

# NSX アップグレードガイド

Update 10

変更日：2018 年 3 月 29 日

VMware NSX Data Center for vSphere 6.3



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 – 2018 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	7
1 NSX のアップグレード	10
NSX のアップグレードの準備	10
NSX 6.3.x へのアップグレード	27
Cross-vCenter NSX 環境での NSX 6.3.x へのアップグレード	41
2 NSX 環境での vSphere のアップグレード	60
NSX 環境での ESXi 6.0 へのアップグレード	61
NSX 環境での ESXi 6.5 へのアップグレード	63
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	67

# NSX アップグレード ガイド

『NSX アップグレード ガイド』では、NSX Manager ユーザー インターフェイスと vSphere Web Client を使用して、VMware NSX<sup>®</sup> for vSphere<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 Server 環境で NSX をアップグレード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。本書は、VMware ESXi、vCenter Server、vSphere Web Client を含む VMware vSphere についての知識があることを前提としています。

## VMware の技術ドキュメントの用語集

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

## 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 ([http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php#interop&93](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&93)) [相互運用性 (Interoperability)] タブを参照してください。

## アップグレード パスのマトリックス

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。VMware 製品の相互運用性マトリックス ([http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php#upgrade&solution=93](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#upgrade&solution=93)) [アップグレード パス (Upgrade Path)] タブを参照してください。

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

## ハードウェア

次の表は、NSX アプライアンスのハードウェア要件です。

表 1. アプライアンスのハードウェア要件

アプライアンス	メモリ	vCPU	ディスク容量
NSX Manager	16 GB (大規模な NSX 環境の場合は 24 GB)	4 (大規模な NSX 環境の場合は 8)	60 GB
NSX Controller	4 GB	4	28 GB
NSX Edge	<ul style="list-style-type: none"> <li>■ [Compact] : 512 MB</li> <li>■ [Large] : 1 GB</li> <li>■ [Quad Large] : 2 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]、[Large]、[Quad Large] : 584 MB のディスク 1 台 + 512 MB のディスク 1 台</li> <li>■ [XLarge] : 584 MB のディスク 1 台 + 2 GB のディスク 1 台 + 256 MB のディスク 1 台</li> </ul>
ゲスト イントロスペクション	2 GB	2	5 GB (プロビジョニング後の容量は 6.26 GB)

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

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

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

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

## ネットワークの遅延

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

表 2. コンポーネント間のネットワーク遅延の最大値

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

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

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

コンポーネント	バージョン
NSX Manager	6.2 以降
NSX Controller	6.2 以降
vCenter Server	6.0 以降
ESXi	<ul style="list-style-type: none"> <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 ネットワークとセキュリティ (<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>) を参照してください。

## クライアントとユーザー アクセス

NSX 環境を管理するには、次が必要です。

- 正引き/逆引きの名前解決。これは、vSphere インベントリに ESXi ホストを名前を追加した場合に必要です。この機能がないと、NSX Manager は IP アドレスを解決できません。
- 仮想マシンを追加、パワーオンの権限
- 仮想マシンのファイルを保存するデータストアへのアクセス、そのデータストアにファイルをコピーするためのアカウント権限
- NSX Manager ユーザー インターフェイスにアクセスするには、Web ブラウザで Cookie を有効にする必要があります。
- NSX Manager と ESXi ホスト、vCenter Server、デプロイする NSