチェックサムを比較します。2 つのチェックサムが一致しない場合は、アップグレード バンドルのダウンロードをやり直します。

## vCloud Director 環境のアップグレード準備の追加手順

vCloud Director のネットワークの分離 (VCDNI) は NSX でサポートされますが、このテクノロジーの使用は現在推奨されていません。

VXLAN が広く導入される前、vCloud Director は vCloud ネットワーク分離テクノロジーを使用して、論理ネットワーク オーバーレイを提供していました。この MAC-in-MAC の独自のカプセル化は現在でもサポートされていますが、現在は推奨されないテクノロジーです。VXLAN とは異なり、VCDNI 論理ネットワークは vCloud Director によって直接作成されます。vCloud Director は、VMkernel で実行される vCloud エージェントを経由して、ESXi ホストと通信します。したがって、vCloud Networking and Security をアップグレードしても VCDNI ネットワークに影響しないことから、VCDNI ネットワークと NSX を併用することに制限はありません。

しかし、VCDNI は廃止されたテクノロジーであり、サポート対象はレガシー環境でのみであるため、VXLAN テクノロジーの使用が推奨されます。

## vCloud Networking and Security 5.5.x から NSX 6.2.x へのアップグレード

NSX 6.2.x にアップグレードするには、本書に記載された順序で各 vCloud Networking and Security コンポーネントをアップグレードする必要があります。

vCloud Networking and Security コンポーネントは次の順序で NSX にアップグレードする必要があります。

- 1 vShield Manager から NSX Manager へのアップグレード
- 2 NSX Controller クラスタの展開 (オプション)。分散論理ルーターと、制御プレーンのモードをハイブリッドまたはユニキャストに変更するために必要
- 3 ホスト クラスタの更新
- 4 トランスポート ゾーンの更新 (オプション)。NSX Controller クラスタを展開している場合、ハイブリッドまたはユニキャストに変更可能
- 5 vShield App から NSX 分散ファイアウォールへのアップグレード
- 6 vShield Edge から NSX Edge へのアップグレード
- 7 vShield Endpoint から NSX ゲスト イントロスペクションへのアップグレード

アップグレード プロセスは、vShield Manager によって管理されます。コンポーネントのアップグレードが失敗または中断されたためにアップグレードをやり直したまたは再開する場合、プロセスは、最初からではなく中断された時点から開始されます。

---

**重要:** 環境内で仮想ワイヤーがある場合は、NSX Manager へのアップグレード後にホスト クラスタを更新する必要があります。

---

## vShield Manager から NSX Manager へのアップグレード

NSX インフラストラクチャのアップグレード プロセスでは、最初に NSX Manager アプライアンスのアップグレードを行います。



**警告:** vShield Manager アプライアンスのデプロイ済みインスタンスはアンインストールしないでください。

---

### 前提条件

- システム要件の確認とバックアップの作成も含めて、[「NSX にアップグレードするための vCloud Networking and Security の準備」](#)に記載されているアップグレード準備タスクがすべて完了していることを確認します。
- NSX Manager へのアップグレードに必要なディスク容量が vShield Manager にあることを確認します。[「NSX のシステム要件」](#)を参照してください。
- NSX 6.2.x にアップグレードする前に、vShield Manager 仮想アプライアンスの予約済みメモリを 16 GB 以上に増加し、仮想 CPU を 4 個割り当てます。  
[「NSX のシステム要件」](#)を参照してください。
- vShield Edge 5.5 より前のバージョンのインスタンスの場合は、すべて Shield バージョン 5.5 にアップグレードしてください。

---

vShield Manager を NSX Manager にアップグレードした後は、vShield Edge 5.5 より前のバージョンのインスタンスを管理または削除できません。

---

### 手順

- 1 vShield Manager から参照できる場所に NSX のアップグレード バンドルをダウンロードします。アップグレード バンドル ファイルは、**VMware-vShield-Manager-upgrade-bundle-to-NSX-<release>-<buildNumber>.tar.gz** のような名前になっています。
- 2 vShield Manager 5.5 インベントリ パネルから [設定とレポート] をクリックします。
- 3 [アップデート] タブ、[アップグレード バンドルのアップロード] の順にクリックします。
- 4 [ファイルを選択] を選択し、**VMware-vShield-Manager-upgrade-bundle-to-NSX-<release>-<buildNumber>.tar.gz** ファイルを選択して、[開く] をクリックします。
- 5 [ファイルのアップロード] をクリックします。  
ファイルのアップロードには数分かかります。
- 6 [インストール] をクリックして、アップグレード プロセスを開始します。

- 7 [インストールの確認] をクリックします。アップグレード プロセスによって vShield Manager が再起動されるため、vShield Manager ユーザー インターフェイスへの接続が失われる可能性があります。その他の vShield コンポーネントは再起動されません。
- 8 再起動後、Web ブラウザ ウィンドウを開き、https://10.10.10.10 のように IP アドレスを入力して、NSX Manager 仮想マシンにログインします。アップグレードされた NSX Manager の IP アドレスは、vShield Manager と同じです。  
  
[サマリ] タブにインストールした NSX Manager のバージョンが表示されます。
- 9 [ホーム] - [vCenter Server 登録の管理] の順に移動し、vCenter Server のステータスが **接続中** であることを確認します。
- 10 vSphere Web Client にアクセスしている既存のブラウザ セッションを閉じます。数分待ち、ブラウザ キャッシュをクリアしてから vSphere Web Client に再ログインします。
- 11 vShield Manager で SSH が有効になっていた場合は、アップグレード後に NSX Manager で有効にする必要があります。NSX Manager 仮想アプライアンスにログインし、[サマリの表示] をクリックします。[システム レベルのコンポーネント] で、SSH サービスの [開始] をクリックします。

---

**重要:** vCloud Networking and Security 5.x を NSX 6.x にアップグレードした後は、CLI 管理者のログイン認証情報を使用して、NSX Manager にログインする必要があります。これまで、vCloud Networking and Security では、CLI とユーザー インターフェイスにそれぞれ 1 つ、合わせて 2 つのパスワードが必要でした。NSX 6.x からは、1 つのパスワードのみが必要になります。次はその例です。

vCloud Networking and Security のパスワード

- CLI のパスワード mypassword#123
- ユーザー インターフェイスのパスワード mypassword#456

NSX にアップグレードした後のパスワード

- CLI のパスワード mypassword#123
- ユーザー インターフェイスのパスワード mypassword#123

---

NSX Manager のアップグレード後に、vSphere Web Client からログアウトし、再度ログインする必要があります。

NSX プラグインが vSphere Web Client に正しく表示されない場合、ブラウザのキャッシュと履歴をクリアしてください。この手順を行わないと、vSphere Web Client で NSX の設定を変更したときに「内部エラーが発生しました - エラー #1009」のようなエラーが表示される場合があります。

vSphere Web Client で [Networking and Security] タブが表示されない場合には、vSphere Web Client サーバをリセットします。

- vCenter Server 5.5 で https://<vcenter-ip>:5480 を開き、Web Client サーバを再起動します。

- vCenter Server Appliance 6.0 で、vCenter Server シェルに root ユーザーとしてログインし、次のコマンドを実行します。

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Windows の vCenter Server 6.0 では、次のコマンドを実行するとアップグレードできます。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

異なるバージョンの NSX プラグインが実行中の場合は、予期しないエラーを回避するため、異なるバージョンの NSX Manager を実行している vCenter Server の管理に別々の Web Client を使用することをお勧めします。

NSX Manager がアップグレードされたら、新しい NSX Manager バックアップ ファイルを作成します。[「NSX のバックアップとリストア」](#)を参照してください。以前の NSX Manager バックアップは、以前のリリースに対してのみ有効です。

#### 次のステップ

[「NSX ライセンスのインストールおよび割り当て」](#)。

## NSX ライセンスのインストールおよび割り当て

NSX Manager のアップグレードが完了した後に、vSphere Web Client を使用して、NSX for vSphere のライセンスのインストールと割り当てを実行できます。

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

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

NSX ライセンスに関する FAQ (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>) を参照してください。

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



## 手順

- vSphere 5.5 で、次の手順を実行して NSX のライセンスを追加します。
  - a vSphere Web Client にログインします。
  - b [管理 (Administration)] をクリックして、[ライセンス (Licenses)] をクリックします。
  - c [ソリューション (Solutions)] タブをクリックします。
  - d [ソリューション] リストで NSX for vSphere を選択します。[ライセンス キーの割り当て (Assign a license key)] をクリックします。
  - e ドロップダウン メニューから [新しいライセンス キーの割り当て (Assign a new license key)] を選択します。
  - f ライセンス キーを入力し、この新しいキーのラベル (オプション) を入力します。
  - g [デコード (Decode)] をクリックします。

ライセンス キーをデコードして、そのキーが正しい形式であるか、および資産のライセンス供与に対して十分なキャパシティがあるかを確認します。
  - h [OK] をクリックします。
- vSphere 6.0 で、次の手順を実行して NSX のライセンスを追加します。
  - a vSphere Web Client にログインします。
  - b [管理 (Administration)] をクリックして、[ライセンス (Licenses)] をクリックします。
  - c [資産 (Assets)] タブをクリックして、[ソリューション (Solutions)] タブをクリックします。
  - d [ソリューション] リストで NSX for vSphere を選択します。[すべてのアクション (All Actions)] ドロップダウン メニューから、[ライセンスの割り当て... (Assign license...)] を選択します。
  - e [追加 (+) (Add)] アイコンをクリックします。ライセンス キーを入力して、[次へ (Next)] をクリックします。ライセンスの名前を追加して、[次へ (Next)] をクリックします。[終了 (Finish)] をクリックして、ライセンスを追加します。
  - f 新しいライセンスを選択します。
  - g (オプション) [機能の表示 (View Features)] アイコンをクリックして、このライセンスで有効になっている機能を表示します。[キャパシティ (Capacity)] 列で、ライセンスのキャパシティを確認します。
  - h [OK] をクリックして、新しいライセンスを NSX に割り当てます。

## 次のステップ

[「NSX コントローラ クラスターの展開」](#)。

コントローラを展開しない場合、[「ホスト クラスターの更新」](#)。

## NSX コントローラ クラスタの展開

NSX コントローラは、NSX の論理スイッチングおよびルーティング機能の制御プレーンとして機能する高度な分散状態管理システムです。これは、ネットワーク内のすべての論理スイッチの集中管理ポイントとして機能するもので、すべてのホスト、論理スイッチ (VXLAN)、および分散論理ルーターの情報を管理します。1) 分散論理ルーター、あるいは 2) ユニキャストまたはハイブリッド モードの VXLAN のデプロイを計画する場合、コントローラが必要になります。

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

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

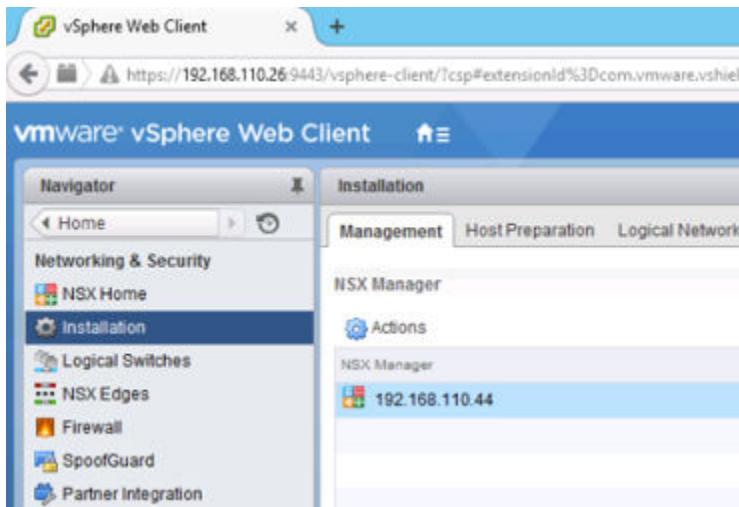
### 前提条件

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

### 手順

- 1 vSphere Web Client で [ホーム] > [Networking and Security] > [インストール] の順に移動し、[管理] タブを選択します。

次はその例です。



- 2 [NSX コントローラ ノード] セクションで、[ノードの追加] (🟢) アイコンをクリックします。

### 3 環境に適した NSX コントローラ設定を入力します。

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

次はその例です。

### 4 コントローラ クラスタの IP アドレス ルールをまだ設定していない場合は、ここで [新規 IP プール] をクリックして設定します。

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

次はその例です。

## 5 コントローラのパスワードを入力し、再入力します。

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

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

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

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

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

### 次のステップ

[「ホスト クラスタの更新」](#)

## ホスト クラスタの更新

vCenter Server の各クラスタ レベルにネットワーク インフラストラクチャ コンポーネントをインストールし、ネットワーク仮想化環境の準備を行う必要があります。これにより、必要なソフトウェアがクラスタ内のすべてのホストにインストールされ、仮想ワイヤーから NSX 論理スイッチに変更されます。このプロセスで、クラスタ内の各ホストはソフトウェアの更新を受け取り、再起動されます。

環境内で仮想ワイヤーがある場合は、NSX Manager へのアップグレード後にホスト クラスタを更新する必要があります。

データ センターのメンテナンス期間中にホスト クラスタを更新することをお勧めします。

DRS が有効である場合、ホストの退避の進捗、メンテナンス モードに入るホスト、およびホストの再起動を監視します。DRS が無効、あるいは手動モードである場合、ホストの退避と再起動は手動で実行する必要があります。ホストの準備中に、警告が発生する場合があります。警告のアイコンをクリックして表示できます。必要な場合は、[解決 (Resolve)] をクリックします。

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

**注:** vCloud Networking and Security で作成された VTEP は、DHCP または手動で割り当てられた IP アドレスを使用します。IP アドレス プールは使用しません。

### 前提条件

- vShield Manager が NSX Manager にアップグレードされていることを確認します。
- [ホストの準備] タブの [VXLAN] 列で、[有効 (Enabled)] と表示されていることを確認します。
- すべてのホストの完全修飾ドメイン名 (FQDN) を解決できることを確認します。

- DRS が無効な場合は、アップグレードを開始する前に、手動で仮想マシンのパワーオフまたは vMotion を実行します。
- DRS が有効な場合は、実行中の仮想マシンは、ホスト クラスタのアップグレード中に自動的に移動されます。アップグレードを開始する前に、環境内で DRS が機能できることを確認します。
  - ホスト クラスタで DRS が有効になっていることを確認します。
  - vMotion が正しく機能していることを確認します。
  - ホストと vCenter Server の接続状態を確認します。
  - 各ホスト クラスタに、少なくとも 3 台の ESXi ホストがあることを確認します。1 台または 2 台のホストを持つホスト クラスタでは、NSX のアップグレード中に、DRS のアドミSSION コントロールの問題が発生することがあります。NSX を正しくアップグレードするため、各ホスト クラスタに少なくとも 3 台のホストを含めることをお勧めします。クラスタに含まれるホストが 3 台より少ない場合は、ホストを手動で退避させることが推奨されます。

## 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [ホストの準備 (Host Preparation)] タブをクリックします。

インフラストラクチャ内のすべてのクラスタが表示されます。

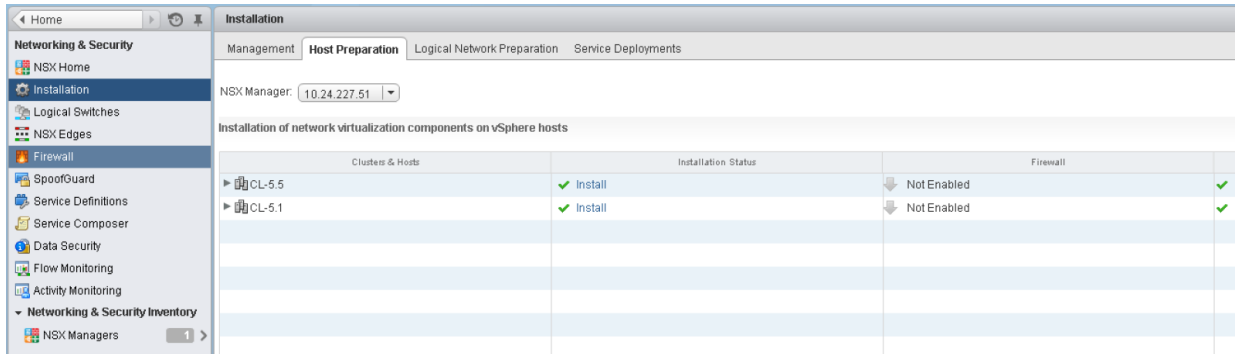
バージョン 5.5 の環境内で仮想ワイヤーを使用していた場合、[インストールの状態 (Installation Status)] 列に [レガシー (legacy)]、[更新 (Update)] および [アンインストール (Uninstall)] と表示されます。

図 1-1. バージョン 5.5 の環境内で仮想ワイヤーを使用している場合、[インストールの状態] が [更新] と表示される

Clusters & Hosts	Installation Status	Firewall	vXLAN
CL-5.5	legacy Update Uninstall	Not Enabled	Enabled
CL-5.1	legacy Update Uninstall	Not Enabled	Enabled

バージョン 5.5 の環境内で仮想ワイヤーを使用していなかった場合、[インストールの状態 (Installation Status)] 列に [インストール (Install)] と表示されます。

図 1-2. バージョン 5.5 の環境内で仮想ワイヤーを使用している場合、[インストールの状態] に [インストール] と表示される



- 4 個々のクラスターで、[インストールの状態] 列の [更新 (Update)] または [インストール (Install)] をクリックします。クラスター内の各ホストが新しい論理スイッチ ソフトウェアを受け取ります。

ホストのアップグレードによりホストのスキャンが開始されます。以前の VIB は削除されます（再起動までは完全には削除されません）。新しい VIB が altboot パーティションにインストールされます。まだ再起動されていないホスト上の新しい VIB を表示するには、`esxcli software vib list --rebooting-image | grep esx` コマンドを実行します。

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

クラスターで DRS が有効になっている場合、DRS は、仮想マシンの動作を停止しない制御された方法で、ホストの再起動を試みます。vMotion は実行中の仮想マシンをクラスター内の他のホストに移動し、ホストをメンテナンス モードにします。

高可用性の要件や DRS ルールの設定など、ホストをメンテナンス モードにする前に手動による作業が必要な場合は、アップグレード プロセスが停止し、クラスターの [インストールの状態 (Installation Status)] に [準備ができていません (Not Ready)] と表示されます。🚨 をクリックしてエラーを表示します。

ホストを手動で退避させた後、クラスターを選択して [解決 (Resolve)] アクションをクリックします。[解決 (Resolve)] アクションにより、アップグレードの完了と、クラスター内の全ホストの再起動が試行されます。何らかの理由でホストの再起動が失敗した場合、[解決 (Resolve)] アクションは停止します。[ホストおよびクラスター (Hosts and Clusters)] ビューでホストを参照し、ホストがパワーオンおよび接続されていて、実行中の仮想マシンが含まれないことを確認します。再び [解決 (Resolve)] アクションを実行します。

5.5 インフラストラクチャ内のすべての仮想ワイヤーの名前が NSX 論理スイッチに変更され、クラスターの [VXLAN] 列に [有効 (Enabled)] と表示されます。

[ホストの準備] タブの [VXLAN] 列に [有効 (Enabled)] と表示されていることを確認します。

クラスターが更新されると、[インストールの状態 (Installation Status)] 列に更新が完了したソフトウェア バージョンが表示されます。

ホストの更新を確認するには、クラスター内のホストのいずれかにログインして `esxcli software vib list | grep esx` コマンドを実行します。次の VIB が正しいバージョンに更新されたことを確認します。

- esx-vsip

## ■ esx-vxlan

**注:** NSX 6.2 では、esx-dvfilter-switch-security VIB は、esx-vxlan VIB の中に組み込まれています。

ホストのアップグレードに失敗した場合は、次のトラブルシューティング手順を実行します。

- vCenter Server の ESX Agent Manager で、アラートおよびエラーを確認します。
- ホストにログインし、`/var/log/esxupdate.log` ログ ファイルで最近のアラートとエラーを確認します。
- DNS と NTP がホストに設定されていることを確認します。

### 次のステップ

#### [\[VXLAN ポートの変更\]](#)

## VXLAN ポートの変更

VXLAN トラフィックに使用するポートを変更できます。

NSX 6.2.3 以降では、デフォルトの VXLAN ポートは 4789 となり、標準ポートは IANA により割り当てられます。NSX 6.2.3 より前では、デフォルトの VXLAN UDP ポート番号は 8472 でした。

すべての新しい NSX インストール環境では、VXLAN に UDP ポート 4789 が使用されます。

NSX 6.2.2 以前のバージョンから NSX 6.2.3 以降にアップグレードする場合、アップグレード前の NSX で以前のデフォルト (8472) またはカスタム ポート番号 (8888 など) が使用されていた場合は、アップグレード後も、ユーザーが変更しない限り、引き続きそのポートが使用されます。

アップグレードされた NSX でハードウェア VTEP ゲートウェイ (ToR ゲートウェイ) が使用されている、またはその予定がある場合は、VXLAN ポート 4789 に切り替える必要があります。

Cross-vCenter NSX では、VXLAN ポートに 4789 を使用する必要はありませんが、同じ VXLAN ポートを使用するように Cross-vCenter NSX 環境にあるすべてのホストを設定する必要があります。ポート 4789 に切り替えると、Cross-vCenter NSX に追加される新しいすべての NSX インストール環境では、既存の NSX 環境と同じポートが使用されます。

VXLAN ポートの変更は 3 つのプロセスで行われ、処理中に VXLAN のトラフィックが中断されることはありません。

- 1 NSX Manager は、古いポートと新しいポートの両方で VXLAN トラフィックを待機するようにすべてのホストを設定します。ホストは引き続き、古いポートで VXLAN トラフィックを送信します。
- 2 NSX Manager は、新しいポートでトラフィックを送信するようにすべてのホストを設定します。
- 3 NSX Manager は、古いポートでの待機を停止するようにすべてのホストを設定します。すべてのトラフィックは新しいポートで送受信されます。

Cross-vCenter NSX 環境では、プライマリ NSX Manager でポート変更を開始する必要があります。各ステージにおいて、次のステージに進む前に、Cross-vCenter NSX 環境内のすべてのホストで設定変更が行われます。

### 前提条件

- VXLAN に使用するポートがファイアウォールによってブロックされていないことを確認します。
- VXLAN ポートの変更時にホストの準備が実行されないことを確認します。

## 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [論理ネットワークの準備 (Logical Network Preparation)] タブをクリックし、次に [VXLAN 転送 (VXLAN Transport)] をクリックします。
- 4 [VXLAN ポート] パネルの [変更 (Change)] ボタンをクリックします。切り替え先のポートを入力します。4789 は、IANA が VXLAN 用に割り当てているポート番号です。

すべてのホストにポートの変更が適用されるまで、少し時間がかかります。

- 5 (オプション) ポート変更の進捗状況を確認するには、API 要求 `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` を使用します。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TW0</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

## 次のステップ

[「トランスポート ゾーンと論理スイッチの更新」](#)。

## トランスポート ゾーンと論理スイッチの更新

NSX Controller クラスタを展開すると、論理ネットワークでマルチキャストに依存する必要がなくなります。トランスポート ゾーンと論理スイッチの制御プレーン モードをユニキャストまたはハイブリッドに更新できます。

制御プレーン モードの変更や既存の論理スイッチの移行を行っても、ネットワーク データ プレーンのトラフィックに影響しません。



## 手順

- 1 vSphere Web Client で、[ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [論理ネットワークの準備 (Logical Network Preparation)] - [トランスポート ゾーン (Transport Zones)] の順に移動します。
- 2 トランスポート ゾーンを選択して、[アクション (Actions)] - [設定の編集 (Edit Settings)] の順にクリックします。次のように、必要なレプリケーション モードを選択します。
  - [マルチキャスト (Multicast)] : 物理ネットワーク上のマルチキャスト IP アドレスを制御プレーンに使用します。このモードは、古い VXLAN デプロイからアップグレードする場合にのみ推奨されます。物理ネットワークに PIM/IGMP が必要です。
  - [ユニキャスト (Unicast)] : 制御プレーンは、NSX コントローラによって処理されます。すべてのユニキャストトラフィックで、最適化されたヘッドエンド レプリケーションを利用します。マルチキャスト IP アドレスや特別なネットワーク設定は必要ありません。
  - [ハイブリッド (Hybrid)] : ローカルトラフィック レプリケーションを物理ネットワーク (L2 マルチキャスト) にオフロードします。最初のホップのスイッチで IGMP スヌーピング、各 VTEP サブネットでは IGMP クエリアへのアクセスが必要ですが、PIM は不要です。最初のホップスイッチは、サブネットのトラフィック レプリケーションを処理します。
- 3 [既存の論理スイッチを新しい制御プレーン モードに移行します。 (Migrate existing Logical Switches to the new control plane mode)] のチェック ボックスを選択して [OK] をクリックします。

## 次のステップ

[\[vShield App から Distributed Firewall へのアップグレード\]](#)。

## vShield App から Distributed Firewall へのアップグレード

Distributed Firewall へのアップグレードは、vShield App バージョン 5.5 からのみ可能です。vShield App 5.5 より前のバージョンをインフラストラクチャで使用している場合は、バージョン 6.2.x にアップグレードする前に 5.5 にアップグレードする必要があります。バージョン 5.5 へのアップグレードの詳細については、バージョン 5.5 の『vShield インストールとアップグレード ガイド』を参照してください。

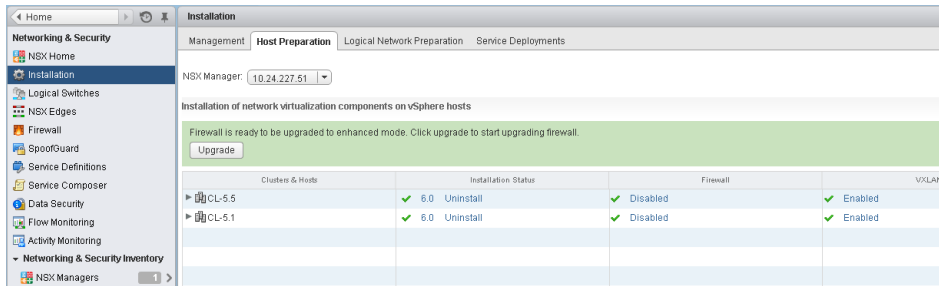
次の手順に要する時間は、ユーザー環境のルールの数によって変わります。vShield App から NSX Distributed Firewall (拡張モード) に移行する場合、ルールが移行されプッシュされます。これにより、トラフィックの中断が発生します。この作業は、メンテナンス期間中に完了する必要があります。

## 前提条件

- vShield Manager が NSX Manager にアップグレードされている。
- 仮想ワイヤーが NSX 論理スイッチにアップグレードされている。VXLAN ユーザーでない場合は、ネットワーク仮想化コンポーネントをインストールしている。
- vShield App 5.5 のルールを Distributed Firewall に移行する場合、Distributed Firewall にアップグレードする前に、vShield App アプライアンスを削除しないでください。

## 手順

- 1 環境のすべてのクラスタでネットワーク仮想化コンポーネントへの準備が完了すると、ファイアウォールをアップグレードする準備ができたことを示すメッセージが表示されます。



- 2 [アップグレード (Upgrade)] をクリックします。

vShield App 5.5 のルールは、次の方法で NSX に移行されます。

- a 中央のファイアウォール テーブルには、vShield App バージョン 5.5 で設定される名前空間（データセンターと仮想ワイヤー）ごとに新しいセクションが作成されます。各セクションには、対応するファイアウォール ルールが含まれます。
- b [AppliedTo] フィールドは、各セクションのすべてのルールで同じ値になります。これには、データセンター名前空間のデータセンター ID、仮想ワイヤー名前空間の仮想ワイヤー ID、およびポート グループ ベースの名前空間のポート グループ ID が含まれます。
- c 異なる名前空間レベルで作成されたコンテナはグローバル レベルに移動されます。
- d アップグレード後もファイアウォールの動作が変わらないよう、セクションの順序は次のようになります。

```
<Section_Namespace_Portgroup-1>
.....
<Section_Namespace_Portgroup-N>
<Section_Namespace_VirtualWire-1 >
.....
<Section_Namespace_VirtualWire-N>
<Section_Namespace_Datacenter_1>
.....
<Section_Namespace_Datacenter_N>
<Default_Section_DefaultRule >
```

アップグレードの完了後、[ファイアウォール] 列に [有効 (Enabled)] と表示されます。

- 3 [ホーム (Home)] - [ホストとクラスタ (Hosts and Clusters)] の順にクリックし、vShield App サービス仮想マシンを実行しているホストの順に移動します。レガシーの vShield App サービス仮想マシンをシャットダウンします。

- 4 [Networking and Security (Networking & Security)] - [ファイアウォール (Firewall)] の順に移動し、アップグレードした各セクションとルールを確認して、問題なく機能することを確認します。
- 5 [インストール手順 (Installation)] - [サービス デプロイ (Service Deployments)] タブの順に移動して、すべてのアラームが解決し、レガシーの vShield App サービス ステータスが [成功しました (Succeeded)] と表示されていることを確認します。
- 6 ルールが正常に機能している場合、[サービス デプロイ (Service Deployments)] タブで vShield App を選択し、[サービス デプロイを削除します (Delete Service Deployment)](✖) をクリックして、レガシーの vShield App サービス仮想マシンを削除します。

#### 次のステップ

[\[vShield Edge から NSX Edge へのアップグレード\]](#)

## vShield Edge から NSX Edge へのアップグレード

NSX Edge 6.2.x へのアップグレードは、vShield Edge 5.5 からのみ可能です。vShield Edge 5.5 より前のバージョンをインフラストラクチャに使用している場合は、バージョン 6.2.x にアップグレードする前にバージョン 5.5 にアップグレードする必要があります。バージョン 5.5 へのアップグレードの詳細については、『vShield インストールとアップグレード ガイド』バージョン 5.5 を参照してください。

アップグレード プロセス中、新しい Edge 仮想アプライアンスは既存のものと一緒にデプロイされます。新しい Edge の準備ができると、古い Edge の vNIC が切断され、新しい Edge の vNIC が接続されます。次に、新しい Edge は、接続されたスイッチの ARP キャッシュを更新するために、Gratuitous ARP (GARP) パケットを送信します。高可用性構成の場合は、アップグレード プロセスが 2 回実行されます。

このプロセスが、パケットの転送に一時的に影響する場合があります。Edge が ECMP モードで動作するように設定することで、この影響を抑えることができます。

グレースフル リスタートが有効ではない場合、アップグレード中に OSPF 近接関係が取り出されます。

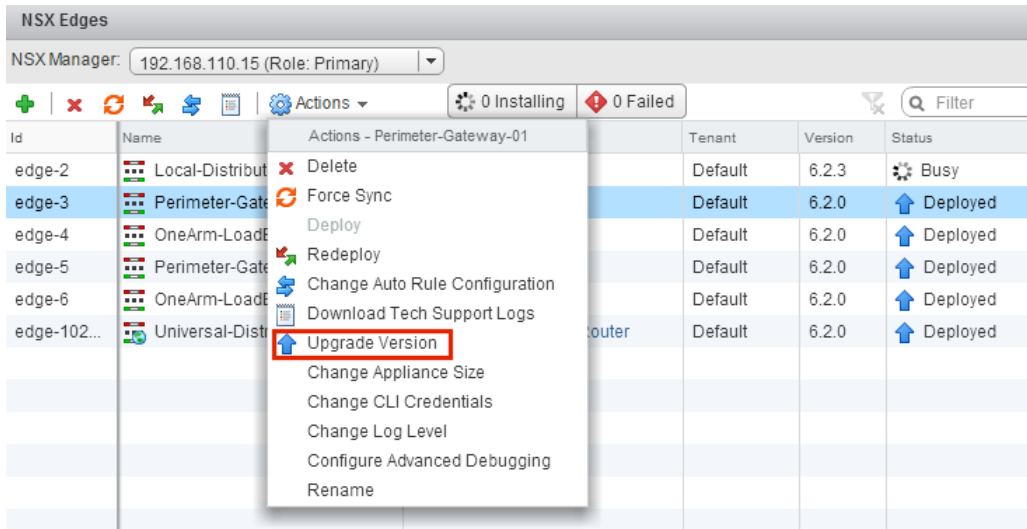
#### 前提条件

- vShield Manager が NSX Manager にアップグレードされていることを確認します。
- NSX Edge のアップグレード進行中に発生する運用上の影響について理解しておく必要があります。[\[vCloud Networking and Security のアップグレードによる動作上の影響\]](#) を参照してください。
- NSX 論理スイッチを作成する計画がない場合でも、ローカル セグメント ID プールがあることを確認します。
- アップグレード中に追加の NSX Edge Services Gateway アプライアンスを展開するための十分なリソースがホストにあることを確認します。これは特に複数の NSX Edge アプライアンスを並行してアップグレードする場合に重要です。各サイズの NSX Edge で必要とされるリソースについては、[\[NSX のシステム要件\]](#) を参照してください。
- アップグレード時は、1 台の NSX Edge インスタンスにつき、フルサイズの新しい NSX Edge アプライアンスがもう 1 台ホスト上に存在し、2 台ともパワーオン状態となります。

- NSX 6.2.3 以降は、高可用性 (HA) 構成の 2 台の NSX Edge インスタンスを再デプロイする場合、2 台の新しいアプライアンスをデプロイしてから、2 台の古いアプライアンスと置き換えます。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 4 台存在することになります。NSX Edge インスタンスがアップグレードされると、高可用性アプライアンスのいずれかがアクティブになります。
- NSX 6.2.3 より前は、HA 構成の NSX Edge インスタンスのアップグレードで古いアプライアンスを置き換える場合、一度につき新しいアプライアンスを 1 台展開していました。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 3 台存在することになります。NSX Edge インスタンスがアップグレードされると、通常は HA インデックスが 0 の NSX Edge アプライアンスがアクティブになります。
- L2 VPN が有効になっている場合、バージョン 5.5 または 6.0 の NSX Edge はアップグレードできません。アップグレードの前に、L2 VPN 設定を削除する必要があります。L2 VPN は、アップグレード後に再設定できます。詳細については、『NSX インストール ガイド』の「L2 VPN の概要」を参照してください。

#### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 各 NSX Edge インスタンスで、[操作 (Actions)] メニューから [アップグレード バージョン (Upgrade Version)] を選択します。



「Edge アプライアンスをデプロイできませんでした。」というエラーメッセージが出てアップグレードが失敗した場合は、NSX Edge アプライアンスがデプロイされているホストが接続されており、メンテナンス モードになっていないことを確認します。

NSX Edge が正常にアップグレードされると、[ステータス (Status)] は [デプロイ済み] になり、[バージョン (Version)] 列に NSX のバージョンが表示されます。

Edge のアップグレードが失敗し、以前のバージョンにロールバックしない場合は、[NSX Edge の再デプロイ (Redeploy NSX Edge)] アイコンをクリックして、アップグレードを再試行します。

NSX Edge ファイアウォール ルールは sourcePort をサポートしていないため、sourcePort を含むバージョン 5.5 の vShield Edge ルールはアップグレード中に次のように変更されます。

- ルールで application が使用されていない場合、サービスは「protocol=any」、「port=any」、および「sourcePort=asDefinedInTheRule」として作成されます。
- ルールに application または applicationGroup が使用されている場合、sourcePort を追加することで、これらのグループオブジェクトが重複します。このため、ファイアウォール ルールで使用する groupingObjectId がアップグレード後に変更されます。

NSX Edge 6.x のユーザー ファイアウォール ルールでは、REST API からの入力に基づく内部 IPSet および applicationSet を生成しません。代わりに、これらを未加工のまま保持します。アップグレード中に、内部で生成された IPSet と applicationSet は、raw データでルールを作成する際に使用されます。内部 groupingObject は、ユーザーのファイアウォール ルールには表示されなくなります。

#### 次のステップ

必要な場合、L2 VPN 設定を再度行います。L2 VPN の概要については、『NSX インストール ガイド』を参照してください。

[「ゲスト イントロスペクションのアップグレード」](#)

## vShield Endpoint から NSX ゲスト イントロスペクションへのアップグレード

ゲスト イントロスペクションをアップグレードする場合、NSX Manager と同じバージョンにすることが重要です。

---

**注:** ゲスト イントロスペクション サービス仮想マシンは、vSphere Web Client からアップグレードできます。NSX Manager のアップグレード後に、サービス仮想マシンをアップグレードするために削除する必要はありません。サービス仮想マシンを削除すると、エージェント仮想マシンが欠落するため、サービス ステータスが**失敗**と表示されます。[解決 (Resolve)] をクリックして新しいサービス仮想マシンを展開し、[アップグレードを利用可能 (Upgrade Available)] をクリックして最新のゲスト イントロスペクション サービス仮想マシンを展開します。

---

#### 前提条件

NSX Manager、コントローラ、準備済みホスト クラスタ、および NSX Edge が 6.2.x にアップグレードされている必要があります。

## 手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	✓ Succeeded ↑ Upgrade Available	✓ Up	Comp...	ds-site...	vds-sit...	GI Pool

[インストールの状態 (Installation Status)] 列に [アップグレードを利用可能 (Upgrade Available)] と表示されます。

- 2 アップグレード対象のゲスト イントロスペクション デプロイを選択します。  
サービス テーブルの上のツールバーで、[アップグレード (Upgrade)] (↑) アイコンが有効になります。
- 3 [アップグレード (Upgrade)] (↑) アイコンをクリックして、ユーザー インターフェイスのプロンプトに従います。

**Confirm Upgrade**

Upgrade Guest Introspection service

Datastore \* ds-site-a-nfs01

Network \* vds-site-a\_Management...

IP assignment \* GI Pool

**Specify schedule:**

☒ Upgrade now

☐ Schedule the upgrade  6:29 PM

OK Cancel

ゲスト イントロスペクションをアップグレードすると、インストールの状態は **成功しました** になり、サービスのステータスは **接続中** になります。ゲスト イントロスペクション サービスの仮想マシンは、vCenter Server インベントリに表示されます。

## 次のステップ

特定のクラスタのゲスト イントロスペクションをアップグレードした後、パートナー ソリューションをアップグレードできます。パートナー ソリューションが有効な場合、パートナーが提供するアップグレードのドキュメントを参照してください。パートナー ソリューションをアップグレードしない場合でも、保護が維持されます。

パートナー ソリューションを NSX で認定されているバージョンにアップグレードする場合は、Service Composer を使用して、パートナー ソリューション ベースのポリシーを作成し、保護を維持する必要があります。『NSX 管理ガイド』の「Service Composer の使用」を参照してください。

## 直接アップグレードをサポートしない NSX サービス

VMware Partner Security Virtual Appliances などのいくつかの NSX サービスは、直接アップグレードをサポートしません。この場合、サービスをアンインストールしてから、再度インストールを行う必要があります。

### VMware Partner Security Virtual Appliances

VMware パートナーのセキュリティ仮想アプライアンスがアップグレード可能かどうかは、パートナーが提供するドキュメントでご確認してください。

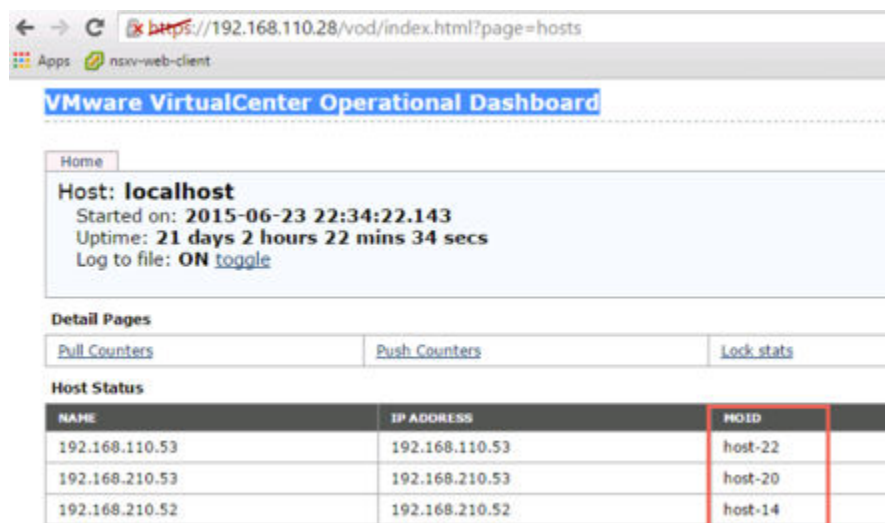
### NSX Data Security

NSX Data Security をアンインストールした後に NSX をアップグレードし、NSX のアップグレードが完了してから NSX Data Security を再インストールすることをお勧めします。NSX Data Security をアンインストールせずに NSX をアップグレードした場合は、REST API 呼び出しを使用して Data Security をアンインストールする必要があります。

次の API 呼び出しを実行します。

**DELETE** `https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds`

host-id は、ESXi ホストの MOID です。MOID を取得するには、VMware VirtualCenter Operational Dashboard (`https://<vcenter-ip>/vod/index.html?page=hosts`) を開きます。



vCenter Server 192.168.110.28 上にある、MOID が "host-22" の ESXi ホストの場合、API 呼び出しは次のような形式になります。

**DELETE** `https://192.168.110.28/api/1.0/vshield/host-22/vsds`

すべての ESXi ホストで API 呼び出しを実行するようにします。

Data Security のアンインストール後に、新しいバージョンをインストールできます。[「NSX Data Security のインストール」](#) を参照してください。

## NSX SSL VPN

NSX 6.2 以降、SSL VPN ゲートウェイで許容されるのは、TLS プロトコルのみにになります。しかし、NSX 6.2 以降へのアップグレード後、ユーザーが新規で作成するクライアントでは、接続を確立する間、自動的に TLS プロトコルが使用されます。また、NSX 6.2.3 以降では、TLS 1.0 は廃止されています。

プロトコルが変更されると、NSX 6.0.x クライアントが NSX 6.2 以降のゲートウェイへ接続する際、SSL ハンドシェイクの段階で接続の確立に失敗します。

NSX 6.0.x からのアップグレード後は、古い SSL VPN クライアントをアンインストールし、NSX 6.2.x バージョンの SSL VPN クライアントをインストールしてください。『NSX 管理ガイド』の「リモート サイトへの SSL クライアントのインストール」を参照してください。

## NSX L2 VPN

バージョン 5.5.x または 6.0.x の NSX Edge に L2 VPN がインストールされている場合、NSX Edge はアップグレードできません。NSX Edge をアップグレードする前に、すべての L2 VPN の設定を削除する必要があります。

## NSX Data Security のインストール

---

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


---

### 前提条件

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

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

### 手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 [新しいサービスの展開 (New Service Deployment)] (  ) アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログボックスで、[Data Security] を選択し、[次へ (Next)] をクリックします。
- 4 [スケジュールを指定する (Specify schedule)] (ダイアログ ボックス下部) で、[今すぐデプロイする (Deploy now)] を選択して Data Security がインストールされたらすぐにデプロイするか、またはデプロイの日付と時間を選択します。
- 5 [次へ (Next)] をクリックします。
- 6 Data Security をインストールするデータセンターおよびクラスタを選択し、[次へ (Next)] をクリックします。



- 7 [ストレージおよび管理ネットワークの選択] ページで、サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み (Specified on host)] を選択します。

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

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

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

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

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

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

- 9 [IP 割り当て] で、次のいずれかを選択します。

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

固定 IP アドレスはサポートされていないことに注意してください。

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

## アップグレード後のチェックリスト

アップグレードが完了したら、次の手順を実行します。

### 手順

- 1 アップグレード後に NSX Manager の現在のバックアップを作成します。

- 2 VIB がホストにインストールされていることを確認します。

NSX によって、これらの VIB がインストールされます。

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

ゲスト イントロスペクションがインストールされている場合、この VIB がホストに存在していることも確認します。

```
esxcli software vib get --vibname epsec-mux
```

- 3 ホストのメッセージバスを再同期します。VMware は、アップグレード後に再同期することをすべてのカスタマにお勧めしています。

次の API コールを使用して、各ホストで再同期を実行します。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
```

Headers:

```
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

## vCloud Director 環境での vCloud Networking and Security 5.5.x から NSX へのアップグレード

vCloud Director のバージョンによって、アップグレード後の NSX のバージョンが決まります。環境内の他のソリューションやツールと互換性があり、サポートされている最新のバージョンに、NSX をアップグレードすることをお勧めします。

[https://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php) に掲載されている『VMware 製品の相互運用性マトリックス』を参照してください。

NSX にアップグレードするには、本書に記載された順序で vCloud Networking and Security の各コンポーネントをアップグレードする必要があります。

vCloud Networking and Security コンポーネントは次の順序でアップグレードする必要があります。

- 1 vShield Manager から NSX Manager へのアップグレード
- 2 NSX Controller クラスターの展開（オプション）。分散論理ルーターと、制御プレーンのモードをハイブリッドまたはユニキャストに変更するために必要
- 3 ホスト クラスターの更新

- 4 トランSPORT ゾーン の更新 (オプション)。NSX Controller クラスタを展開している場合、ハイブリッドまたはユニキャストに変更可能
- 5 NSX Edge : vCloud Director 8.10 以降を使用している場合のみ NSX Edge にアップグレードしてください。

**重要:** 環境内で仮想ワイヤーがある場合は、NSX Manager へのアップグレード後にホスト クラスタを更新する必要があります。

次に示すオプションの vCloud Networking and Security コンポーネントは、vCloud Director と連携しません。

- 1 vShield App : 「[vShield App から Distributed Firewall へのアップグレード](#)」を参照してください。
- 2 vShield Endpoint : 「[vShield Endpoint から NSX ゲスト イントロスペクションへのアップグレード](#)」を参照してください。
- 3 vShield Data Security : アップグレードに対応していません。アンインストールの手順は、「[直接アップグレードをサポートしない NSX サービス](#)」を参照してください。インストールの手順は、「[NSX Data Security のインストール](#)」を参照してください。

## vCloud Director 環境での vShield Manager から NSX Manager へのアップグレード

NSX インフラストラクチャのアップグレード プロセスでは、最初に NSX Manager アプライアンスのアップグレードを行います。



**警告:** vShield Manager アプライアンスのデプロイ済みインスタンスはアンインストールしないでください。

### 前提条件

- システム要件の確認とバックアップの作成も含めて、[NSX にアップグレードするための vCloud Networking and Security の準備](#)に記載されているアップグレード準備タスクがすべて完了していることを確認します。
- NSX Manager へのアップグレードに必要なディスク容量が vShield Manager にあることを確認します。[NSX のシステム要件](#)を参照してください。
- NSX 6.2.x にアップグレードする前に、vShield Manager 仮想アプライアンスの予約済みメモリを 16 GB 以上に増加し、仮想 CPU を 4 個割り当てます。  
[NSX のシステム要件](#)を参照してください。
- vShield Edge 5.5 より前のバージョンのインスタンスの場合は、すべて Shield バージョン 5.5 にアップグレードしてください。

vShield Manager を NSX Manager にアップグレードした後は、vShield Edge 5.5 より前のバージョンのインスタンスを管理または削除できません。

### 手順

- 1 vShield Manager から参照できる場所に NSX のアップグレード バンドルをダウンロードします。アップグレード バンドル ファイルは、`VMware-vShield-Manager-upgrade-bundle-to-NSX-<release>-<buildNumber>.tar.gz` のような名前になっています。

- 2 vShield Manager 5.5 インベントリ パネルから [設定とレポート] をクリックします。
- 3 [アップデート] タブ、[アップグレード バンドルのアップロード] の順にクリックします。
- 4 [ファイルを選択] を選択し、**VMware-vShield-Manager-upgrade-bundle-to-NSX-<release>-<buildNumber>.tar.gz** ファイルを選択して、[開く] をクリックします。
- 5 [ファイルのアップロード] をクリックします。  
ファイルのアップロードには数分かかります。
- 6 [インストール] をクリックして、アップグレード プロセスを開始します。
- 7 [インストールの確認] をクリックします。アップグレード プロセスによって vShield Manager が再起動されるため、vShield Manager ユーザー インターフェイスへの接続が失われる可能性があります。その他の vShield コンポーネントは再起動されません。
- 8 再起動後、Web ブラウザ ウィンドウを開き、https://10.10.10.10 のように IP アドレスを入力して、NSX Manager 仮想マシンにログインします。アップグレードされた NSX Manager の IP アドレスは、vShield Manager と同じです。  
[サマリ] タブにインストールした NSX Manager のバージョンが表示されます。
- 9 [ホーム] - [vCenter Server 登録の管理] の順に移動し、vCenter Server のステータスが **接続中** であることを確認します。
- 10 vSphere Web Client にアクセスしている既存のブラウザ セッションを閉じます。数分待ち、ブラウザ キャッシュをクリアしてから vSphere Web Client に再ログインします。
- 11 vShield Manager で SSH が有効になっていた場合は、アップグレード後に NSX Manager で有効にする必要があります。NSX Manager 仮想アプライアンスにログインし、[サマリの表示] をクリックします。[システム レベルのコンポーネント] で、SSH サービスの [開始] をクリックします。

---

**重要:** vCloud Networking and Security 5.x を NSX 6.x にアップグレードした後は、CLI 管理者のログイン認証情報を使用して、NSX Manager にログインする必要があります。これまで、vCloud Networking and Security では、CLI とユーザー インターフェイスにそれぞれ 1 つ、合わせて 2 つのパスワードが必要でした。NSX 6.x からは、1 つのパスワードのみが必要になります。次はその例です。

vCloud Networking and Security のパスワード

- CLI のパスワード mypassword#123
- ユーザー インターフェイスのパスワード mypassword#456

NSX にアップグレードした後のパスワード

- CLI のパスワード mypassword#123
- ユーザー インターフェイスのパスワード mypassword#123

---

NSX Manager のアップグレード後に、vSphere Web Client からログアウトし、再度ログインする必要があります。

NSX プラグインが vSphere Web Client に正しく表示されない場合、ブラウザのキャッシュと履歴をクリアしてください。この手順を行わないと、vSphere Web Client で NSX の設定を変更したときに「内部エラーが発生しました - エラー #1009」のようなエラーが表示される場合があります。

vSphere Web Client で [Networking and Security] タブが表示されない場合には、vSphere Web Client サーバをリセットします。

- vCenter Server 5.5 で `https://<vcenter-ip>:5480` を開き、Web Client サーバを再起動します。
- vCenter Server Appliance 6.0 で、vCenter Server シェルに root ユーザーとしてログインし、次のコマンドを実行します。

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Windows の vCenter Server 6.0 では、次のコマンドを実行するとアップグレードできます。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

異なるバージョンの NSX プラグインが実行中の場合は、予期しないエラーを回避するため、異なるバージョンの NSX Manager を実行している vCenter Server の管理に別々の Web Client を使用することをお勧めします。

NSX Manager がアップグレードされたら、新しい NSX Manager バックアップ ファイルを作成します。[\[NSX のバックアップとリストア\]](#) を参照してください。以前の NSX Manager バックアップは、以前のリリースに対してのみ有効です。

#### 次のステップ

[\[vCloud Director 環境での NSX ライセンスのインストールと割り当て\]](#)

## vCloud Director 環境での NSX ライセンスのインストールと割り当て

NSX Manager のアップグレードが完了した後に、vSphere Web Client を使用して、NSX for vSphere のライセンスのインストールと割り当てを実行できます。

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

NSX と vCloud Director を併用するには、NSX Edge など、必要な追加の NSX 機能に対応する NSX ライセンスを購入する必要があります。

NSX ライセンスに関する FAQ (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>) を参照してください。

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

## 手順

- vSphere 5.5 で、次の手順を実行して NSX のライセンスを追加します。
  - a vSphere Web Client にログインします。
  - b [管理 (Administration)] をクリックして、[ライセンス (Licenses)] をクリックします。
  - c [ソリューション (Solutions)] タブをクリックします。
  - d [ソリューション] リストで NSX for vSphere を選択します。[ライセンス キーの割り当て (Assign a license key)] をクリックします。
  - e ドロップダウン メニューから [新しいライセンス キーの割り当て (Assign a new license key)] を選択します。
  - f ライセンス キーを入力し、この新しいキーのラベル (オプション) を入力します。
  - g [デコード (Decode)] をクリックします。  
ライセンス キーをデコードして、そのキーが正しい形式であるか、および資産のライセンス供与に対して十分なキャパシティがあるかを確認します。
  - h [OK] をクリックします。
- vSphere 6.0 で、次の手順を実行して NSX のライセンスを追加します。
  - a vSphere Web Client にログインします。
  - b [管理 (Administration)] をクリックして、[ライセンス (Licenses)] をクリックします。
  - c [資産 (Assets)] タブをクリックして、[ソリューション (Solutions)] タブをクリックします。
  - d [ソリューション] リストで NSX for vSphere を選択します。[すべてのアクション (All Actions)] ドロップダウン メニューから、[ライセンスの割り当て... (Assign license...)] を選択します。
  - e [追加 (+) (Add)] アイコンをクリックします。ライセンス キーを入力して、[次へ (Next)] をクリックします。ライセンスの名前を追加して、[次へ (Next)] をクリックします。[終了 (Finish)] をクリックして、ライセンスを追加します。
  - f 新しいライセンスを選択します。
  - g (オプション) [機能の表示 (View Features)] アイコンをクリックして、このライセンスで有効になっている機能を表示します。[キャパシティ (Capacity)] 列で、ライセンスのキャパシティを確認します。
  - h [OK] をクリックして、新しいライセンスを NSX に割り当てます。

## 次のステップ

[\[vCloud Director 環境の NSX 向け NSX コントローラ クラスターの展開\]](#) (オプション。制御プレーン モードで、マルチキャスト以外を選択できるようになります)

コントローラを展開しない場合、[\[vCloud Director 環境でホスト クラスタを vCNS から NSX へ更新\]](#)。

## vCloud Director 環境の NSX 向け NSX コントローラ クラスタの展開

NSX コントローラは、NSX の論理スイッチングおよびルーティング機能の制御プレーンとして機能する高度な分散状態管理システムです。これは、ネットワーク内のすべての論理スイッチの集中管理ポイントとして機能するもので、すべてのホスト、論理スイッチ (VXLAN)、および分散論理ルーターの情報を管理します。1) 分散論理ルーター、あるいは 2) ユニキャストまたはハイブリッド モードの VXLAN のデプロイを計画する場合、コントローラが必要になります。

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

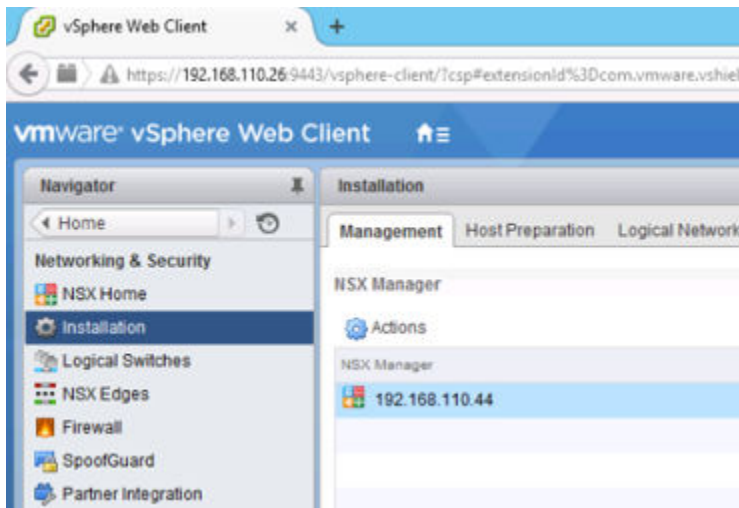
### 前提条件

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

### 手順

- 1 vSphere Web Client で [ホーム] > [Networking and Security] > [インストール] の順に移動し、[管理] タブを選択します。

次はその例です。



- 2 [NSX コントローラ ノード] セクションで、[ノードの追加] (+) アイコンをクリックします。

### 3 環境に適した NSX コントローラ設定を入力します。

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

次はその例です。

### 4 コントローラ クラスタの IP アドレス ルールをまだ設定していない場合は、ここで [新規 IP プール] をクリックして設定します。

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

次はその例です。



## 5 コントローラのパスワードを入力し、再入力します。

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

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

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

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

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

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

各コントローラに SSH で接続し、ホスト管理インターフェイスの IP アドレスに ping できることを確認します。ping が失敗する場合、すべてのコントローラに適切なデフォルト ゲートウェイがあることを確認します。コントローラのルーティング テーブルを表示するには、[show network routes] コマンドを実行します。コントローラのデフォルト ゲートウェイを変更するには、[clear network routes] コマンドを実行した後、[add network default-route <IP アドレス>] コマンドを実行します。

以下のコマンドを実行し、コントロール クラスタが想定どおりに動作することを確認します。

### ■ show control-cluster status

Type	Status	Since
Join status:	Join complete	05/04 02:36:03
Majority status:	Connected to cluster majority	05/19 23:57:23
Restart status:	This controller can be safely restarted	05/19 23:57:12
Cluster ID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Node UUID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

Join status で、コントローラ ノードが参加完了 (Join Complete) であることを確認します。

Majority status で、コントローラがクラスタ マジョリティ (cluster majority) に接続していることを確認します。

Cluster ID で、クラスタ内のすべてのコントローラ ノードのクラスタ ID が同じであることを確認します。

Configured status および Active status で、すべてのコントローラ ロールが有効 (enabled) であり、アクティベーション済み (activated) であることを確認します。

#### ■ show control-cluster roles

	Listen-IP	Master?	Last-Changed	Count
api_provider	Not configured	Yes	06/02 08:49:31	4
persistence_server	N/A	Yes	06/02 08:49:31	4
switch_manager	127.0.0.1	Yes	06/02 08:49:31	4
logical_manager	N/A	Yes	06/02 08:49:31	4
directory_server	N/A	Yes	06/02 08:49:31	4

1 台のコントローラ ノードが各ロールのマスターになります。この例では、1 台のノードがすべてのロールのマスターになっています。

あるロールのマスター NSX コントローラ インスタンスが失敗した場合、クラスタはそのロールの新しいマスターを、利用可能な NSX コントローラ インスタンスから選択します。

NSX コントローラ インスタンスは制御プレーン上にあるため、NSX コントローラ に障害が発生してもデータ プレーントラフィックに影響はありません。

#### ■ show control-cluster connections

role	port	listening	open conns
api_provider	api/443	Y	2
persistence_server	server/2878	Y	2
	client/2888	Y	1
	election/3888	Y	0
switch_manager	ovsmgmt/6632	Y	0
	openflow/6633	Y	0
system	cluster/7777	Y	0

このコマンドはクラスタ内の通信ステータスを表示します。

コントローラ クラスタのマジョリティ リーダーはポート 2878 を listen しています ([listening] 列に [Y] が示されています)。他のコントローラ ノードのポート 2878 の [listening] 列にはダッシュ (-) が表示されます。

他のすべてのポートは 3 台すべてのコントローラ ノードを listen する必要があります。

[open conns] 列には、コントローラ ノードに含まれる、他のコントローラ ノードに対して確立された接続数が示されます。3 ノードのコントローラ クラスタでは、2 つ以下の接続を確立することはできません。

## 次のステップ



**警告:** コントローラのステータスが [デプロイ中です] の間は、環境に論理スイッチまたは分散ルーティングの追加や変更をしないでください。また、ホストの準備手順を続行しないでください。コントローラ クラスタに新しいコントローラが追加されると、すべてのコントローラが少しの間 (5 分以内) 非アクティブになります。このダウンタイム中にコントローラに関連する操作 (ホストの準備など) を行うと、予期しない結果になる可能性があります。ホストの準備が正常に完了したように思われても、SSL 証明書が正しく確立されていないことがあります。このため、VXLAN ネットワークに問題が生じます。

展開したコントローラを削除する必要がある場合は、『NSX 管理ガイド』の「NSX コントローラの障害からのリカバリ」を参照してください。

NSX コントローラ ノードを最初に展開したホストでは、NSX によって、仮想マシンの自動起動/シャットダウンが有効になります。その後、コントローラ ノードの仮想マシンを別のホストに移行した場合、新しいホストで仮想マシンの自動起動/シャットダウンが有効にならない場合があります。そのため、クラスタ内のすべてのホストをチェックし、仮想マシンの自動起動/シャットダウンが有効になっていることを確認することをお勧めします。

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

## vCloud Director 環境でホスト クラスタを vCNS から NSX へ更新

vCenter Server の各クラスタ レベルにネットワーク インフラストラクチャ コンポーネントをインストールし、ネットワーク仮想化環境の準備を行う必要があります。これにより、必要なソフトウェアがクラスタ内のすべてのホストにインストールされ、仮想ワイヤーから NSX 論理スイッチに変更されます。このプロセスでは、クラスタ内の各ホストがソフトウェア アップデートを受け取り、再起動されます。

環境内で仮想ワイヤーがある場合は、NSX Manager へのアップグレード後にホスト クラスタを更新する必要があります。

データ センターのメンテナンス期間中にホスト クラスタを更新することをお勧めします。

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

NSX をインストールまたはアップグレードすると、各ホストを自動的にメンテナンス モードに移行し再起動するように試行されます。これは、vCloud Director 環境では推奨されません。

代わりに、各クラスタで VIB をアップグレードし、[解決 (Resolve)] はクリックしないでください。メンテナンス モードに入り、再起動する前に、vCloud Director でホストを無効にする必要があります。

**注:** vCloud Networking and Security で作成された VTEP は、DHCP または手動で割り当てられた IP アドレスを使用します。IP アドレス プールは使用しません。

### 手順

#### 1 vCloud Director 環境内のホスト上の VIB のアップグレード

vCloud Director 環境では、クラスタで VIB をアップグレードする前に DRS を手動に設定する必要があります。これを行わないと、NSX がホストをメンテナンス モードに切り替えようとします。

## 2 vCloud Director 環境で VIB をインストールした後の手動によるホストの再起動

インストールされた NSX VIB を有効にするには、ホストを再起動する必要があります。再起動する前に vCloud Director にあるホストを無効にする必要があります。これにより、再起動中に vCloud Director によってこれらのホストが使用されなくなります。

### vCloud Director 環境内のホスト上の VIB のアップグレード

vCloud Director 環境では、クラスタで VIB をアップグレードする前に DRS を手動に設定する必要があります。これを行わないと、NSX がホストをメンテナンス モードに切り替えようとします。

#### 前提条件

- vShield Manager が NSX Manager にアップグレードされていることを確認します。
- [ホストの準備] タブの [VXLAN] 列で、[有効 (Enabled)] と表示されていることを確認します。
- すべてのホストの完全修飾ドメイン名 (FQDN) を解決できることを確認します。
- アップグレードを開始する前に、環境内で DRS が機能できることを確認します。
  - ホスト クラスタで DRS が有効になっていることを確認します。
  - vMotion が正しく機能していることを確認します。
  - ホストと vCenter Server の接続状態を確認します。
  - 各ホスト クラスタに、少なくとも 3 台の ESXi ホストがあることを確認します。1 台または 2 台のホストを持つホスト クラスタでは、NSX のアップグレード中に、DRS のアドミSSION コントロールの問題が発生することがあります。NSX を正しくアップグレードするため、各ホスト クラスタに少なくとも 3 台のホストを含めることをお勧めします。クラスタに含まれるホストが 3 台より少ない場合は、ホストを手動で退避させることが推奨されます。
- DRS が有効な場合は、実行中の仮想マシンは、ホスト クラスタのアップグレード中に自動的に移動されます。アップグレードを開始する前に、環境内で DRS が機能できることを確認します。
  - ホスト クラスタで DRS が有効になっていることを確認します。
  - vMotion が正しく機能していることを確認します。
  - ホストと vCenter Server の接続状態を確認します。
  - 各ホスト クラスタに、少なくとも 3 台の ESXi ホストがあることを確認します。1 台または 2 台のホストを持つホスト クラスタでは、NSX のアップグレード中に、DRS のアドミSSION コントロールの問題が発生することがあります。NSX を正しくアップグレードするため、各ホスト クラスタに少なくとも 3 台のホストを含めることをお勧めします。クラスタに含まれるホストが 3 台より少ない場合は、ホストを手動で退避させることが推奨されます。

#### 手順

- 1 vSphere Web Client で、[ホーム (Home)] - [ホストおよびクラスタ (Hosts and Clusters)] の順に移動します。

- 2 ホスト クラスタで DRS を手動に設定します。vCloud Networking and Security がインストールされているすべてのクラスタでこれらの手順を繰り返します。



**警告:** DRS は無効にしないでください。DRS を無効にすると、リソース プールが削除され、vCloud Director インストール環境で不具合が発生します。

- a クラスタを選択し、次に、[管理 (Manage)] - [設定 (Settings)] - [vSphere DRS] の順に移動します。
  - b この変更は後で戻しますので、現在の [DRS 自動化 (DRS Automation)] の設定をメモしておきます。
  - c [編集 (Edit)] をクリックします。[DRS 自動化 (DRS Automation)] セクションで、[手動 (Manual)] を選択して、[OK] をクリックします。
- 3 [ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] の順に移動します。
  - 4 [ホストの準備 (Host Preparation)] タブをクリックします。

インフラストラクチャ内のすべてのクラスタが表示されます。

バージョン 5.5 の環境内で仮想ワイヤーを使用していた場合、[インストールの状態 (Installation Status)] 列に [レガシー (legacy)]、[更新 (Update)] および [アンインストール (Uninstall)] と表示されます。

図 1-3. バージョン 5.5 の環境内で仮想ワイヤーを使用している場合、[インストールの状態] が [更新] と表示される

Clusters & Hosts	Installation Status	Firewall	VLAN
CL-5.5	legacy Update Uninstall	Not Enabled	Enabled
CL-5.1	legacy Update Uninstall	Not Enabled	Enabled

バージョン 5.5 の環境内で仮想ワイヤーを使用していなかった場合、[インストールの状態 (Installation Status)] 列に [インストール (Install)] と表示されます。

図 1-4. バージョン 5.5 の環境内で仮想ワイヤーを使用している場合、[インストールの状態] に [インストール] と表示される

Clusters & Hosts	Installation Status	Firewall	VLAN
CL-5.5	Install	Not Enabled	Enabled
CL-5.1	Install	Not Enabled	Enabled

- 5 個々のクラスタで、[インストールの状態] 列の [更新 (Update)] または [インストール (Install)] をクリックします。  
クラスタ内の各ホストが新しい論理スイッチ ソフトウェアを受け取ります。  
ホストのアップグレードによりホストのスキャンが開始されます。以前の VIB は削除されます（再起動までは完全には削除されません）。新しい VIB が altboot パーティションにインストールされます。まだ再起動されていないホスト上の新しい VIB を表示するには、**esxcli software vib list --rebooting-image | grep esx** コマンドを実行します。
- 6 [インストールの状態 (Installation Status)] 列に [準備ができていません (Not Ready)] と表示されるまで、インストールの進捗を監視します。  
[解決 (Resolve)] をクリックしないでください。
- 7 [ホーム (Home)] - [ホストおよびクラスタ (Hosts and Clusters)] の順に移動します。
- 8 ホスト クラスタで DRS の変更を戻します。NSX がインストールされているすべてのクラスタでこれらの手順を繰り返します。
  - a クラスタを選択し、次に、[管理 (Manage)] - [設定 (Settings)] の順に移動します。
  - b [vSphere DRS] を選択し、[編集 (Edit)] をクリックします。[DRS 自動化 (DRS Automation)] セクションで、元の DRS 設定を選択して、[OK] をクリックします。

#### 次のステップ

[\[vCloud Director 環境で VIB をインストールした後の手動によるホストの再起動\]](#)。

### vCloud Director 環境で VIB をインストールした後の手動によるホストの再起動

インストールされた NSX VIB を有効にするには、ホストを再起動する必要があります。再起動する前に vCloud Director にあるホストを無効にする必要があります。これにより、再起動中に vCloud Director によってこれらのホストが使用されなくなります。

#### 前提条件

- すべてのホストのステータスが [準備ができていません (Not Ready)] になっていることを確認します。
- 1 台のホストが稼動しなくても、一時的に実行できるだけの十分なキャパシティが各 vSphere クラスタにあることを確認します。
- DRS が有効であり、[手動] に設定されていないことを確認します。

#### 手順

- 1 vCloud Director で、ホストを無効にします。
  - a [管理および監視 (Manage & Monitor)] - [ホスト (Hosts.)] の順に移動します。
  - b ホストを右クリックして、[ホストを無効にする (Disable Host)] を選択します。
- 2 vSphere Web Client で、[ホーム (Home)] - [ホストおよびクラスタ (Hosts and Clusters)] の順に移動します。

- 3 vCloud Director で無効にしたホストを右クリックして、[メンテナンス モードに切り替え (Enter Maintenance Mode)] を選択します。[メンテナンス モードの確認] ダイアログ ボックスで、[クラスタにある他のホストにパワーオフおよび中断された仮想マシンを移動する (Move powered-off and suspended virtual machines to other hosts in the cluster)] を選択して、[OK] をクリックします。
- 4 他のホストにすべての仮想マシンが移行しない場合、手動で移動します。
- 5 ホストがメンテナンス モードに切り替わったら、ホストを右クリックして、[再起動 (Reboot)] を選択します。再起動の理由を入力し、[OK] をクリックします。
- 6 ホストがバックアップされたら、[メンテナンス モードを終了 (Exit Maintenance Mode)] を選択します。
- 7 vCloud Director で、ホストを有効にします。
  - a [管理および監視 (Manage & Monitor)] - [ホスト (Hosts.)] の順に移動します。
  - b ホストを右クリックして、[ホストを有効にする (Enable Host)] を選択します。
- 8 vCloud Director でホストが有効になったら、次のホストでこれらの手順を繰り返します。

5.5 インフラストラクチャ内のすべての仮想ワイヤーの名前が NSX 論理スイッチに変更され、クラスタの [VXLAN] 列に [有効 (Enabled)] と表示されます。

[有効 (Enabled)]

クラスタが更新されると、[インストールの状態 (Installation Status)] 列に更新が完了したソフトウェア バージョンが表示されます。

ホストの更新を確認するには、クラスタ内のホストのいずれかにログインして **esxcli software vib list | grep esx** コマンドを実行します。次の VIB が正しいバージョンに更新されたことを確認します。

- esx-vsip
- esx-vxlan

---

**注:** NSX 6.2 では、esx-dvfilter-switch-security VIB は、esx-vxlan VIB の中に組み込まれています。

---

ホストのアップグレードに失敗した場合は、次のトラブルシューティング手順を実行します。

- vCenter Server の ESX Agent Manager で、アラートおよびエラーを確認します。
- ホストにログインし、**/var/log/esxupdate.log** ログ ファイルで最近のアラートとエラーを確認します。
- DNS と NTP がホストに設定されていることを確認します。

#### 次のステップ

NSX コントローラ クラスタを展開済みの場合、オプションで制御プレーンのモードを変更することができます。[「vCloud Director 環境でのトランスポート ゾーンと論理スイッチの更新」](#)を参照してください。

NSX コントローラ クラスタを展開していない場合は、[「vCloud Director 環境での vShield Edge アップグレードの決定」](#)を参照してください。

## vCloud Director 環境でのトランスポート ゾーンと論理スイッチの更新

NSX Controller クラスタを展開すると、論理ネットワークでマルチキャストに依存する必要がなくなります。トランスポート ゾーンと論理スイッチの制御プレーン モードをユニキャストまたはハイブリッドに更新できます。

制御プレーン モードの変更や既存の論理スイッチの移行を行っても、ネットワーク データ プレーンのトラフィックに影響しません。

### 手順

- 1 vSphere Web Client で、[ホーム (Home)] - [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [論理ネットワークの準備 (Logical Network Preparation)] - [トランスポート ゾーン (Transport Zones)] の順に移動します。
- 2 トランスポート ゾーンを選択して、[アクション (Actions)] - [設定の編集 (Edit Settings)] の順にクリックします。次のように、必要なレプリケーション モードを選択します。
  - [マルチキャスト (Multicast)] : 物理ネットワーク上のマルチキャスト IP アドレスを制御プレーンに使用します。このモードは、古い VXLAN デプロイからアップグレードする場合にのみ推奨されます。物理ネットワークに PIM/IGMP が必要です。
  - [ユニキャスト (Unicast)] : 制御プレーンは、NSX コントローラによって処理されます。すべてのユニキャストトラフィックで、最適化されたヘッドエンド レプリケーションを利用します。マルチキャスト IP アドレスや特別なネットワーク設定は必要ありません。
  - [ハイブリッド (Hybrid)] : ローカルトラフィック レプリケーションを物理ネットワーク (L2 マルチキャスト) にオフロードします。最初のホップのスイッチで IGMP スヌーピング、各 VTEP サブネットの IGMP クエリアへのアクセスが必要ですが、PIM は不要です。最初のホップスイッチは、サブネットのトラフィックレプリケーションを処理します。
- 3 [既存の論理スイッチを新しい制御プレーン モードに移行します。 (Migrate existing Logical Switches to the new control plane mode)] のチェック ボックスを選択して [OK] をクリックします。

### 次のステップ

[\[vCloud Director 環境での vShield Edge アップグレードの決定\]](#)

## vCloud Director 環境での vShield Edge アップグレードの決定

vShield Edge をアップグレードする必要があるかどうかは、vCloud Director のバージョンによって決まります。

vCloud Director の 8.10 より前のバージョンを使用している場合は、vShield Edge をアップグレードすることはできません。

また、vCloud Director 5.x を使用している場合、vCloud Director データベースで設定を変更して、vCloud Director によって再展開時に Edge がアップグレードされないようにする必要があります。[\[vCloud Director 環境におけるレガシー vShield Edge の再デプロイの防止\]](#) を参照してください。

vCloud Director 8.10 以降では、NSX Edge 6.x がサポートされているため、vShield Edge を NSX Edge 6.x にアップグレードできます。詳細については、[\[vCloud Director 環境での vShield Edge から NSX Edge へのアップグレード\]](#) を参照してください。



## vCloud Director 環境におけるレガシー vShield Edge の再デプロイの防止

vCloud Director 5.x を使用している場合、NSX にアップグレードした後に、レガシーの vShield Edge アプライアンスが NSX Edge として展開されないようにデータベースを変更する必要があります。

レガシーの Edge Services Gateway を VMware NSX 6.x にアップグレードしないように注意してください。アップグレード、vCloud Director との互換性がなくなります。vCloud Director 5.x は、Edge が再展開されるときに vCloud Director 上の Edge をアップグレードします。この動作を防ぐには、vCloud Network and Security を移行する前に、次に示すデータベースの変更を vCloud Director で行う必要があります。

詳細については、ナレッジベースの記事 <http://kb.vmware.com/kb/2096351> および <http://kb.vmware.com/kb/2108913> を参照してください。

### 手順

- 1 vCloud Director SQL Server データベースにログインします。
- 2 この行を構成テーブルに追加します。

```
INSERT INTO config (cat, name, value, sortorder) VALUES
('vcloud','networking.edge_version_for_vsm6.2', '5.5', 0);
```

**注:** NSX 6.1 が使用されている場合、**networking.edge\_version\_for\_vsm6.1** を使用し、NSX 6.0 が使用されている場合、**networking.edge\_version\_for\_vsm6.0** を使用します。

## vCloud Director 環境での vShield Edge から NSX Edge へのアップグレード

vCloud Director 8.10 は NSX Edge 6.x をサポートしているため、vShield Edge を NSX Edge にアップグレードできます。vCloud Director の以前のバージョンを使用している場合、NSX Edge 6.x はサポートされていないため、NSX Edge にアップグレードすることはできません。

vShield Edge から NSX Edge へのアップグレードには、NSX を使用方法と、vCloud Director を使用方法の 2 種類があります。

vCloud Director を使用して Edge をアップグレードするには、『vCloud Director インストールおよびアップグレードガイド』の「vCenter Server システム、ホスト、および NSX Edge のアップグレード」セクションを参照してください。



**注目:** vCloud Director 8.10 より前のバージョンを使用している場合は、NSX Edge をアップグレードしないでください。

### 前提条件

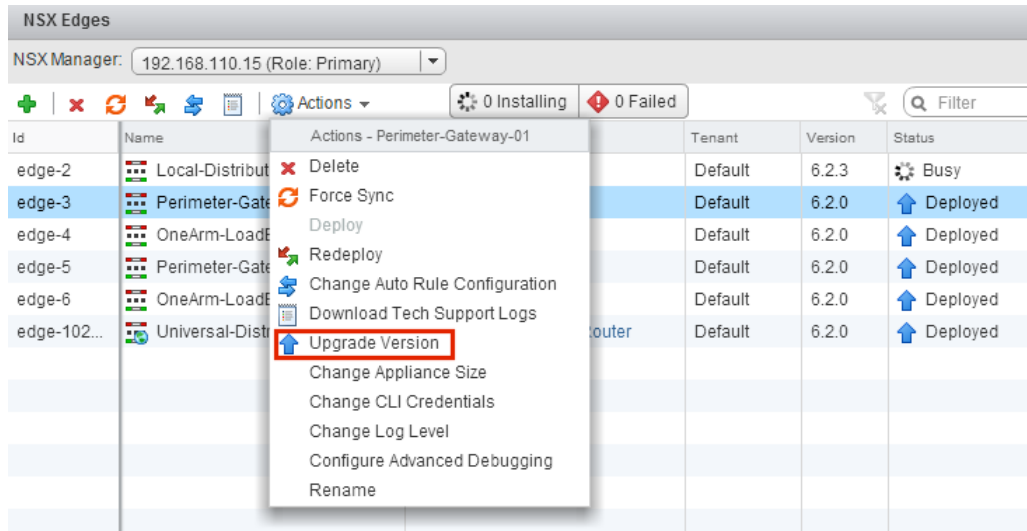
- vShield Manager が NSX Manager にアップグレードされていることを確認します。
- NSX Edge のアップグレード進行中に発生する運用上の影響について理解しておく必要があります。[\[vCloud Networking and Security のアップグレードによる動作上の影響\]](#) を参照してください。
- NSX 論理スイッチを作成する計画がない場合でも、ローカル セグメント ID プールがあることを確認します。

- アップグレード中に追加の NSX Edge Services Gateway アプライアンスを展開するための十分なリソースがホストにあることを確認します。これは特に複数の NSX Edge アプライアンスを並行してアップグレードする場合に重要です。各サイズの NSX Edge で必要とされるリソースについては、[「NSX のシステム要件」](#) を参照してください。
- アップグレード時は、1 台の NSX Edge インスタンスにつき、フルサイズの新しい NSX Edge アプライアンスがもう 1 台ホスト上に存在し、2 台ともパワーオン状態となります。
- NSX 6.2.3 以降は、高可用性 (HA) 構成の 2 台の NSX Edge インスタンスを再デプロイする場合、2 台の新しいアプライアンスをデプロイしてから、2 台の古い アプライアンスと置き換えます。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 4 台存在することになります。NSX Edge インスタンスがアップグレードされると、高可用性アプライアンスのいずれかがアクティブになります。
- NSX 6.2.3 より前は、HA 構成の NSX Edge インスタンスのアップグレードで古いアプライアンスを置き換える場合、一度につき新しいアプライアンスを 1 台展開していました。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 3 台存在することになります。NSX Edge インスタンスがアップグレードされると、通常は HA インデックスが 0 の NSX Edge アプライアンスがアクティブになります。
- L2 VPN が有効になっている場合、バージョン 5.5 または 6.0 の NSX Edge はアップグレードできません。アップグレードの前に、L2 VPN 設定を削除する必要があります。L2 VPN は、アップグレード後に再設定できます。詳細については、『NSX インストール ガイド』の「L2 VPN の概要」を参照してください。

#### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。

- 3 各 NSX Edge インスタンスで、[操作 (Actions)] メニューから [アップグレード バージョン (Upgrade Version)] を選択します。



「Edge アプライアンスをデプロイできませんでした。」というエラー メッセージが出てアップグレードが失敗した場合は、NSX Edge アプライアンスがデプロイされているホストが接続されており、メンテナンス モードになっていないことを確認します。

NSX Edge が正常にアップグレードされると、[ステータス (Status)] は [デプロイ済み] になり、[バージョン (Version)] 列に NSX のバージョンが表示されます。

Edge のアップグレードが失敗し、以前のバージョンにロールバックしない場合は、[NSX Edge の再デプロイ (Redeploy NSX Edge)] アイコンをクリックして、アップグレードを再試行します。

NSX Edge ファイアウォール ルールは sourcePort をサポートしていないため、sourcePort を含むバージョン 5.5 の vShield Edge ルールはアップグレード中に次のように変更されます。

- ルールで application が使用されていない場合、サービスは「protocol=any」、「port=any」、および「sourcePort=asDefinedInTheRule」として作成されます。
- ルールに application または applicationGroup が使用されている場合、sourcePort を追加することで、これらのグループ オブジェクトが重複します。このため、ファイアウォール ルールで使用される groupingObjectId がアップグレード後に変更されます。

NSX Edge 6.x のユーザー ファイアウォール ルールでは、REST API からの入力に基づく内部 IPSet および applicationSet を生成しません。代わりに、これらを未加工のまま保持します。アップグレード中に、内部で生成された IPSet と applicationSet は、raw データでルールを作成する際に使用されます。内部 groupingObject は、ユーザーのファイアウォール ルールには表示されなくなります。

#### 次のステップ

必要な場合、L2 VPN 設定を再度行います。L2 VPN の概要については、『NSX インストール ガイド』を参照してください。

## アップグレード後のチェックリスト

アップグレードが完了したら、次の手順を実行します。

### 手順

- 1 アップグレード後に NSX Manager の現在のバックアップを作成します。
- 2 VIB がホストにインストールされていることを確認します。

NSX によって、これらの VIB がインストールされます。

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

ゲスト イントロスペクションがインストールされている場合、この VIB がホストに存在していることも確認します。

```
esxcli software vib get --vibname epsec-mux
```

- 3 ホストのメッセージ バスを再同期します。VMware は、アップグレード後に再同期することをすべてのカスタマにお勧めしています。

次の API コールを使用して、各ホストで再同期を実行します。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
```

Headers:

```
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

# NSX アップグレード

この章には、次のトピックが含まれています。

- NSX のアップグレードの準備
- NSX 6.1.x または 6.2.x から NSX 6.2.x へのアップグレード
- Cross-vCenter NSX での NSX 6.2.x へのアップグレード

## NSX のアップグレードの準備

NSX を正常にアップグレードするには、リリース ノートでアップグレードの問題を確認し、正しいアップグレード手順を実行していて、インフラストラクチャがアップグレードに適切に準備されていることを確認します。



**警告:** ダウングレードはサポートされない:

- アップグレードの前に、必ず NSX Manager をバックアップしてください。
- NSX Manager が正常にアップグレードされたあとは、NSX をダウングレードできません。

アップグレードは、企業で定められているメンテナンス期間中に実施することをお勧めします。

次のガイドラインは、アップグレード前のチェックリストとして使用できます。

- 1 vCenter Server が NSX のシステム要件を満たしていることを確認します。「[NSX のシステム要件](#)」を参照してください。
- 2 ゲスト イントロスペクションまたはネットワーク拡張性に関するパートナー サービスが展開されている場合、アップグレードの前に互換性を確認します。
  - ほとんどの場合、パートナー ソリューションに影響を与えることなく NSX をアップグレードできます。アップグレードする NSX のバージョンと、パートナー ソリューションとの間に互換性がない場合、NSX をアップグレードする前に、パートナー ソリューションを互換性のあるバージョンにアップグレードする必要があります。
  - VMware 互換性ガイドでネットワークとセキュリティについて確認します。  
<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security> を参照してください。
  - パートナー製品のドキュメントで、互換性とアップグレードの詳細について確認します。

- 3 環境内に Data Security がある場合は、NSX Manager のアップグレード前にアンインストールしておきます。  
[NSX Data Security のアンインストール] を参照してください。
- 4 同一の SSO サーバを使用する vCenter Server システム（拡張リンク モードの vCenter Server システムを含む）に接続している NSX Manager をすべてアップグレードすることを検討します。それが不可能な場合は、<https://kb.vmware.com/kb/2127061> で回避策を確認ください。
- 5 NSX Manager、vCenter Server、およびその他の NSX コンポーネントの最新のバックアップが作成済みであることを確認します。[NSX のバックアップとリストア] を参照してください。
- 6 テクニカル サポート バンドルを作成します。
- 7 nslookup コマンドを使用して、正引き/逆引きのドメイン名解決が動作していることを確認します。
- 8 環境で vSphere Update Manager (VUM) を使用している場合は、vCenter Server で bypassVumEnabled フラグが True に設定されていることを確認します。この設定によって、VUM がインストールされているときや使用できないときでも、VIB を ESXi ホストに直接インストールするように ESX Agent Manager (EAM) が設定されます。<http://kb.vmware.com/kb/2053782> を参照してください。
- 9 アップグレード バンドルをダウンロードしてステージングし、md5sum を使用して検証します。[NSX アップグレード バンドルのダウンロードと MD5 の確認] を参照してください。
- 10 ベスト プラクティスとして、すべてのアップグレード手順が完了するまでの間、環境内ですべての運用を停止することをお勧めします。
- 11 指示があるまでは、NSX のコンポーネントとアプライアンスのパワーオフや削除を行わないでください。

## NSX のアップグレードに必要なライセンスの確認

NSX では、2016 年 5 月から新しいライセンス モデルが導入されました。

有効なサポート契約を締結しており、前のバージョンの NSX から NSX 6.2.3 にアップグレードする場合、既存のライセンスは NSX Enterprise ライセンスに変換され、Enterprise 製品と同じ機能を利用する資格が付与されます。

NSX ライセンスに関する FAQ (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>) を参照してください。

## NSX アップグレードの運用上の影響

NSX のアップグレード、特にホストの再起動が必要になる ESXi ホストのアップグレードには時間がかかります。ホストの一部のみがアップグレードされている場合や、NSX Edge がまだアップグレードされていない場合など、アップグレード中の NSX コンポーネントの運用状態を理解しておくことが重要です。

1 回のメンテナンス期間ですべての NSX コンポーネントをアップグレードすることをお勧めします。この理由は、ダウンタイムを最小に抑えること、またアップグレード中に一部の NSX 管理機能を利用できなくなるため、NSX ユーザーの混乱を回避することです。しかし、サイトの要件により 1 回のメンテナンス期間でアップグレードを完了できない場合、以下の情報を参照することで、NSX ユーザーはアップグレード中にどの機能が利用可能かを確認できます。

NSX 環境のアップグレードは、次の順序で進みます。

NSX Manager -> NSX Controller クラスタ -> NSX ホスト クラスタ -> 分散論理ルーター -> ゲスト イントロスペクション

Edge Services Gateway は、NSX Manager のアップグレード後はいつでもアップグレードできます。

**重要:** アップグレードを開始する前に、[「NSX のアップグレードの準備」](#) および『NSX for vSphere リリース ノート』で、アップグレードの前提条件と既知の問題についてご確認ください。

## NSX Manager のアップグレード

NSX Manager アップグレードの計画：

- Cross-vCenter NSX 環境では、最初にプライマリ NSX Manager を、次にセカンダリ NSX Manager をアップグレードする必要があります。
- Cross-vCenter NSX 環境では、同じメンテナンス期間中にすべての NSX Manager をアップグレードする必要があります。
- NSX 6.1.x から NSX 6.2.x 以降にアップグレードする場合は、NSX Manager および NSX Controller クラスタを同じメンテナンス期間にアップグレードする必要があります。

NSX Manager アップグレード時の影響：

- vSphere Web Client と API を使用した NSX Manager 設定はブロックされます。
- 既存の仮想マシンの接続は引き続き機能します。
- 新しい仮想マシンのプロビジョニングは引き続き vSphere で機能しますが、NSX Manager のアップグレード中は、新しい仮想マシンは NSX に接続することも、論理スイッチから切断することもできません。
- Cross-vCenter NSX 環境で NSX Manager をアップグレードする場合、プライマリとすべてのセカンダリ NSX Manager がアップグレードされるまで、ユニバーサル オブジェクトを変更しないでください。これには、ユニバーサル オブジェクトの作成、更新、削除、ユニバーサル オブジェクトに関連する操作（たとえば、仮想マシンへのユニバーサル セキュリティ タグの適用）などが含まれます。

NSX Manager のアップグレード後：

- NSX の設定の変更はすべて許可されます。
- この段階で、新しい NSX Controller アプライアンスが展開される場合、NSX Controller クラスタがアップグレードされるまで、既存の NSX Controller クラスタに対応するバージョンで展開されます。
- 既存の NSX の設定に対する変更は許可されます。新しい論理スイッチ、分散論理ルーター、および Edge Services Gateway を展開できます。
- 分散ファイアウォールのアップグレード後に新しい機能が追加される場合、すべてのホストがアップグレードされるまで、新機能はユーザー インターフェイスでグレイアウトされ、設定できない状態になります。
- NSX のリリースによっては、NSX Manager のアップグレード完了後に、制御プレーンの [通信チャネルの健全性] のステータスが [不明] と表示されます。ステータスを [接続中] にするには、コントローラとホストのアップグレードを完了する必要があります。

## NSX Controller クラスタのアップグレード

NSX Controller アップグレードの計画：

- NSX Controller クラスタは、NSX Manager をアップグレードしてからアップグレードできます。

- Cross-vCenter NSX 環境では、すべての NSX Manager をアップグレードしてから NSX Controller クラスタをアップグレードする必要があります。
- NSX Manager アップグレードと同じメンテナンス期間中に NSX Controller クラスタをアップグレードすることをお勧めします。
- NSX 6.1.x から NSX 6.2.x 以降にアップグレードする場合は、NSX Manager および NSX Controller クラスタを同じメンテナンス期間にアップグレードする必要があります。

#### NSX Controller アップグレード時の影響：

- 論理ネットワークの作成と変更は、アップグレード プロセスではブロックされます。NSX Controller クラスタのアップグレード中は、論理ネットワークの設定を変更しないでください。
- このプロセスでは、新しい仮想マシンをプロビジョニングしないでください。また、アップグレード中は仮想マシンの移行や、DRS の使用を許可しないでください。
- アップグレード中に、一時的にマジョリティでない状態になることがあっても、既存の仮想マシンからネットワーク接続は失われません。
- アップグレード中、動的なルートの変更は許可しないでください。

#### NSX Controller のアップグレード後：

- 設定の変更は許可されます。

## NSX ホストのアップグレード

#### NSX ホスト クラスタのアップグレードの計画：

- NSX Manager および NSX Controller クラスタをアップグレードしてから、ホスト クラスタをアップグレードできます。
- ホスト クラスタは、NSX Manager および NSX Controller クラスタのアップグレードとは別のメンテナンス期間中にアップグレードできます。
- 同じメンテナンス期間中にすべてのホスト クラスタをアップグレードする必要はありません。
- NSX Manager にインストールされた NSX バージョンの新機能は、vSphere Web Client および API で認識されますが、VIB がアップグレードされるまで機能しない可能性があります。
- 特定の NSX リリースのすべての新機能を活用するにはホスト VIB と NSX Manager のバージョンが一致するように、ホスト クラスタをアップグレードします。

#### NSX ホスト クラスタ アップグレード時の影響：

- 設定の変更は、NSX Manager でブロックされません。
- コントローラからホストへの通信は後方互換です。つまり、アップグレードされたコントローラは、アップグレードされていないホストと通信できます。
- アップグレードはクラスタごとに実行されます。クラスタで DRS が有効な場合、DRS によってホストのアップグレード順序が管理されます。
- アップグレードが進行中のホストはメンテナンス モードにする必要があるため、仮想マシンはパワーオフするか、別のホストに退避させる必要があります。これは、DRS を使用するか、手動で実行できます。



- 論理ネットワークへの追加と変更は許可されます。
- 新しい仮想マシンのプロビジョニングは、メンテナンス モードでないホスト上で引き続き機能します。

## NSX Edge のアップグレード

NSX Edge アップグレードの計画：

- NSX Edge は、その他の NSX コンポーネントとは別のメンテナンス期間中にアップグレードできます。
- NSX Manager、NSX Controller クラスタ、およびホスト クラスタをアップグレードしてから、分散論理ルーターをアップグレードできます。
- NSX Controller クラスタやホスト クラスタをアップグレードしていなくても、Edge Services Gateway をアップグレードできます。
- 同じメンテナンス期間中にすべての NSX Edge をアップグレードする必要はありません。
- NSX Edge のアップグレードが可能だが、まだ実行していない場合、NSX Edge をアップグレードするまで、サイズ、リソース、およびデータストアの変更や、高度なデバッグおよびアプライアンス上の高可用性を有効にすることはできません。

NSX Edge アップグレード時の影響：

- 現在アップグレード中の NSX Edge デバイスでは、設定の変更はブロックされます。論理スイッチへの追加と変更は許可されます。新しい仮想マシンのプロビジョニングは引き続き機能します。
- パケット転送は一時的に中断されます。
- NSX Edge 6.0 以降では、グレースフル リスタートが有効になっていない場合、OSPF の隣接関係はアップグレード中に取り消されます。

NSX Edge のアップグレード後：

- 設定の変更はブロックされません。NSX のアップグレードによって追加された Edge Services Gateway の新機能は、NSX Controller とすべてのホスト クラスタがアップグレードされるまで設定できません。

## ゲスト イントロスペクションのアップグレード

ゲスト イントロスペクション アップグレードの計画：

- NSX Manager、NSX Controller クラスタ、およびホスト クラスタをアップグレードしてから、ゲスト イントロスペクションをアップグレードできます。
- パートナー ソリューションのアップグレード情報については、パートナーのドキュメントを参照してください。

ゲスト イントロスペクション アップグレード時の影響：

- 仮想マシンの追加、削除、また vMotion の実行など、仮想マシンが変更されると、NSX クラスタにある仮想マシンは保護されません。

ゲスト イントロスペクションのアップグレード後：

- 仮想マシンの追加、削除、また vMotion の実行中、仮想マシンは保護されます。

## NSX の動作状態の確認

アップグレードを開始する前に、NSX の動作状態をテストすることが重要です。このテストを実施しないと、アップグレード後に問題が発生した場合に、それがアップグレード プロセスによるものなのか、アップグレード プロセス以前から存在していたのかを判断することができなくなります。

NSX インフラストラクチャのアップグレードを開始する前に、環境内のすべてが問題なく機能していると仮定しないでください。必ず最初に確認を行います。

### 手順

- 1 NSX Manager、vCenter Server、ESXi および NSX Edge の現在のバージョンを記録します。
- 2 管理者ユーザーの ID とパスワードを特定します。
- 3 次のコンポーネントにログインできることを確認します。

- vCenter Server
- NSX Manager Web ユーザー インターフェイス
- Edge Services Gateway アプライアンス
- 分散論理ルーター アプライアンス
- NSX Controller アプライアンス

- 4 VXLAN セグメントが機能することを確認します。

パケット サイズを正しく設定し、DF ビットを含めるようにします。

- 異なるホストの同じ論理スイッチ上にある 2 台の仮想マシン間で ping を実行します。
  - Windows 仮想マシンから : `ping -l 1472 -f <dest VM>`
  - Linux 仮想マシンから : `ping -s 1472 -M do <dest VM>`
- 2 つのホストの VTEP インターフェイス間で ping を実行します。
  - `ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>`

---

**注:** ホストの VTEP IP を取得するには、ホストの [管理 (Manage)] > [ネットワーク (Networking)] > [仮想スイッチ (Virtual Switches)] ページで、vmknicPG IP アドレスを探します。

---

- 5 仮想マシンから ping を実行して、外部ネットワークとの接続性を確認します。
- 6 NSX 環境を視覚的に確認して、すべてのステータス インジケータが緑/正常/デプロイ済みの状態であることを確認します。
  - [インストール手順 (Installation)] > [管理 (Management)] を確認します。
  - [インストール手順 (Installation)] > [ホストの準備 (Host Preparation)] を確認します。
  - [インストール手順 (Installation)] > [論理ネットワークの準備 (Logical Network Preparation)] > [VXLAN 転送 (VXLAN Transport)] を確認します。
  - [論理スイッチ (Logical Switches)] を確認します。

- [NSX Edge (NSX Edges)] を確認します。
- 7 NSX Edge デバイスの BGP と OSPF の状態を記録します。
    - `show ip ospf neighbor`
    - `show ip bgp neighbor`
    - `show ip route`
  - 8 Syslog が設定されていることを確認します。  
[Syslog サーバの指定](#)を参照してください。
  - 9 可能な場合は、アップグレード前の環境で、新しいコンポーネントをいくつか作成して機能をテストします。
    - 新しい論理スイッチを作成します。
    - 新しい Edge Services Gateway と新しい分散論理ルーターを作成します。
    - 新しい論理スイッチに仮想マシンを接続して、機能をテストします。
  - 10 netcpad および vsfwd の user-world agent (UWA) の接続を検証します。
    - ESXi ホストで `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` を実行して、コントローラの接続状態を確認します。
    - NSX Manager で `show tech-support save session` コマンドを実行し、5671 を検索して、すべてのホストが NSX Manager に接続されていることを確認します。
  - 11 (オプション) テスト環境がある場合は、本番環境をアップグレードする前に、アップグレードとアップグレード後の機能をテストします。

## NSX Data Security のアンインストール

NSX Data Security を使用しなくなった、または NSX Manager をアップグレードする場合に、NSX Data Security をアンインストールします。NSX Data Security では直接アップグレードはサポートされていません。NSX Manager をアップグレードする前に、まず NSX Data Security をアンインストールすることが重要です。アップグレードが完了した後、NSX Data Security を再インストールします。

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

### 手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。
- 2 NSX Data Security サービスを選択し、[サービス デプロイを削除します (Delete Service Deployment)] (✖) アイコンをクリックします。
- 3 [削除の確認] ダイアログ ボックスで、[今すぐ削除する (Delete now)] をクリックするか、または削除を有効にする日時を選択します。
- 4 [OK] をクリックします。

## NSX のバックアップとリストア

すべての NSX コンポーネントを正しくバックアップすることは、障害が発生した場合にシステムを正常動作の状態にリストアするために重要です。

NSX Manager のバックアップには、コントローラ、論理スイッチ、ルーティング エンティティ、セキュリティ、ファイアウォール ルール、および NSX Manager ユーザー インターフェイスや API でユーザーが設定したその他のすべてを含む、あらゆる NSX 設定が含まれます。vCenter データベースと仮想スイッチのような関連要素は、別々にバックアップする必要があります。

少なくとも、定期的に NSX Manager と vCenter Server のバックアップを作成することをお勧めします。バックアップの頻度とスケジュールは、ビジネス上のニーズと操作手順によって異なる場合があります。設定の変更を何度も行う場合は、頻繁に NSX バックアップを作成することをお勧めします。

NSX Manager のバックアップは、オンデマンドで作成することも、時間単位、日単位、または週単位で作成することもできます。

次の場合にバックアップを作成することをお勧めします。

- NSX または vCenter Server をアップグレードする前。
- NSX または vCenter Server をアップグレードした後。
- NSX Controller、論理スイッチ、分散論理ルーター、Edge Services Gateway、セキュリティおよびファイアウォール ポリシーを作成した後など、0 日目に NSX コンポーネントをデプロイして初期設定を行った後。
- インフラストラクチャまたはトポロジを変更した後。
- 2 日目に大きな変更を行った後。

任意の時点でシステム全体をロールバックできるように、NSX コンポーネント (NSX Manager など) のバックアップを vCenter Server、クラウド管理システム、操作ツールなどの他の連携コンポーネントのバックアップと同時に行うことをお勧めします。

### NSX Manager データのバックアップ

NSX Manager データは、オンデマンド バックアップまたはスケジュール設定したバックアップを実行してバックアップできます。

NSX Manager のバックアップおよびリストアは、NSX Manager 仮想アプライアンス Web インターフェイスから、または NSX Manager API を使用して設定できます。バックアップは時間単位、日単位、週単位でスケジュール設定できます。

バックアップ ファイルは、NSX Manager が FTP または SFTP でアクセスできるリモートの格納場所に保存されます。NSX Manager データには、構成テーブル、イベント テーブル、監査ログ テーブルが含まれます。構成テーブルは、すべてのバックアップに含まれます。

リストアは、バックアップ バージョンと同じ NSX Manager バージョンでのみサポートされます。そのため、NSX アップグレードを実行する前と後に新規のバックアップ ファイルを作成し、古いバージョンと新しいバージョンのそれぞれにバックアップを作成することが重要です。

## 手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [アプライアンス管理] で、[バックアップとリストア] をクリックします。
- 3 バックアップ先を指定するには、[FTP サーバ設定] の横の [変更] をクリックします。
  - a バックアップシステムの IP アドレスまたはホスト名を入力します。
  - b 送信先でサポートされるプロトコルに応じて、[転送プロトコル] ドロップダウン メニューから [SFTP] または [FTP] を選択します。
  - c 必要に応じてデフォルトのポートを編集します。
  - d バックアップシステムにログインするために必要なユーザー名とパスワードを入力します。
  - e [バックアップディレクトリ] フィールドに、バックアップの保存先の絶対パスを入力します。

絶対パスを確認するには、FTP サーバにログインし、使用するディレクトリに移動して、現在のディレクトリのフルパスを表示するコマンド (**pwd**) を実行します。次はその例です。

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f [ファイル名のプリフィックス] に文字列を入力します。

このテキストがそれぞれのバックアップ ファイル名の前に追加され、バックアップシステムで容易に認識されるようになります。たとえば **ppdb** と入力すると、バックアップ ファイル名は **ppdbHH\_MM\_SS\_DayDDMonYYYY** となります。

- g パス フレーズを入力してバックアップを保護します。

このパス フレーズはバックアップをリストアするために必要となります。

- h [OK] をクリックします。

次はその例です。

- 4 オンデマンド バックアップの場合、[バックアップ] をクリックします。

新しいファイルが [バックアップ履歴] に追加されます。

- 5 スケジュール設定されたバックアップの場合、スケジュールの横にある [変更] をクリックします。

- a [バックアップ頻度] ドロップダウン メニューで、[時間単位]、[日単位]、または [週単位] を選択します。選択したバックアップ頻度によっては、[曜日]、[時間]、および [分] ドロップダウン メニューが無効になります。たとえば、[日単位] を選択すると、[曜日] ドロップダウン メニューは日次バックアップには適用されないため、無効になります。
- b 週単位バックアップの場合、データをバックアップする曜日を選択します。
- c 週単位バックアップまたは日単位バックアップの場合、バックアップを開始する時間を選択します。
- d 開始する分数を選択して、[スケジュール設定] をクリックします。
- 6 ログおよびフロー データをバックアップから除外するには、[除外] の横の [変更] をクリックします。
- a バックアップから除外する項目を選択します。
- b [OK] をクリックします。
- 7 FTP サーバの IP アドレス/ホスト名、認証情報、ディレクトリの詳細、パス フレーズを保存します。この情報は、バックアップをリストアするために必要です。

## NSX Manager バックアップのリストア

NSX Manager をリストアすると、バックアップ ファイルが NSX Manager アプライアンスでロードされます。バックアップ ファイルは、NSX Manager がアクセスできるリモート FTP または SFTP の場所に保存する必要があります。NSX Manager データには、構成テーブル、イベント テーブル、監査ログ テーブルが含まれます。

---

**重要:** バックアップ ファイルをリストアする前に、現在のデータをバックアップしてください。

---

### 前提条件

NSX Manager データをリストアする前に、NSX Manager アプライアンスを再インストールすることをお勧めします。既存の NSX Manager アプライアンスでリストア操作を実行しても機能する可能性はありますが、公式にはサポートされていません。既存の NSX Manager で障害が発生した場合は、新規の NSX Manager アプライアンスをデプロイすることが想定されています。

ベスト プラクティスとしては、新規でデプロイする NSX Manager アプライアンスの IP 情報およびバックアップ場所の情報の指定に使用できるように、既存の NSX Manager アプライアンスの現在の設定のスクリーンショットを取るか、メモを取ります。

### 手順

1 既存の NSX Manager アプライアンスのすべての設定のスクリーンショットを取るか、メモを取ります。

2 NSX Manager アプライアンスを新規にデプロイします。

バージョンはバックアップした NSX Manager アプライアンスと同じである必要があります。

3 新規の NSX Manager アプライアンスにログインします。

4 [アプライアンス管理] で、[バックアップとリストア (Backups & Restore)] をクリックします。

5 [FTP サーバ設定] で、[変更 (Change)] をクリックして設定を追加します。

バックアップ先画面の [ホスト IP アドレス (Host IP Address)]、[ユーザー名 (User Name)]、[パスワード (Password)]、[バックアップディレクトリ (Backup Directory)]、[ファイル名の接頭辞 (Filename Prefix)]、[パスフレーズ (Pass Phrase)] の各フィールドで、リストアするバックアップの場所を識別する必要があります。

6 [バックアップ履歴] セクションで、リストアするバックアップのチェック ボックスを選択し、[リストア (Restore)] をクリックします。

## NSX Edge のバックアップ

すべての NSX Edge 設定（分散論理ルーターおよび Edge Services Gateway）は、NSX Manager データ バックアップの一環としてバックアップされます。

NSX Manager の設定が変更されていない場合、NSX Edge を再デプロイする（vSphere Web Client で [NSX Edge の再デプロイ] アイコンをクリックする）ことで、アクセス不能または障害が発生した Edge Appliance 仮想マシンを再作成できます。

NSX Edge のバックアップを個別に作成することは、サポートされていません。

## vSphere Distributed Switch のバックアップ

vSphere Distributed Switch (VDS) および分散ポート グループの設定をファイルにエクスポートできます。

有効なネットワーク設定がファイルに保存され、ほかのデプロイ環境で利用できるようになります。

この機能は、vSphere Web Client 5.1 以降でのみ使用できます。VDS 設定およびポートグループ設定は、インポートの一環としてインポートされます。

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

## vCenter Server のバックアップ

NSX デプロイを保護するには、vCenter Server データベースをバックアップして仮想マシンのスナップショットを作成することが重要です。

vCenter Server のバックアップとリストアの手順、およびベスト プラクティスについては、お使いのバージョンの vCenter Server ドキュメントを参照してください。

仮想マシンのスナップショットについては、<http://kb.vmware.com/kb/1015180> を参照してください。

vCenter Server 5.5 に役立つリンク：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

vCenter Server 6.0 に役立つリンク：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

## NSX アップグレード バンドルのダウンロードと MD5 の確認

NSX アップグレード バンドルには、NSX インフラストラクチャのアップグレードに必要なすべてのファイルが含まれています。NSX Manager をアップグレードする前に、まず、アップグレードするバージョンに対応したアップグレード バンドルをダウンロードする必要があります。

### 前提条件

MD5 チェックサム ツールを用意します。

### 手順

- 1 NSX のアップグレード バンドルを、NSX Manager から参照できる場所にダウンロードします。アップグレード バンドルのファイル名は、**VMware-NSX-Manager-upgrade-bundle-`<releaseNumber>`-`<NSXbuildNumber>`.tar.gz** のような形式になっています。
- 2 NSX Manager のアップグレード ファイル名の末尾が tar.gz になっていることを確認します。  
一部のブラウザでファイル拡張子を変更される場合があります。たとえば、ダウンロード ファイルの名前が VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz の場合は、  
次のように名前を変更します。



VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.tar.gz

このように変更しないと、アップグレード バンドルのアップロード後に次のようなエラー メッセージが表示されます。「無効なアップグレード バンドル ファイル VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz です。アップグレード ファイル名の拡張子は tar.gz です。」

- 3 MD5 チェックサム ツールを使用して、VMware Web サイトに公開されているアップグレード バンドルの公式な MD5 サムと、チェックサム ツールで計算された MD5 サムを比較します。
  - a MD5 チェックサム ツールで、アップグレード バンドルを参照します。
  - b ツールを使用して、バンドルのチェックサムを計算します。
  - c VMware Web サイトにリストされているチェックサムをコピーアンドペーストします。
  - d ツールを使用して 2 つのチェックサムを比較します。

2 つのチェックサムが一致しない場合は、アップグレード バンドルのダウンロードをやり直します。

## NSX 6.1.x または 6.2.x から NSX 6.2.x へのアップグレード

NSX 6.2.x にアップグレードするには、本書に記載された順序で NSX コンポーネントをアップグレードする必要があります。

NSX コンポーネントは次の順序でアップグレードする必要があります。

- 1 NSX Manager アプライアンス
- 2 NSX Controller クラスタ
- 3 ホスト クラスタ
- 4 NSX Edge
- 5 ゲスト イントロスペクション

アップグレード プロセスは、NSX Manager によって管理されます。コンポーネントのアップグレードが失敗したり中断されたためにアップグレードのやり直しや再開が必要になる場合、プロセスは、最初からではなく中断された時点から開始されます。

アップグレード ステータスは、各ノードのクラスタ レベルで更新されます。

## NSX Manager のアップグレード

NSX インフラストラクチャのアップグレード プロセスでは、最初に NSX Manager アプライアンスのアップグレードを行います。

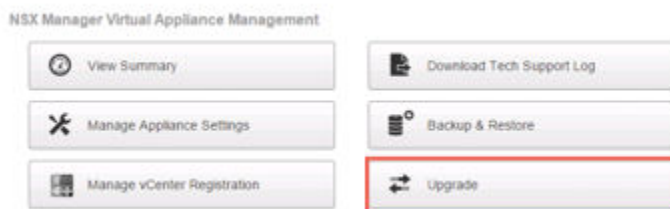
アップグレード中に、NSX のカスタマ エクスペリエンス改善プログラム (CEIP) への参加を選択できます。プログラムへの参加または参加を中止する方法については、『NSX 管理ガイド』の NSX のカスタマ エクスペリエンス改善プログラムのセクションを参照してください。

## 前提条件

- NSX Manager ファイル システムの使用量を確認し、ファイル システムの使用量が 100 パーセントの場合はクリーンアップを実行します。
  - a NSX Manager にログインし、**show filesystems to** を実行して、/dev/sda2 ファイルシステムの使用量を表示します。
  - b 使用率が 100% に達している場合は、**purge log manager** コマンドと **purge log system** コマンドを実行します。
  - c ログのクリーンアップを実行するために NSX Manager アプライアンスを再起動します。
- NSX 6.2.x にアップグレードする前に、NSX Manager 仮想アプライアンスの予約済みメモリを 16 GB 以上に増やします。  
[「NSX のシステム要件」](#) を参照してください。
- 環境内に Data Security がある場合は、NSX Manager のアップグレード前にアンインストールしておきます。  
[「NSX Data Security のアンインストール」](#) を参照してください。
- アップグレード前に、現在の設定をバックアップし、テクニカル サポート ログをダウンロードします。[「NSX のバックアップとリストア」](#) を参照してください。
- アップグレード バンドルをダウンロードして MD5 を確認します。[「NSX アップグレード バンドルのダウンロードと MD5 の確認」](#) を参照してください。
- NSX Manager のアップグレード進行中に発生する運用上の影響をよく理解します。[「NSX アップグレードの運用上の影響」](#) を参照してください。

## 手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 NSX Manager のホーム ページで、[アップグレード] をクリックします。



- 3 [アップグレード] をクリックし、[ファイルを選択] をクリックして、**VMware-NSX-Manager-upgrade-bundle-<releaseNumber>-<NSXbuildNumber>.tar.gz** ファイルを参照します。[続行] をクリックしてアップロードを開始します。

アップロードのステータスがブラウザ ウィンドウに表示されます。

- 4 [アップグレード] ダイアログ ボックスで、SSH を有効にするかどうかを指定し、VMware のカスタム エクスペリエンス改善プログラム (CEIP) に参加するかどうかを選択します。[アップグレード] をクリックしてアップグレードを開始します。

アップグレードのステータスがブラウザ ウィンドウに表示されます。

アップグレード手順が完了し、NSX Manager のログイン ページが表示されるまで待機します。

- 5 NSX Manager 仮想アプライアンスに再度ログインし、アップグレード状態が [完了] になっていることを確認します。また、右上に表示されているバージョンとビルド番号が、インストールしたアップグレード バンドルと一致することを確認します。

NSX Manager のアップグレード後に、vSphere Web Client からログアウトし、再度ログインする必要があります。

NSX プラグインが vSphere Web Client に正しく表示されない場合、ブラウザのキャッシュと履歴をクリアしてください。この手順を行わないと、vSphere Web Client で NSX の設定を変更したときに「内部エラーが発生しました - エラー #1009」のようなエラーが表示される場合があります。

vSphere Web Client で [Networking and Security] タブが表示されない場合には、vSphere Web Client サーバをリセットします。

- vCenter Server 5.5 で https://<vcenter-ip>:5480 を開き、Web Client サーバを再起動します。
- vCenter Server Appliance 6.0 で、vCenter Server シェルに root ユーザーとしてログインし、次のコマンドを実行します。

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Windows の vCenter Server 6.0 では、次のコマンドを実行するとアップグレードできます。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

異なるバージョンの NSX プラグインが実行中の場合は、予期しないエラーを回避するため、異なるバージョンの NSX Manager を実行している vCenter Server の管理に別々の Web Client をを使用することをお勧めします。

NSX Manager がアップグレードされたら、新しい NSX Manager バックアップ ファイルを作成します。[\[NSX のバックアップとリストア\]](#) を参照してください。以前の NSX Manager バックアップは、以前のリリースに対してのみ有効です。

#### 次のステップ

NSX Controller クラスタをアップグレードします。

## NSX Controller クラスタのアップグレード

環境内のコントローラは、クラスタ レベルでアップグレードされます。コントローラ ノードに対してアップグレードが利用可能な場合は、NSX Manager にアップグレード リンクが表示されます。

コントローラのアップグレードは、メンテナンス用時間枠内に実施することをお勧めします。

NSX コントローラのアップグレードを行うと、各コントローラ ノードにアップグレード ファイルがダウンロードされます。コントローラのアップグレードは 1 つずつ実行されます。アップグレードの進行中は、[アップグレードを利用可能] リンクはクリックできません。また、アップグレードが完了するまで、コントローラ クラスタをアップグレードするための API 呼び出しはブロックされます。

既存のコントローラがアップグレードされる前に新しいコントローラをデプロイすると、それらは古いバージョンとしてデプロイされます。クラスタに参加するためには、コントローラ ノードを同じバージョンにする必要があります。

### 前提条件

- すべてのコントローラが正常な状態であることを確認します。切断された状態のコントローラが 1 つでもあると、アップグレードは実行できません。切断されたコントローラを再接続するには、コントローラの仮想アプライアンスのリセットを試行します。[ホストおよびクラスタ] ビューで、コントローラを右クリックし、[パワー] > [リセット] の順に選択します。
- 有効な NSX コントローラ クラスタには、3 台のコントローラ ノードが含まれます。3 台のコントローラ ノードにログインし、[show controller-cluster status] コマンドを実行します。

```
controller-node# show control-cluster status
```

Type	Status	Since
Join status:	Join complete	05/04 02:36:03
Majority status:	Connected to cluster majority	05/19 23:57:23
Restart status:	This controller can be safely restarted	05/19 23:57:12
Cluster ID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Node UUID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

- Join status で、コントローラ ノードが参加完了 (Join Complete) であることを確認します。
- Majority status で、コントローラがクラスタ マジョリティ (cluster majority) に接続していることを確認します。
- Cluster ID で、クラスタ内のすべてのコントローラ ノードのクラスタ ID が同じであることを確認します。
- Configured status および Active status で、すべてのコントローラ ロールが有効 (enabled) であり、アクティベーション済み (activated) であることを確認します。

- NSX コントローラのアップグレード進行中に発生する運用上の影響を理解しておく必要があります。[「NSX アップグレードの運用上の影響」](#)を参照してください。

## 手順

- ◆ vSphere Web Client で [ホーム] > [Networking and Security] > [インストール] の順に移動し、[管理] タブを選択します。次に、[コントローラ クラスタのステータス] 列で [アップグレードを利用可能] をクリックします。

The screenshot shows the 'Installation' tab in the vSphere Web Client. It has sub-tabs for 'Management', 'Host Preparation', 'Logical Network Preparation', and 'Service Deployments'. The 'Management' sub-tab is active, showing 'NSX Managers' and 'NSX Controller nodes'.

**NSX Managers**

NSX Manager	IP Address	vCenter	Version	Controller Cluster Status
192.168.110.44	192.168.110.44	192.168.110.28	6.2.0.2860153	Upgrade Available

1 items

**NSX Controller nodes**

Controller IP Address	ID	Status	Upgrade Status	Software Version	NSX Manager
192.168.110.201	controller-1	✓ Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.202	controller-2	✓ Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.203	controller-3	✓ Normal	Not Started	6.2.4.1894	192.168.110.44

環境内のコントローラが1つずつアップグレードされて再起動されます。アップグレードを開始すると、システムはアップグレード ファイルをダウンロードし、各コントローラをアップグレードします。その後各コントローラを再起動して、各コントローラのアップグレード ステータスを更新します。次のフィールドにコントローラのステータスが表示されます。

- NSX Manager セクションの [コントローラ クラスタのステータス] 列に、クラスタのアップグレード ステータスが表示されます。アップグレードが開始されると、ステータスに [アップグレード ファイルをダウンロードしています] と表示されます。クラスタ内のすべてのコントローラにアップグレード ファイルがダウンロードされると、ステータスは [処理中] に変わります。クラスタ内のすべてのコントローラがアップグレードされると、ステータスに [完了] と表示され、この列は表示されなくなります。
- NSX コントローラ ノード セクションの [ステータス] 列に、[標準] などの、各コントローラのステータスが表示されます。コントローラ サービスがシャットダウンされ、コントローラが再起動されると、ステータスは [切断済み] に変わります。そのコントローラのアップグレードが完了すると、ステータスは再び [標準] になります。
- NSX コントローラ ノード セクションの [アップグレード ステータス] 列に、各コントローラのアップグレード ステータスが表示されます。ステータスは、まず [アップグレード ファイルをダウンロードしています] と表示され、次に [アップグレードが進行中です] となり、その後 [再起動中です] と表示されます。コントローラがアップグレードされると、ステータスは [アップグレード済み] と表示されます。

アップグレードが完了すると、NSX コントローラ ノード セクションの各コントローラの [ソフトウェア バージョン] 列に、[6.2.]<buildNumber> と表示されます。[show controller-cluster status] コマンドを再実行して、コントローラがマジョリティを作成できていることを確認します。NSX コントローラ クラスタ マジョリティが再形成されない場合は、コントローラと NSX Manager のログを確認します。

各アップグレードにかかる平均時間は 6 ～ 8 分です。アップグレードがタイムアウト期間（30 分）内に完了しない場合は、[アップグレード ステータス] 列に [失敗] と表示されます。NSX Manager セクションで再び [アップグレードを利用可能] をクリックし、停止した時点からアップグレード プロセスを再開します。

ネットワークの問題で、30 分のタイムアウト期間中に正常にアップグレードを完了できない場合は、タイムアウト期間の延長が必要になる場合があります。VMware のサポートと連携し、原因となる問題を診断および解決してから、必要に応じてタイムアウト期間を延長します。

コントローラのアップグレードが失敗する場合は、コントローラと NSX Manager の接続を確認します。

1 つ目のコントローラは正常にアップグレードされ、2 つ目は失敗するというシナリオについて考えます。クラスタ内に 3 つのコントローラがあり、1 つ目のコントローラは新しいバージョンに正常にアップグレードされ、2 つ目のコントローラはアップグレード中であるとします。2 つ目のコントローラのアップグレードが失敗する場合は、このコントローラが切断された状態のままになっている可能性があります。さらに、1 つ目と 3 つ目のコントローラがそれぞれ異なるバージョンになる（一方はアップグレード済みでもう一方は未アップグレード）ため、マジョリティを形成できなくなっています。この時点では、アップグレードを再び開始することはできません。このシナリオを解決するには、別のコントローラを作成します。新しく作成したコントローラを以前のバージョン（コントローラ 3 と同じ）にすると、コントローラ 3 と一緒にマジョリティを形成できます。これで、アップグレード手順を再開できるようになりました。

#### 次のステップ

ホスト クラスタをアップグレードします。

## ホスト クラスタのアップグレード

NSX Manager および NSX Controller のバージョン 6.2.x へのアップグレード後に、環境内の適切なクラスタを更新できます。このプロセスでは、クラスタ内の各ホストがソフトウェア アップデートを受け取り、再起動されます。

ホスト クラスタをアップグレードすると、NSX VIB、esx-vsip、および esx-vxlan がアップグレードされます。

- NSX 6.2 より前のバージョンの NSX からアップグレードしている場合、準備済みホストに esx-dvfilter-switch-security という追加の VIB が含まれます。NSX 6.2 以降では、esx-dvfilter-switch-security が esx-vxlan VIB に組み込まれています。
- バージョンが NSX 6.2.4 以降の NSX 6.2.x からアップグレードしている場合、準備済みホストには esx-vdpi という追加の VIB が含まれます。

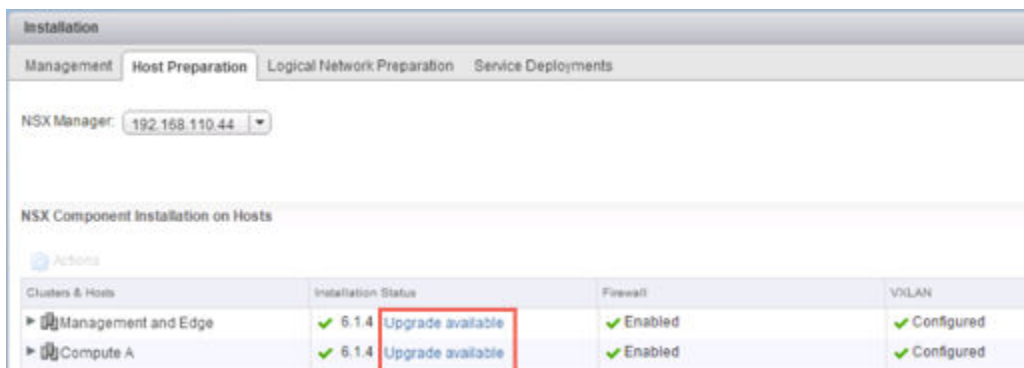
#### 前提条件

- すべてのホストの完全修飾ドメイン名 (FQDN) を解決できることを確認します。
- クラスタ内のホストのいずれかにログインして **esxcli software vib list** コマンドを実行します。次の VIB の現在のバージョンを記録します。
  - esx-vsip

- esx-vxlan
- NSX Manager と NSX Controller クラスタをアップグレードします。
- ホスト クラスタのアップグレード進行中に発生する運用上の影響をよく理解します。[「NSX アップグレードの運用上の影響」](#)を参照してください。
- DRS が無効な場合は、アップグレードを開始する前に、手動で仮想マシンのパワーオフまたは vMotion を実行します。
- DRS が有効な場合は、実行中の仮想マシンは、ホスト クラスタのアップグレード中に自動的に移動されます。アップグレードを開始する前に、環境内で DRS が機能できることを確認します。
  - ホスト クラスタで DRS が有効であることを確認します。
  - vMotion が正しく機能することを確認します。
  - ホストと vCenter Server の接続状態を確認します。
- 各ホスト クラスタに、少なくとも 3 台の ESXi ホストがあることを確認します。1 台または 2 台のホストを持つホスト クラスタでは、NSX のアップグレード中に、DRS のアドミSSION コントロールの問題が発生することがあります。NSX を正しくアップグレードするため、各ホスト クラスタに少なくとも 3 台のホストを含めることをお勧めします。クラスタに含まれるホストが 3 台より少ない場合は、ホストを手動で退避させることが推奨されます。
- ホストが 2 ～ 3 台の小規模クラスタで、特定の仮想マシンを個別のホストに配置することを指示する非アフィニティ ルールを作成している場合、これらのルールにより、アップグレード中の DRS による仮想マシンの移行が阻止される場合があります。クラスタにホストを追加するか、アップグレード中に非アフィニティ ルールを無効にして、アップグレードの完了後に非アフィニティ ルールを再度有効にします。非アフィニティ ルールを無効にするには、[ホストおよびクラスタ (Hosts and Clusters)] - [<Cluster>] - [管理 (Manage)] - [設定 (Settings)] - [仮想マシン/ホスト ルール (VM/Host Rules)] の順に移動します。ルールを編集して [ルールの有効化 (Enable rule)] の選択を解除します。

## 手順

- 1 vSphere Web Client で [ホーム] > [Networking and Security] > [インストール手順 (Home > Networking & Security > Installation)] の順に移動して [ホストの準備 (Host Preparation)] タブを選択します。
- 2 アップグレード対象の各クラスタに対して [アップグレードを利用可能 (Upgrade available)] をクリックします。



[インストール ステータス] に [インストールしています] と表示されています。

- 3 クラスタの [インストール ステータス] に **[準備ができていません]** と表示されています。[準備ができていません (Not Ready)] をクリックすると詳細を確認できます。[すべてを解決 (Resolve all)] をクリックすると、VIB のインストールの完了を試みます。

アップグレードを完了するため、ホストはメンテナンス モードに移行し、必要に応じて再起動されます。

[インストール ステータス] 列には、**[インストールしています]** と表示されます。アップグレードが完了すると、[インストール ステータス] 列に緑色のチェック マークと、アップグレード後の NSX のバージョンが表示されます。

- 4 DRS が有効になっている状態で [解決 (Resolve)] アクションが失敗する場合は、手動によるホストのメンテナンス モードへの移行が必要となることがあります (高可用性の要件や DRS ルールなどが原因)。その場合、アップグレード プロセスは中断し、クラスタの [インストール ステータス] に再度 **[準備ができていません]** と表示されます。[準備ができていません (Not Ready)] をクリックすると詳細を確認できます。[ホストおよびクラスタ (Hosts and Clusters)] ビューでホストを参照し、ホストがパワーオンおよび接続されていて、実行中の仮想マシンが含まれないことを確認します。再び [解決 (Resolve)] アクションを実行します。

[インストール ステータス] 列には、**[インストールしています]** と表示されます。アップグレードが完了すると、[インストール ステータス] 列に緑色のチェック マークと、アップグレード後の NSX のバージョンが表示されます。

ホストの更新を確認するには、クラスタ内のホストのいずれかにログインして **esxcli software vib list | grep esx** コマンドを実行します。次の VIB が正しいバージョンに更新されたことを確認します。

- esx-vsip
- esx-vxlan

ホストのアップグレードに失敗した場合は、次のトラブルシューティング手順を実行します。

- vCenter Server の ESX Agent Manager で、アラートおよびエラーを確認します。
- ホストにログインし、**/var/log/esxupdate.log** ログ ファイルで最近のアラートとエラーを確認します。
- DNS と NTP がホストに設定されていることを確認します。

トラブルシューティング手順の詳細については、『NSX トラブルシューティング ガイド』の「ホストの準備」を参照してください。

#### 次のステップ

[\[VXLAN ポートの変更\]](#)

## VXLAN ポートの変更

VXLAN トラフィックに使用するポートを変更できます。

NSX 6.2.3 以降では、デフォルトの VXLAN ポートは 4789 となり、標準ポートは IANA により割り当てられます。NSX 6.2.3 より前では、デフォルトの VXLAN UDP ポート番号は 8472 でした。

すべての新しい NSX インストール環境では、VXLAN に UDP ポート 4789 が使用されます。

NSX 6.2.2 以前のバージョンから NSX 6.2.3 以降にアップグレードする場合、アップグレード前の NSX で以前のデフォルト (8472) またはカスタム ポート番号 (8888 など) が使用されていた場合は、アップグレード後も、ユーザーが変更しない限り、引き続きそのポートが使用されます。



アップグレードされた NSX でハードウェア VTEP ゲートウェイ (ToR ゲートウェイ) が使用されている、またはその予定がある場合は、VXLAN ポート 4789 に切り替える必要があります。

Cross-vCenter NSX では、VXLAN ポートに 4789 を使用する必要はありませんが、同じ VXLAN ポートを使用するように Cross-vCenter NSX 環境にあるすべてのホストを設定する必要があります。ポート 4789 に切り替えると、Cross-vCenter NSX に追加される新しいすべての NSX インストール環境では、既存の NSX 環境と同じポートが使用されます。

VXLAN ポートの変更は 3 つのプロセスで行われ、処理中に VXLAN のトラフィックが中断されることはありません。

- 1 NSX Manager は、古いポートと新しいポートの両方で VXLAN トラフィックを待機するようにすべてのホストを設定します。ホストは引き続き、古いポートで VXLAN トラフィックを送信します。
- 2 NSX Manager は、新しいポートでトラフィックを送信するようにすべてのホストを設定します。
- 3 NSX Manager は、古いポートでの待機を停止するようにすべてのホストを設定します。すべてのトラフィックは新しいポートで送受信されます。

Cross-vCenter NSX 環境では、プライマリ NSX Manager でポート変更を開始する必要があります。各ステージにおいて、次のステージに進む前に、Cross-vCenter NSX 環境内のすべてのホストで設定変更が行われます。

#### 前提条件

- VXLAN に使用するポートがファイアウォールによってブロックされていないことを確認します。
- VXLAN ポートの変更時にホストの準備が実行されないことを確認します。

#### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [論理ネットワークの準備 (Logical Network Preparation)] タブをクリックし、次に [VXLAN 転送 (VXLAN Transport)] をクリックします。
- 4 [VXLAN ポート] パネルの [変更 (Change)] ボタンをクリックします。切り替え先のポートを入力します。4789 は、IANA が VXLAN 用に割り当てているポート番号です。

すべてのホストにポートの変更が適用されるまで、少し時間がかかります。

- 5 (オプション) ポート変更の進捗状況を確認するには、API 要求 `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` を使用します。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TW0</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

次のステップ

[「NSX Edge のアップグレード」](#)

## NSX Edge のアップグレード

NSX Edge は、NSX Controller クラスタやホスト クラスタのアップグレードに依存せずにアップグレードできます。NSX Controller クラスタやホスト クラスタをアップグレードしていなくても、NSX Edge をアップグレードできます。

アップグレード プロセス中、新しい Edge 仮想アプライアンスは既存のものと一緒にデプロイされます。新しい Edge の準備ができると、古い Edge の vNIC が切断され、新しい Edge の vNIC が接続されます。次に、新しい Edge は、接続されたスイッチの ARP キャッシュを更新するために、Gratuitous ARP (GARP) パケットを送信します。高可用性構成の場合は、アップグレード プロセスが 2 回実行されます。

このプロセスが、パケットの転送に一時的に影響する場合があります。Edge が ECMP モードで動作するように設定することで、この影響を抑えることができます。

グレースフル リスタートが有効ではない場合、アップグレード中に OSPF 近接関係が取り出されます。

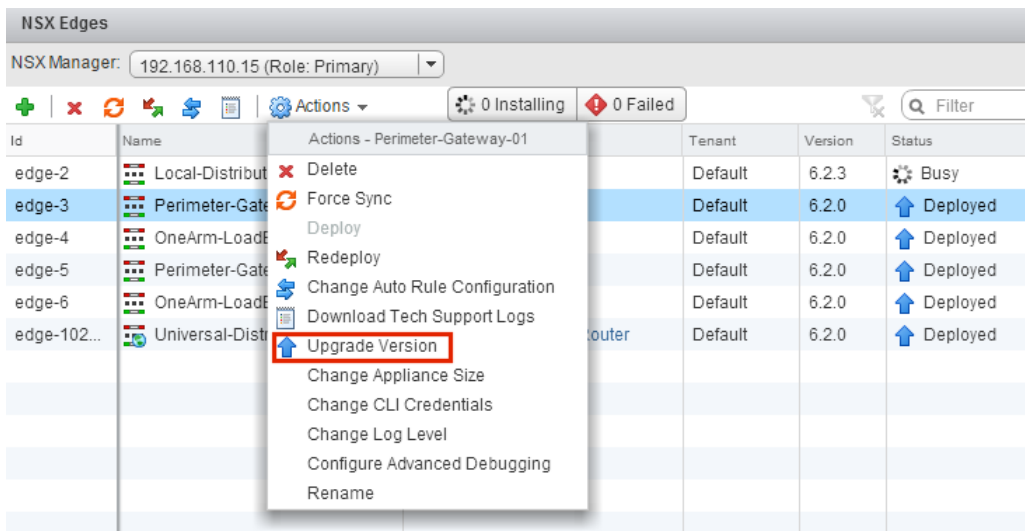
### 前提条件

- NSX Manager が 6.2.x にアップグレードされていることを確認します。
- NSX 論理スイッチを作成する計画がない場合でも、ローカル セグメント ID プールがあることを確認します。
- アップグレード中に追加の NSX Edge Services Gateway アプライアンスを展開するための十分なリソースがホストにあることを確認します。これは特に複数の NSX Edge アプライアンスを並行してアップグレードする場合に重要です。各サイズの NSX Edge で必要とされるリソースについては、[「NSX のシステム要件」](#)を参照してください。
  - アップグレード時は、1 台の NSX Edge インスタンスにつき、フルサイズの新しい NSX Edge アプライアンスがもう 1 台ホスト上に存在し、2 台ともパワーオン状態となります。
  - NSX 6.2.3 以降は、高可用性 (HA) 構成の 2 台の NSX Edge インスタンスを再デプロイする場合、2 台の新しいアプライアンスをデプロイしてから、2 台の古い アプライアンスと置き換えます。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 4 台存在することになります。NSX Edge インスタンスがアップグレードされると、高可用性アプライアンスのいずれかがアクティブになります。

- NSX 6.2.3 より前は、HA 構成の NSX Edge インスタンスのアップグレードで古いアプライアンスを置き換える場合、一度につき新しいアプライアンスを 1 台展開していました。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 3 台存在することになります。NSX Edge インスタンスがアップグレードされると、通常は HA インデックスが 0 の NSX Edge アプライアンスがアクティブになります。
- NSX Edge のアップグレード進行中に発生する運用上の影響について理解しておく必要があります。[\[NSX アップグレードの運用上の影響\]](#) を参照してください。
- L2 VPN が有効になっている場合、バージョン 5.5 または 6.0 の NSX Edge はアップグレードできません。アップグレードの前に、L2 VPN 設定を削除する必要があります。L2 VPN は、アップグレード後に再設定できます。詳細については、『NSX インストール ガイド』の「L2 VPN の概要」を参照してください。
- NSX 6.2.x から NSX 6.2.3 へのアップグレードで、ロード バランサがされている場合は、アップグレードの問題を回避するためのナレッジベースの記事 <https://kb.vmware.com/kb/2145887> を参照してください。

#### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 各 NSX Edge インスタンスで、[操作 (Actions)] メニューから [アップグレード バージョン (Upgrade Version)] を選択します。



「Edge アプライアンスをデプロイできませんでした。」というエラー メッセージが出てアップグレードが失敗した場合は、NSX Edge アプライアンスがデプロイされているホストが接続されており、メンテナンス モードになっていないことを確認します。

NSX Edge が正常にアップグレードされると、[ステータス (Status)] は [デプロイ済み] になり、[バージョン (Version)] 列に NSX のバージョンが表示されます。

Edge のアップグレードが失敗し、以前のバージョンにロールバックしない場合は、[NSX Edge の再デプロイ (Redeploy NSX Edge)] アイコンをクリックして、アップグレードを再実行します。

## 次のステップ

必要な場合、L2 VPN 設定を再度行います。L2 VPN の概要については、『NSX インストール ガイド』を参照してください。

## ゲスト イントロスペクションのアップグレード

ゲスト イントロスペクションをアップグレードする場合、NSX Manager と同じバージョンにすることが重要です。

**注:** ゲスト イントロスペクション サービス仮想マシンは、vSphere Web Client からアップグレードできます。NSX Manager のアップグレード後に、サービス仮想マシンをアップグレードするために削除する必要はありません。サービス仮想マシンを削除すると、エージェント仮想マシンが欠落するため、サービス ステータスが**失敗**と表示されます。[解決 (Resolve)] をクリックして新しいサービス仮想マシンを展開し、[アップグレードを利用可能 (Upgrade Available)] をクリックして最新のゲスト イントロスペクション サービス仮想マシンを展開します。

### 前提条件

NSX Manager、コントローラ、準備済みホスト クラスタ、および NSX Edge が 6.2.x にアップグレードされている必要があります。

### 手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。

The screenshot shows the NSX Manager interface. At the top, there's a tab bar with 'Installation', 'Management', 'Host Preparation', 'Logical Network Preparation', and 'Service Deployments'. The 'Service Deployments' tab is selected. Below the tabs, there's a dropdown for 'NSX Manager' showing '192.168.110.15 (Role: Primary)'. Underneath, there's a section titled 'Network & Security Service Deployments' with a description: 'Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.' Below this is a toolbar with icons for adding (+), deleting (x), refreshing (circular arrow), and upgrading (up arrow). To the right is a search filter box. The main part of the screenshot is a table with the following columns: Service, Version, Installation Status, Service Status, Cluster, Datastore, Port Group, and IP Address Range. The table contains one row for 'Guest Introspection' with version '6.2.0'. In the 'Installation Status' column, it shows a green checkmark for 'Succeeded' and a blue up arrow for 'Upgrade Available'. The 'Service Status' column shows a green checkmark for 'Up'. The 'Cluster' column shows 'Comp...', 'Datastore' shows 'ds-site...', 'Port Group' shows 'vds-sit...', and 'IP Address Range' shows 'GI Pool'.

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	Succeeded Upgrade Available	Up	Comp...	ds-site...	vds-sit...	GI Pool

[インストールの状態 (Installation Status)] 列に [アップグレードを利用可能 (Upgrade Available)] と表示されます。

- 2 アップグレード対象のゲスト イントロスペクション デプロイを選択します。

サービス テーブルの上のツールバーで、[アップグレード (Upgrade)] ( アイコンが有効になります。

- 3 [アップグレード (Upgrade)] (📌) アイコンをクリックして、ユーザー インターフェイスのプロンプトに従います。

**Confirm Upgrade**

Upgrade Guest Introspection service

Datastore \* ds-site-a-nfs01 ▼

Network \* vds-site-a\_Management... ▼

IP assignment \* GI Pool ▼

**Specify schedule:**

☒ Upgrade now

☐ Schedule the upgrade  6:29 PM ▼

OK Cancel

ゲスト イントロスペクションをアップグレードすると、インストールの状態は **成功しました** になり、サービスのステータスは **接続中** になります。ゲスト イントロスペクション サービスの仮想マシンは、vCenter Server インベントリに表示されます。

特定のクラスタのゲスト イントロスペクションをアップグレードした後、パートナー ソリューションをアップグレードできます。パートナー ソリューションが有効な場合、パートナーが提供するアップグレードのドキュメントを参照してください。パートナー ソリューションをアップグレードしない場合でも、保護が維持されます。

## 直接アップグレードをサポートしない NSX サービス

VMware Partner Security Virtual Appliances などのいくつかの NSX サービスは、直接アップグレードをサポートしません。この場合、サービスをアンインストールしてから、再度インストールを行う必要があります。

### VMware Partner Security Virtual Appliances

VMware パートナーのセキュリティ仮想アプライアンスがアップグレード可能かどうかは、パートナーが提供するドキュメントでご確認してください。

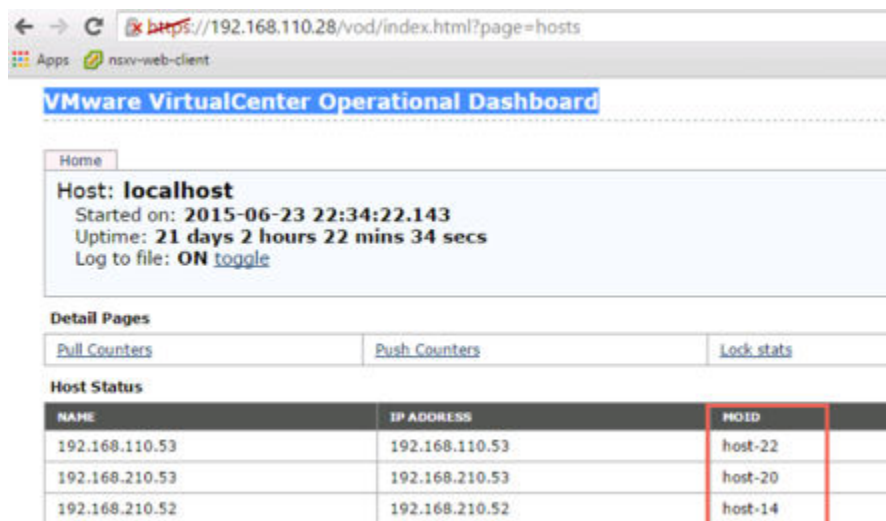
### NSX Data Security

NSX Data Security をアンインストールした後に NSX をアップグレードし、NSX のアップグレードが完了してから NSX Data Security を再インストールすることをお勧めします。NSX Data Security をアンインストールせずに NSX をアップグレードした場合は、REST API 呼び出しを使用して Data Security をアンインストールする必要があります。

次の API 呼び出しを実行します。

**DELETE** <https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds>

host-id は、ESXi ホストの MOID です。MOID を取得するには、VMware VirtualCenter Operational Dashboard (<https://<vcenter-ip>/vod/index.html?page=hosts>) を開きます。



vCenter Server 192.168.110.28 上にある、MOID が "host-22" の ESXi ホストの場合、API 呼び出しは次のような形式になります。

**DELETE** <https://192.168.110.28/api/1.0/vshield/host-22/vsds>

すべての ESXi ホストで API 呼び出しを実行するようにします。

Data Security のアンインストール後に、新しいバージョンをインストールできます。[「NSX Data Security のインストール」](#) を参照してください。

## NSX SSL VPN

NSX 6.2 以降、SSL VPN ゲートウェイで許容されるのは、TLS プロトコルのみにになります。しかし、NSX 6.2 以降へのアップグレード後、ユーザーが新規で作成するクライアントでは、接続を確立する間、自動的に TLS プロトコルが使用されます。また、NSX 6.2.3 以降では、TLS 1.0 は廃止されています。

プロトコルが変更されると、NSX 6.0.x クライアントが NSX 6.2 以降のゲートウェイへ接続する際、SSL ハンドシェイクの段階で接続の確立に失敗します。

NSX 6.0.x からのアップグレード後は、古い SSL VPN クライアントをアンインストールし、NSX 6.2.x バージョンの SSL VPN クライアントをインストールしてください。『NSX 管理ガイド』の「リモート サイトへの SSL クライアントのインストール」を参照してください。

## NSX L2 VPN

バージョン 5.5.x または 6.0.x の NSX Edge に L2 VPN がインストールされている場合、NSX Edge はアップグレードできません。NSX Edge をアップグレードする前に、すべての L2 VPN の設定を削除する必要があります。

## NSX Data Security のインストール

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

## 前提条件

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

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

## 手順

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

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

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

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

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

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

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

- 9 [IP 割り当て] で、次のいずれかを選択します。

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

固定 IP アドレスはサポートされていないことに注意してください。

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

## アップグレード後のチェックリスト

アップグレードが完了したら、次の手順を実行します。

### 手順

- 1 アップグレード後に NSX Manager の現在のバックアップを作成します。
- 2 VIB がホストにインストールされていることを確認します。

NSX によって、これらの VIB がインストールされます。

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

ゲスト イントロスペクションがインストールされている場合、この VIB がホストに存在していることも確認します。

```
esxcli software vib get --vibname epsec-mux
```

- 3 ホストのメッセージ バスを再同期します。VMware は、アップグレード後に再同期することをすべてのカスタマにお勧めしています。

次の API コールを使用して、各ホストで再同期を実行します。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

## Cross-vCenter NSX での NSX 6.2.x へのアップグレード

Cross-vCenter 環境で NSX 6.2.x にアップグレードするには、本書に記載された順序で NSX コンポーネントをアップグレードする必要があります。



NSX コンポーネントは次の順序でアップグレードする必要があります。

- 1 プライマリ NSX Manager アプライアンス
- 2 すべてのセカンダリ NSX Manager アプライアンス
- 3 NSX Controller クラスタ
- 4 ホスト クラスタ
- 5 NSX Edge
- 6 ゲスト イントロスペクション

アップグレード プロセスは、NSX Manager によって管理されます。コンポーネントのアップグレードが失敗または中断されたためにアップグレードをやり直したまたは再開する場合、プロセスは、最初からではなく中断された時点から開始されます。

アップグレード ステータスは、各ノードのクラスタ レベルで更新されます。

## Cross-vCenter NSX でのプライマリ NSX Manager のアップグレード

NSX インフラストラクチャのアップグレード プロセスでは、最初に、プライマリ NSX Manager アプライアンスのアップグレードを行います。

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



**警告:** Cross-vCenter NSX 環境で、異なるバージョンの NSX Manager のアプライアンスを実行することはできません。プライマリ NSX Manager アプライアンスをアップグレードしたら、セカンダリ NSX Manager アプライアンスをアップグレードする必要があります。

### 前提条件

- NSX Manager ファイル システムの使用量を確認し、ファイル システムの使用量が 100 パーセントの場合はクリーンアップを実行します。
  - a NSX Manager にログインし、**show filesystems to** を実行して、/dev/sda2 ファイルシステムの使用量を表示します。
  - b 使用率が 100% に達している場合は、**purge log manager** コマンドと **purge log system** コマンドを実行します。
  - c ログのクリーンアップを実行するために NSX Manager アプライアンスを再起動します。
- NSX 6.2.x にアップグレードする前に、NSX Manager 仮想アプライアンスの予約済みメモリを 16 GB 以上に増やします。

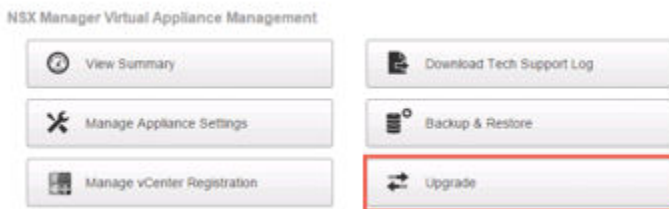
[「NSX のシステム要件」](#) を参照してください。

- 環境内に Data Security がある場合は、NSX Manager のアップグレード前にアンインストールしておきます。[「NSX Data Security のアンインストール」](#) を参照してください。

- アップグレード前に、現在の設定をバックアップし、テクニカル サポート ログをダウンロードします。[「NSX のバックアップとリストア」](#) を参照してください。
- アップグレード バンドルをダウンロードして MD5 を確認します。[「NSX アップグレード バンドルのダウンロードと MD5 の確認」](#) を参照してください。
- NSX Manager のアップグレード進行中に発生する運用上の影響をよく理解します。[「NSX アップグレードの運用上の影響」](#) を参照してください。

#### 手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 NSX Manager のホーム ページで、[アップグレード] をクリックします。



- 3 [アップグレード] をクリックし、[ファイルを選択] をクリックして、**VMware-NSX-Manager-upgrade-bundle--<releaseNumber>-<NSXbuildNumber>.tar.gz** ファイルを参照します。[続行] をクリックしてアップロードを開始します。

アップロードのステータスがブラウザ ウィンドウに表示されます。

- 4 [アップグレード] ダイアログ ボックスで、SSH を有効にするかどうかを指定し、VMware のカスタム エクスペリエンス改善プログラム (CEIP) に参加するかどうかを選択します。[アップグレード] をクリックしてアップグレードを開始します。

アップグレードのステータスがブラウザ ウィンドウに表示されます。

アップグレード手順が完了し、NSX Manager のログイン ページが表示されるまで待機します。

- 5 NSX Manager 仮想アプライアンスに再度ログインし、アップグレード状態が [完了] になっていることを確認します。また、右上に表示されているバージョンとビルド番号が、インストールしたアップグレード バンドルと一致することを確認します。

アップグレード中に vSphere Web Client にログインすると、[Networking and Security] - [インストール手順] - [管理] ページに同期の問題に関する警告が表示されます。これは、異なるバージョンの NSX で NSX Manager アプライアンスを使用しているためです。セカンダリ NSX Manager アプライアンスをアップグレードしなければ、次のアップグレード手順に進むことはできません。

NSX Manager のアップグレード後に、vSphere Web Client からログアウトし、再度ログインする必要があります。

NSX プラグインが vSphere Web Client に正しく表示されない場合、ブラウザのキャッシュと履歴をクリアしてください。この手順を行わないと、vSphere Web Client で NSX の設定を変更したときに「内部エラーが発生しました - エラー #1009」のようなエラーが表示される場合があります。

vSphere Web Client で [Networking and Security] タブが表示されない場合には、vSphere Web Client サーバをリセットします。

- vCenter Server 5.5 で `https://<vcenter-ip>:5480` を開き、Web Client サーバを再起動します。
- vCenter Server Appliance 6.0 で、vCenter Server シェルに root ユーザーとしてログインし、次のコマンドを実行します。

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Windows の vCenter Server 6.0 では、次のコマンドを実行するとアップグレードできます。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

異なるバージョンの NSX プラグインが実行中の場合は、予期しないエラーを回避するため、異なるバージョンの NSX Manager を実行している vCenter Server の管理に別々の Web Client を使用することをお勧めします。

NSX Manager がアップグレードされたら、新しい NSX Manager バックアップ ファイルを作成します。[「NSX のバックアップとリストア」](#) を参照してください。以前の NSX Manager バックアップは、以前のリリースに対してのみ有効です。

#### 次のステップ

すべてのセカンダリ NSX Manager アプライアンスをアップグレードします。

## Cross-vCenter NSX でのすべてのセカンダリ NSX Manager アプライアンスのアップグレード

他の NSX コンポーネントをアップグレードする前に、すべてのセカンダリ NSX Manager アプライアンスをアップグレードする必要があります。

次の手順で、セカンダリ NSX Manager アプライアンスをアップグレードします。Cross-vCenter NSX 環境にあるすべてのセカンダリ NSX Manager アプライアンスでこれらの手順を繰り返します。

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

## 前提条件

- プライマリ NSX Manager がアップグレードされていることを確認します。
- NSX Manager ファイル システムの使用量を確認し、ファイル システムの使用量が 100 パーセントの場合はクリーンアップを実行します。
  - a NSX Manager にログインし、**show filesystems to** を実行して、/dev/sda2 ファイルシステムの使用量を表示します。
  - b 使用率が 100% に達している場合は、**purge log manager** コマンドと **purge log system** コマンドを実行します。
  - c ログのクリーンアップを実行するために NSX Manager アプライアンスを再起動します。
- NSX 6.2.x にアップグレードする前に、NSX Manager 仮想アプライアンスの予約済みメモリを 16 GB 以上に増やします。  
[「NSX のシステム要件」](#) を参照してください。
- 環境内に Data Security がある場合は、NSX Manager のアップグレード前にアンインストールしておきます。  
[「NSX Data Security のアンインストール」](#) を参照してください。
- アップグレード前に、現在の設定をバックアップし、テクニカル サポート ログをダウンロードします。[「NSX のバックアップとリストア」](#) を参照してください。
- アップグレードバンドルをダウンロードして MD5 を確認します。[「NSX アップグレードバンドルのダウンロードと MD5 の確認」](#) を参照してください。
- NSX Manager のアップグレード進行中に発生する運用上の影響をよく理解します。[「NSX アップグレードの運用上の影響」](#) を参照してください。

## 手順

- 1 [アップグレード] をクリックし、[ファイルを選択] をクリックして、**VMware-NSX-Manager-upgrade-bundle-<releaseNumber>-<NSXbuildNumber>.tar.gz** ファイルを参照します。[続行] をクリックしてアップロードを開始します。  
 アップロードのステータスがブラウザ ウィンドウに表示されます。
- 2 [アップグレード] ダイアログ ボックスで、SSH を有効にするかどうかを指定し、VMware のカスタマ エクスペリエンス改善プログラム (CEIP) に参加するかどうかを選択します。[アップグレード] をクリックしてアップグレードを開始します。  
 アップグレードのステータスがブラウザ ウィンドウに表示されます。  
 アップグレード手順が完了し、NSX Manager のログイン ページが表示されるまで待機します。
- 3 NSX Manager 仮想アプライアンスに再度ログインし、アップグレード状態が [完了] になっていることを確認します。また、右上に表示されているバージョンとビルド番号が、インストールしたアップグレードバンドルと一致することを確認します。

NSX Manager のアップグレード後に、vSphere Web Client からログアウトし、再度ログインする必要があります。

NSX プラグインが vSphere Web Client に正しく表示されない場合、ブラウザのキャッシュと履歴をクリアしてください。この手順を行わないと、vSphere Web Client で NSX の設定を変更したときに「内部エラーが発生しました - エラー #1009」のようなエラーが表示される場合があります。

vSphere Web Client で [Networking and Security] タブが表示されない場合には、vSphere Web Client サーバをリセットします。

- vCenter Server 5.5 で https://<vcenter-ip>:5480 を開き、Web Client サーバを再起動します。
- vCenter Server Appliance 6.0 で、vCenter Server シェルに root ユーザーとしてログインし、次のコマンドを実行します。

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Windows の vCenter Server 6.0 では、次のコマンドを実行するとアップグレードできます。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

異なるバージョンの NSX プラグインが実行中の場合は、予期しないエラーを回避するため、異なるバージョンの NSX Manager を実行している vCenter Server の管理に別々の Web Client を使用することをお勧めします。

NSX Manager がアップグレードされたら、新しい NSX Manager バックアップ ファイルを作成します。[\[NSX のバックアップとリストア\]](#) を参照してください。以前の NSX Manager バックアップは、以前のリリースに対してのみ有効です。

#### 次のステップ

[\[Cross-vCenter NSX での NSX Controller クラスタのアップグレード\]](#)

## Cross-vCenter NSX での NSX Controller クラスタのアップグレード

環境内のコントローラは、クラスタ レベルでアップグレードされます。NSX Controller クラスタに対してアップグレードが利用可能な場合は、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [管理 (Management)] パネルの順に移動します。プライマリ NSX Manager の横にアップグレード リンクが表示されます。

コントローラのアップグレードは、メンテナンス用時間枠内に実施することをお勧めします。

NSX コントローラのアップグレードを行うと、各コントローラ ノードにアップグレード ファイルがダウンロードされます。コントローラのアップグレードは 1 つずつ実行されます。アップグレードの進行中は、[アップグレードを利用可能] リンクはクリックできません。また、アップグレードが完了するまで、コントローラ クラスタをアップグレードするための API 呼び出しはブロックされます。

既存のコントローラがアップグレードされる前に新しいコントローラをデプロイすると、それらは古いバージョンとしてデプロイされます。クラスタに参加するためには、コントローラ ノードを同じバージョンにする必要があります。

## 前提条件

- すべてのコントローラが正常な状態であることを確認します。切断された状態のコントローラが 1 つでもあると、アップグレードは実行できません。切断されたコントローラを再接続するには、コントローラの仮想アプライアンスのリセットを試行します。[ホストおよびクラスタ] ビューで、コントローラを右クリックし、[パワー] > [リセット] の順に選択します。
- 有効な NSX コントローラ クラスタには、3 台のコントローラ ノードが含まれます。3 台のコントローラ ノードにログインし、[show controller-cluster status] コマンドを実行します。

```
controller-node# show control-cluster status
```

Type	Status	Since
Join status:	Join complete	05/04 02:36:03
Majority status:	Connected to cluster majority	05/19 23:57:23
Restart status:	This controller can be safely restarted	05/19 23:57:12
Cluster ID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Node UUID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

- Join status で、コントローラ ノードが参加完了 (Join Complete) であることを確認します。
- Majority status で、コントローラがクラスタ マジョリティ (cluster majority) に接続していることを確認します。
- Cluster ID で、クラスタ内のすべてのコントローラ ノードのクラスタ ID が同じであることを確認します。
- Configured status および Active status で、すべてのコントローラ ロールが有効 (enabled) であり、アクティベーション済み (activated) であることを確認します。
- NSX コントローラのアップグレード進行中に発生する運用上の影響を理解しておく必要があります。[「NSX アップグレードの運用上の影響」](#) を参照してください。

## 手順

- ◆ vSphere Web Client で [ホーム] > [Networking and Security] > [インストール] の順に移動し、[管理] タブを選択します。次に、[コントローラ クラスタのステータス] 列で [アップグレードを利用可能] をクリックします。

The screenshot shows the 'Installation' tab in the vSphere Web Client. It has sub-tabs: Management, Host Preparation, Logical Network Preparation, and Service Deployments. The 'NSX Managers' section shows a table with one entry: IP Address 192.168.110.44, vCenter 192.168.110.28, Version 6.2.0.2860153, and Controller Cluster Status Upgrade Available (highlighted with a red box). The 'NSX Controller nodes' section shows a table with three entries, all with Status Normal and Upgrade Status Not Started.

NSX Manager	IP Address	vCenter	Version	Controller Cluster Status
192.168.110.44	192.168.110.44	192.168.110.28	6.2.0.2860153	Upgrade Available

Controller IP Address	ID	Status	Upgrade Status	Software Version	NSX Manager
192.168.110.201	controller-1	✓ Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.202	controller-2	✓ Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.203	controller-3	✓ Normal	Not Started	6.2.4.1894	192.168.110.44

環境内のコントローラが1つずつアップグレードされて再起動されます。アップグレードを開始すると、システムはアップグレードファイルをダウンロードし、各コントローラをアップグレードします。その後各コントローラを再起動して、各コントローラのアップグレードステータスを更新します。次のフィールドにコントローラのステータスが表示されます。

- NSX Manager セクションの [コントローラ クラスタのステータス] 列に、クラスタのアップグレードステータスが表示されます。アップグレードが開始されると、ステータスに [アップグレードファイルをダウンロードしています] と表示されます。クラスタ内のすべてのコントローラにアップグレードファイルがダウンロードされると、ステータスは [処理中] に変わります。クラスタ内のすべてのコントローラがアップグレードされると、ステータスに [完了] と表示され、この列は表示されなくなります。
- NSX コントローラ ノード セクションの [ステータス] 列に、[標準] などの、各コントローラのステータスが表示されます。コントローラ サービスがシャットダウンされ、コントローラが再起動されると、ステータスは [切断済み] に変わります。そのコントローラのアップグレードが完了すると、ステータスは再び [標準] になります。
- NSX コントローラ ノード セクションの [アップグレードステータス] 列に、各コントローラのアップグレードステータスが表示されます。ステータスは、まず [アップグレードファイルをダウンロードしています] と表示され、次に [アップグレードが進行中です] となり、その後 [再起動中です] と表示されます。コントローラがアップグレードされると、ステータスは [アップグレード済み] と表示されます。

アップグレードが完了すると、NSX コントローラ ノード セクションの各コントローラの [ソフトウェアバージョン] 列に、[6.2.]<buildNumber> と表示されます。[show controller-cluster status] コマンドを再実行して、コントローラがマジョリティを作成できていることを確認します。NSX コントローラ クラスタ マジョリティが再形成されない場合は、コントローラと NSX Manager のログを確認します。

コントローラをアップグレードした後、1 台以上のコントローラ ノードに新しいコントローラ ID が割り当てられる場合があります。この動作は予期されるもので、セカンダリの NSX Manager がノードをポーリングするタイミングによって行われます。

各アップグレードにかかる平均時間は 6 ～ 8 分です。アップグレードがタイムアウト期間（30 分）内に完了しない場合は、[アップグレード ステータス] 列に [失敗] と表示されます。NSX Manager セクションで再び [アップグレードを利用可能] をクリックし、停止した時点からアップグレード プロセスを再開します。

ネットワークの問題で、30 分のタイムアウト期間中に正常にアップグレードを完了できない場合は、タイムアウト期間の延長が必要になる場合があります。VMware のサポートと連携し、原因となる問題を診断および解決してから、必要に応じてタイムアウト期間を延長します。

コントローラのアップグレードが失敗する場合は、コントローラと NSX Manager の接続を確認します。

1 つ目のコントローラは正常にアップグレードされ、2 つ目は失敗するというシナリオについて考えます。クラスタ内に 3 つのコントローラがあり、1 つ目のコントローラは新しいバージョンに正常にアップグレードされ、2 つ目のコントローラはアップグレード中であるとします。2 つ目のコントローラのアップグレードが失敗する場合は、このコントローラが切断された状態のままになっている可能性があります。さらに、1 つ目と 3 つ目のコントローラがそれぞれ異なるバージョンになる（一方はアップグレード済みでもう一方は未アップグレード）ため、マジョリティを形成できなくなっています。この時点では、アップグレードを再び開始することはできません。このシナリオを解決するには、別のコントローラを作成します。新しく作成したコントローラを以前のバージョン（コントローラ 3 と同じ）にすると、コントローラ 3 と一緒にマジョリティを形成できます。これで、アップグレード手順を再開できるようになりました。

#### 次のステップ

[「Cross-vCenter NSX 環境でのホスト クラスタのアップグレード」](#)。

## Cross-vCenter NSX 環境でのホスト クラスタのアップグレード

すべての NSX Manager アプライアンスと NSX Controller クラスタを NSX 6.2.x にアップグレードした後、Cross-vCenter NSX 環境のすべてのホスト クラスタを更新する必要があります。このプロセスでは、クラスタ内の各ホストがソフトウェア アップデートを受け取り、再起動されます。

ホスト クラスタをアップグレードすると、NSX VIB、esx-vsip、および esx-vxlan がアップグレードされます。

- NSX 6.2 より前のバージョンの NSX からアップグレードしている場合、準備済みホストに esx-dvfilter-switch-security という追加の VIB が含まれます。NSX 6.2 以降では、esx-dvfilter-switch-security が esx-vxlan VIB に組み込まれています。
- バージョンが NSX 6.2.4 以降の NSX 6.2.x からアップグレードしている場合、準備済みホストには esx-vmapi という追加の VIB が含まれます。

#### 前提条件

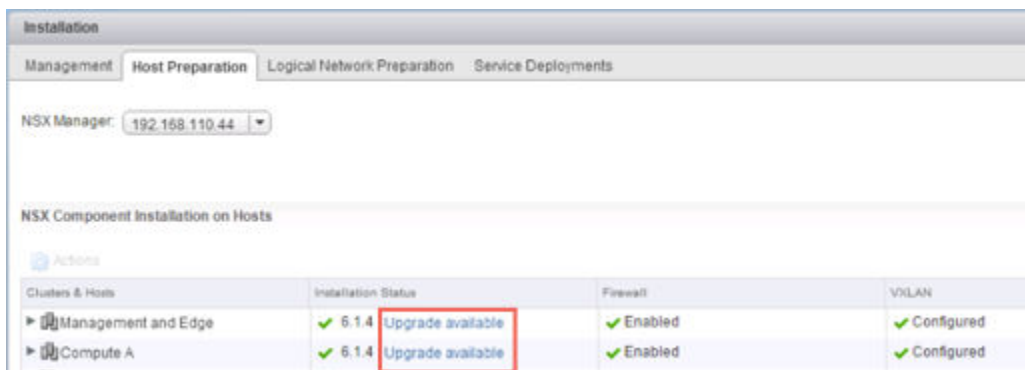
- すべてのホストの完全修飾ドメイン名 (FQDN) を解決できることを確認します。
- クラスタ内のホストのいずれかにログインして **esxcli software vib list** コマンドを実行します。次の VIB の現在のバージョンを記録します。
  - esx-vsip



- esx-vxlan
- NSX Manager と NSX Controller クラスタをアップグレードします。
- ホスト クラスタのアップグレード進行中に発生する運用上の影響をよく理解します。[「NSX アップグレードの運用上の影響」](#)を参照してください。
- DRS が無効な場合は、アップグレードを開始する前に、手動で仮想マシンのパワーオフまたは vMotion を実行します。
- DRS が有効な場合は、実行中の仮想マシンは、ホスト クラスタのアップグレード中に自動的に移動されます。アップグレードを開始する前に、環境内で DRS が機能できることを確認します。
  - ホスト クラスタで DRS が有効であることを確認します。
  - vMotion が正しく機能することを確認します。
  - ホストと vCenter Server の接続状態を確認します。
- 各ホスト クラスタに、少なくとも 3 台の ESXi ホストがあることを確認します。1 台または 2 台のホストを持つホスト クラスタでは、NSX のアップグレード中に、DRS のアドミッション コントロールの問題が発生することがあります。NSX を正しくアップグレードするため、各ホスト クラスタに少なくとも 3 台のホストを含めることをお勧めします。クラスタに含まれるホストが 3 台より少ない場合は、ホストを手動で退避させることが推奨されます。
- ホストが 2 ～ 3 台の小規模クラスタで、特定の仮想マシンを個別のホストに配置することを指示する非アフィニティ ルールを作成している場合、これらのルールにより、アップグレード中の DRS による仮想マシンの移行が阻止される場合があります。クラスタにホストを追加するか、アップグレード中に非アフィニティ ルールを無効にして、アップグレードの完了後に非アフィニティ ルールを再度有効にします。非アフィニティ ルールを無効にするには、[ホストおよびクラスタ (Hosts and Clusters)] - [<Cluster>] - [管理 (Manage)] - [設定 (Settings)] - [仮想マシン/ホスト ルール (VM/Host Rules)] の順に移動します。ルールを編集して [ルールの有効化 (Enable rule)] の選択を解除します。

## 手順

- 1 vSphere Web Client で [ホーム] > [Networking and Security] > [インストール手順 (Home > Networking & Security > Installation)] の順に移動して [ホストの準備 (Host Preparation)] タブを選択します。
- 2 アップグレード対象の各クラスタに対して [アップグレードを利用可能 (Upgrade available)] をクリックします。



[インストール ステータス] に [インストールしています] と表示されています。

- 3 クラスタの [インストール ステータス] に **[準備ができていません]** と表示されています。[準備ができていません (Not Ready)] をクリックすると詳細を確認できます。[すべてを解決 (Resolve all)] をクリックすると、VIB のインストールの完了を試みます。

アップグレードを完了するため、ホストはメンテナンス モードに移行し、必要に応じて再起動されます。

[インストール ステータス] 列には、**[インストールしています]** と表示されます。アップグレードが完了すると、[インストール ステータス] 列に緑色のチェック マークと、アップグレード後の NSX のバージョンが表示されます。

- 4 DRS が有効になっている状態で [解決 (Resolve)] アクションが失敗する場合は、手動によるホストのメンテナンス モードへの移行が必要となることがあります (高可用性の要件や DRS ルールなどが原因)。その場合、アップグレード プロセスは中断し、クラスタの [インストール ステータス] に再度 **[準備ができていません]** と表示されます。[準備ができていません (Not Ready)] をクリックすると詳細を確認できます。[ホストおよびクラスタ (Hosts and Clusters)] ビューでホストを参照し、ホストがパワーオンおよび接続されていて、実行中の仮想マシンが含まれないことを確認します。再び [解決 (Resolve)] アクションを実行します。

[インストール ステータス] 列には、**[インストールしています]** と表示されます。アップグレードが完了すると、[インストール ステータス] 列に緑色のチェック マークと、アップグレード後の NSX のバージョンが表示されます。

ホストの更新を確認するには、クラスタ内のホストのいずれかにログインして **esxcli software vib list | grep esx** コマンドを実行します。次の VIB が正しいバージョンに更新されたことを確認します。

- esx-vsip
- esx-vxlan

ホストのアップグレードに失敗した場合は、次のトラブルシューティング手順を実行します。

- vCenter Server の ESX Agent Manager で、アラートおよびエラーを確認します。
- ホストにログインし、**/var/log/esxupdate.log** ログ ファイルで最近のアラートとエラーを確認します。
- DNS と NTP がホストに設定されていることを確認します。

トラブルシューティング手順の詳細については、『NSX トラブルシューティング ガイド』の「ホストの準備」を参照してください。

## Cross-vCenter NSX での VXLAN ポートの変更

VXLAN トラフィックに使用するポートを変更できます。

NSX 6.2.3 以降では、デフォルトの VXLAN ポートは 4789 となり、標準ポートは IANA により割り当てられます。NSX 6.2.3 より前では、デフォルトの VXLAN UDP ポート番号は 8472 でした。

すべての新しい NSX インストール環境では、VXLAN に UDP ポート 4789 が使用されます。

NSX 6.2.2 以前のバージョンから NSX 6.2.3 以降にアップグレードする場合、アップグレード前の NSX で以前のデフォルト (8472) またはカスタム ポート番号 (8888 など) が使用されていた場合は、アップグレード後も、ユーザーが変更しない限り、引き続きそのポートが使用されます。

アップグレードされた NSX でハードウェア VTEP ゲートウェイ (ToR ゲートウェイ) が使用されている、またはその予定がある場合は、VXLAN ポート 4789 に切り替える必要があります。

Cross-vCenter NSX では、VXLAN ポートに 4789 を使用する必要はありませんが、同じ VXLAN ポートを使用するように Cross-vCenter NSX 環境にあるすべてのホストを設定する必要があります。ポート 4789 に切り替えると、Cross-vCenter NSX に追加される新しいすべての NSX インストール環境では、既存の NSX 環境と同じポートが使用されます。

VXLAN ポートの変更は 3 つのプロセスで行われ、処理中に VXLAN のトラフィックが中断されることはありません。

- 1 NSX Manager は、古いポートと新しいポートの両方で VXLAN トラフィックを待機するようにすべてのホストを設定します。ホストは引き続き、古いポートで VXLAN トラフィックを送信します。
- 2 NSX Manager は、新しいポートでトラフィックを送信するようにすべてのホストを設定します。
- 3 NSX Manager は、古いポートでの待機を停止するようにすべてのホストを設定します。すべてのトラフィックは新しいポートで送受信されます。

Cross-vCenter NSX 環境では、プライマリ NSX Manager でポート変更を開始する必要があります。各ステージにおいて、次のステージに進む前に、Cross-vCenter NSX 環境内のすべてのホストで設定変更が行われます。

#### 前提条件

- VXLAN に使用するポートがファイアウォールによってブロックされていないことを確認します。
- VXLAN ポートの変更時にホストの準備が実行されないことを確認します。

#### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [論理ネットワークの準備 (Logical Network Preparation)] タブをクリックし、次に [VXLAN 転送 (VXLAN Transport)] をクリックします。
- 4 [VXLAN ポート] パネルの [変更 (Change)] ボタンをクリックします。切り替え先のポートを入力します。4789 は、IANA が VXLAN 用に割り当てているポート番号です。

すべてのホストにポートの変更が適用されるまで、少し時間がかかります。

- 5 (オプション) ポート変更の進捗状況を確認するには、API 要求 `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` を使用します。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TW0</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

#### 次のステップ

[「Cross-vCenter NSX での NSX Edge のアップグレード」](#)

## Cross-vCenter NSX での NSX Edge のアップグレード

NSX Edge は、NSX Controller クラスタやホスト クラスタのアップグレードに依存せずにアップグレードできます。NSX Controller クラスタやホスト クラスタをアップグレードしていなくても、NSX Edge をアップグレードできます。Cross-vCenter NSX 環境のすべての NSX インスタンスで NSX Edge をアップグレードします。

アップグレード プロセス中、新しい Edge 仮想アプライアンスは既存のものと一緒にデプロイされます。新しい Edge の準備ができると、古い Edge の vNIC が切断され、新しい Edge の vNIC が接続されます。次に、新しい Edge は、接続されたスイッチの ARP キャッシュを更新するために、Gratuitous ARP (GARP) パケットを送信します。高可用性構成の場合は、アップグレード プロセスが 2 回実行されます。

このプロセスが、パケットの転送に一時的に影響する場合があります。Edge が ECMP モードで動作するように設定することで、この影響を抑えることができます。

グレースフル リスタートが有効ではない場合、アップグレード中に OSPF 近接関係が取り出されます。

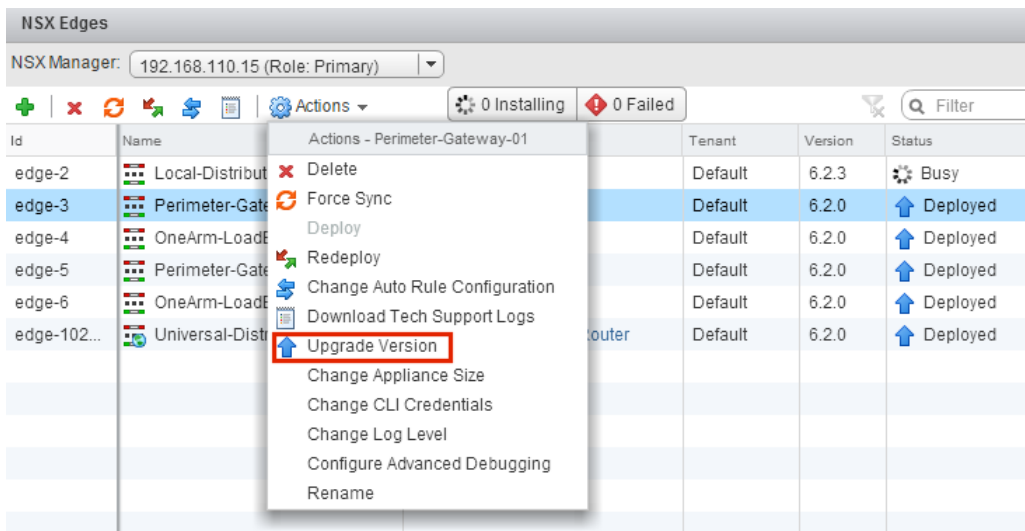
#### 前提条件

- NSX Manager が 6.2.x にアップグレードされていることを確認します。
- NSX 論理スイッチを作成する計画がない場合でも、ローカル セグメント ID プールがあることを確認します。
- アップグレード中に追加の NSX Edge Services Gateway アプライアンスを展開するための十分なリソースがホストにあることを確認します。これは特に複数の NSX Edge アプライアンスを並行してアップグレードする場合に重要です。各サイズの NSX Edge で必要とされるリソースについては、[「NSX のシステム要件」](#)を参照してください。
  - アップグレード時は、1 台の NSX Edge インスタンスにつき、フルサイズの新しい NSX Edge アプライアンスがもう 1 台ホスト上に存在し、2 台ともパワーオン状態となります。
  - NSX 6.2.3 以降は、高可用性 (HA) 構成の 2 台の NSX Edge インスタンスを再デプロイする場合、2 台の新しいアプライアンスをデプロイしてから、2 台の古いアプライアンスと置き換えます。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 4 台存在することになります。NSX Edge インスタンスがアップグレードされると、高可用性アプライアンスのいずれかがアクティブになります。

- NSX 6.2.3 より前は、HA 構成の NSX Edge インスタンスのアップグレードで古いアプライアンスを置き換える場合、一度につき新しいアプライアンスを 1 台展開していました。つまり、パワーオン状態のフルサイズの NSX Edge アプライアンスが、NSX Edge のアップグレード中に 3 台存在することになります。NSX Edge インスタンスがアップグレードされると、通常は HA インデックスが 0 の NSX Edge アプライアンスがアクティブになります。
- NSX Edge のアップグレード進行中に発生する運用上の影響について理解しておく必要があります。[\[NSX アップグレードの運用上の影響\]](#) を参照してください。
- L2 VPN が有効になっている場合、バージョン 5.5 または 6.0 の NSX Edge はアップグレードできません。アップグレードの前に、L2 VPN 設定を削除する必要があります。L2 VPN は、アップグレード後に再設定できます。詳細については、『NSX インストール ガイド』の「L2 VPN の概要」を参照してください。
- NSX 6.2.x から NSX 6.2.3 へのアップグレードで、ロード バランサがされている場合は、アップグレードの問題を回避するためのナレッジベースの記事 <https://kb.vmware.com/kb/2145887> を参照してください。

#### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 各 NSX Edge インスタンスで、[操作 (Actions)] メニューから [アップグレード バージョン (Upgrade Version)] を選択します。



「Edge アプライアンスをデプロイできませんでした。」というエラー メッセージが出てアップグレードが失敗した場合は、NSX Edge アプライアンスがデプロイされているホストが接続されており、メンテナンス モードになっていないことを確認します。

NSX Edge が正常にアップグレードされると、[ステータス (Status)] は [デプロイ済み] になり、[バージョン (Version)] 列に NSX のバージョンが表示されます。

Edge のアップグレードが失敗し、以前のバージョンにロールバックしない場合は、[NSX Edge の再デプロイ (Redeploy NSX Edge)] アイコンをクリックして、アップグレードを再試行します。

## 次のステップ

必要な場合、L2 VPN 設定を再度行います。L2 VPN の概要については、『NSX インストール ガイド』を参照してください。

[「Cross-vCenter NSX でのゲスト イントロスペクションのアップグレード」](#)

## Cross-vCenter NSX でのゲスト イントロスペクションのアップグレード

ゲスト イントロスペクションをアップグレードする場合、NSX Manager と同じバージョンにすることが重要です。

**注:** ゲスト イントロスペクション サービス仮想マシンは、vSphere Web Client からアップグレードできます。NSX Manager のアップグレード後に、サービス仮想マシンをアップグレードするために削除する必要はありません。サービス仮想マシンを削除すると、エージェント仮想マシンが欠落するため、サービス ステータスが**失敗**と表示されます。[解決 (Resolve)] をクリックして新しいサービス仮想マシンを展開し、[アップグレードを利用可能 (Upgrade Available)] をクリックして最新のゲスト イントロスペクション サービス仮想マシンを展開します。

## 前提条件

NSX Manager、コントローラ、準備済みホスト クラスタ、および NSX Edge が 6.2.x にアップグレードされている必要があります。

## 手順

- 1 [インストール手順 (Installation)] タブで、[サービス デプロイ (Service Deployments)] をクリックします。

The screenshot shows the NSX Manager interface. At the top, there's a tab bar with 'Management', 'Host Preparation', 'Logical Network Preparation', and 'Service Deployments'. Below the tabs, it says 'NSX Manager: 192.168.110.15 (Role: Primary)'. The main section is titled 'Network & Security Service Deployments' and contains a table of service deployments.

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	<div>✓ Succeeded</div> <div>⬆ Upgrade Available</div>	✓ Up	Comp...	ds-site...	vds-sit...	GI Pool

[インストールの状態 (Installation Status)] 列に [アップグレードを利用可能 (Upgrade Available)] と表示されます。

- 2 アップグレード対象のゲスト イントロスペクション デプロイを選択します。

サービス テーブルの上のツールバーで、[アップグレード (Upgrade)] (⬆ アイコン) が有効になります。

- 3 [アップグレード (Upgrade)] (📌) アイコンをクリックして、ユーザー インターフェイスのプロンプトに従います。

**Confirm Upgrade**

Upgrade Guest Introspection service

Datastore \* ds-site-a-nfs01 ▼

Network \* vds-site-a\_Management... ▼

IP assignment \* GI Pool ▼

**Specify schedule:**

☒ Upgrade now

☐ Schedule the upgrade  6:29 PM ▼

OK Cancel

ゲスト イントロスペクションをアップグレードすると、インストールの状態は **成功しました** になり、サービスのステータスは **接続中** になります。ゲスト イントロスペクション サービスの仮想マシンは、vCenter Server インベントリに表示されます。

#### 次のステップ

特定のクラスタのゲスト イントロスペクションをアップグレードした後、パートナー ソリューションをアップグレードできます。パートナー ソリューションが有効な場合、パートナーが提供するアップグレードのドキュメントを参照してください。パートナー ソリューションをアップグレードしない場合でも、保護が維持されます。

## 直接アップグレードをサポートしない NSX サービス

VMware Partner Security Virtual Appliances などのいくつかの NSX サービスは、直接アップグレードをサポートしません。この場合、サービスをアンインストールしてから、再度インストールを行う必要があります。

### VMware Partner Security Virtual Appliances

VMware パートナーのセキュリティ仮想アプライアンスがアップグレード可能かどうかは、パートナーが提供するドキュメントでご確認してください。

### NSX Data Security

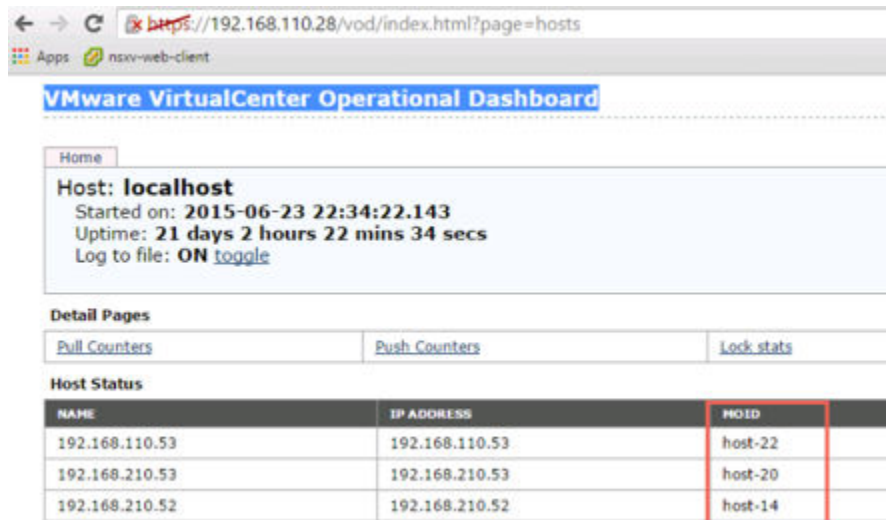
NSX Data Security をアンインストールした後に NSX をアップグレードし、NSX のアップグレードが完了してから NSX Data Security を再インストールすることをお勧めします。NSX Data Security をアンインストールせずに NSX をアップグレードした場合は、REST API 呼び出しを使用して Data Security をアンインストールする必要があります。

次の API 呼び出しを実行します。

**DELETE** <https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds>

host-id は、ESXi ホストの MOID です。MOID を取得するには、VMware VirtualCenter Operational Dashboard (<https://<vcenter-ip>/vod/index.html?page=hosts>) を開きます。





vCenter Server 192.168.110.28 上にある、MOID が "host-22" の ESXi ホストの場合、API 呼び出しは次のような形式になります。

**DELETE** <https://192.168.110.28/api/1.0/vshield/host-22/vsds>

すべての ESXi ホストで API 呼び出しを実行するようにします。

Data Security のアンインストール後に、新しいバージョンをインストールできます。[「NSX Data Security のインストール」](#) を参照してください。

## NSX SSL VPN

NSX 6.2 以降、SSL VPN ゲートウェイで許容されるのは、TLS プロトコルのみにになります。しかし、NSX 6.2 以降へのアップグレード後、ユーザーが新規で作成するクライアントでは、接続を確立する間、自動的に TLS プロトコルが使用されます。また、NSX 6.2.3 以降では、TLS 1.0 は廃止されています。

プロトコルが変更されると、NSX 6.0.x クライアントが NSX 6.2 以降のゲートウェイへ接続する際、SSL ハンドシェイクの段階で接続の確立に失敗します。

NSX 6.0.x からのアップグレード後は、古い SSL VPN クライアントをアンインストールし、NSX 6.2.x バージョンの SSL VPN クライアントをインストールしてください。『NSX 管理ガイド』の「リモート サイトへの SSL クライアントのインストール」を参照してください。

## NSX L2 VPN

バージョン 5.5.x または 6.0.x の NSX Edge に L2 VPN がインストールされている場合、NSX Edge はアップグレードできません。NSX Edge をアップグレードする前に、すべての L2 VPN の設定を削除する必要があります。

## アップグレード後のチェックリスト

アップグレードが完了したら、次の手順を実行します。

### 手順

- 1 アップグレード後に NSX Manager の現在のバックアップを作成します。



## 2 VIB がホストにインストールされていることを確認します。

NSX によって、これらの VIB がインストールされます。

```
esxcli software vib get --vibname esx-vxlan  
esxcli software vib get --vibname esx-vsip
```

ゲスト イントロスペクションがインストールされている場合、この VIB がホストに存在していることも確認します。

```
esxcli software vib get --vibname epsec-mux
```

## 3 ホストのメッセージバスを再同期します。VMware は、アップグレード後に再同期することをすべてのカスタマにお勧めしています。

次の API コールを使用して、各ホストで再同期を実行します。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>  
HTTP Method : POST
```

**Headers:**

```
Authorization : base64encoded value of username password  
Accept : application/xml  
Content-Type : application/xml
```

# NSX 環境での vSphere のアップグレード

# 3

NSX 環境で vSphere をアップグレードする場合、NSX と vSphere のバージョンに互換性があることを確認する必要があります。

VMware 製品の相互運用性マトリックスで、該当する NSX インストール環境と互換性のある vSphere と ESXi のバージョンを確認してください。 [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php) を参照してください。

vSphere のアップグレードの詳細な手順については、『vSphere アップグレード ガイド』と『VMware vSphere Update Manager のインストールと管理ガイド』を含む、該当するバージョンの vSphere のドキュメントを参照してください。

ホストで ESXi をアップグレードする場合、新しいバージョンの ESXi との互換性を確保するため、ホストに新しい NSX VIB をインストールする必要があります。NSX VIB がアップデートされるまで、アップグレードされたホスト上で NSX のワークロードを実行できません。

この章には、次のトピックが含まれています。

- [NSX 環境での ESXi のアップグレード](#)
- [ESXi アップグレード後のゲスト イントロスペクションの再デプロイ](#)

## NSX 環境での ESXi のアップグレード

使用する NSX VIB は、ホストにインストールされている ESXi のバージョンによって異なります。ESXi をアップグレードする場合、新しい ESXi バージョンに対応した適切な NSX VIB を新しくインストールする必要があります。

---

**重要:** アップグレード プロセスでは、ホストをメンテナンス モードにしておく必要があります。これは、アップグレードが完了するまで、DRS または vMotion によるホストへの仮想マシンの移行を防止するためです。

---

### 前提条件

- VMware 製品の相互運用性マトリックスで、該当する NSX インストール環境と互換性のある vSphere と ESXi のバージョンを確認してください。  
[http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php) を参照してください。
- vSphere のアップグレードの詳細な手順については、『vSphere アップグレード ガイド』と『VMware vSphere Update Manager のインストールと管理ガイド』を含む、該当するバージョンの vSphere のドキュメントをお読みください。

- Platform Services Controller および vCenter Server システムが新しい vSphere バージョンにアップグレードされていることを確認します。
- すべてのホストの完全修飾ドメイン名 (FQDN) を解決できることを確認します。
- DRS が無効な場合は、アップグレードを開始する前に、手動で仮想マシンのパワーオフまたは vMotion を実行します。
- DRS が有効な場合は、実行中の仮想マシンは、ホスト クラスタのアップグレード中に自動的に移動されます。アップグレードを開始する前に、環境内で DRS が機能できることを確認します。
  - ホスト クラスタで DRS が有効であることを確認します。
  - vMotion が正しく機能することを確認します。
  - ホストと vCenter Server の接続状態を確認します。
  - 各ホスト クラスタに、少なくとも 3 台の ESXi ホストがあることを確認します。1 台または 2 台のホストを持つホスト クラスタでは、NSX のアップグレード中に、DRS のアドミSSION コントロールの問題が発生することがあります。NSX を正しくアップグレードするため、各ホスト クラスタに少なくとも 3 台のホストを含めることをお勧めします。クラスタに含まれるホストが 3 台より少ない場合は、ホストを手動で退避させることが推奨されます。
  - ホストが 2 ～ 3 台の小規模クラスタで、特定の仮想マシンを個別のホストに配置することを指示する非アフィニティ ルールを作成している場合、これらのルールにより、アップグレード中の DRS による仮想マシンの移行が阻止される場合があります。クラスタにホストを追加するか、アップグレード中に非アフィニティ ルールを無効にして、アップグレードの完了後に非アフィニティ ルールを再度有効にします。非アフィニティ ルールを無効にするには、[ホストおよびクラスタ (Hosts and Clusters)] - [Cluster] - [管理 (Manage)] - [設定 (Settings)] - [仮想マシン/ホスト ルール (VM/Host Rules)] の順に移動します。ルールを編集して [ルールの有効化 (Enable rule)] の選択を解除します。

## 手順

- ◆ アップグレードが必要なホストごとに、次の手順を行います。
  - a ホストをメンテナンス モードに切り替えます。

クラスタで DRS が有効になっている場合、DRS は仮想マシンをその他のホストに移行しようとします。何らかの理由で DRS が失敗した場合、仮想マシンを手動で移行してから、ホストをメンテナンス モードに切り替える必要があります。
  - b ホスト上の ESXi をアップグレードします。

ESXi のアップグレードが完了したら、ホストを再起動します。
  - c 再起動後、ホストのステータスが **[未接続]** の場合はホストを接続します。ホストを右クリックし、[接続 (Connection)] - [接続 (Connect)] の順に選択します。
  - d [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [ホストの準備 (Host Preparation)] の順に移動します。
  - e ESXi をアップグレードしたホストを選択します。[インストール ステータス] に [準備ができていません (Not Ready)] と表示されています。

f [アクション (Actions)] - [解決 (Resolve)] の順にクリックして NSX VIB のアップデートを完了します。

NSX VIB がホスト上でアップデートされ、ホストが再起動します。

g ホストの再起動が完了したら、メンテナンス モードを終了します。

VIB が更新されていることを確認するには、ホストのコマンドラインにアクセスし、**esxcli software vib list | grep esx-v** コマンドを発行します。VIB バージョンの最初の部分に、対応する ESXi のバージョンが表示されます。たとえば、ESXi 5.5 から ESXi 6.0 にアップグレードする前は、次のようになります。

```
[root@host-1:~] esxcli software vib list | grep esx-v
esx-vsip      5.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
esx-vxlan     5.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
```

ESXi 6.0 にアップグレードした後は、次のようになります。

```
[root@host-1:~] esxcli software vib list | grep esx-v
esx-vsip      6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
esx-vxlan     6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
```

## ESXi アップグレード後のゲスト イントロスペクションの再デプロイ

ゲスト イントロスペクションがデプロイされているクラスタで ESXi をアップグレードする場合は、[サービス デプロイ] タブでゲスト イントロスペクションの再デプロイが必要かどうかを確認することをお勧めします。

**重要:** ゲスト イントロスペクションの再デプロイ前に、ESXi のアップグレードおよび関連する NSX VIB のアップグレードを完了しておく必要があります。

### 前提条件

- ESXi のアップグレードを完了します。
- ESXi のアップグレード後に NSX VIB (ホストの準備) のアップグレードを完了します。

### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [[サービス デプロイ] (Service Deployments)] タブをクリックします。
- 4 [インストール ステータス] 列に **[成功しました]** と表示されている場合は、再デプロイは不要です。
- 5 [インストール ステータス] 列に **[準備ができていません]** と表示されている場合は、**[準備ができていません (Not Ready)]** リンクをクリックします。**[すべてを解決 (Resolve all)]** をクリックしてゲスト イントロスペクションを再デプロイします。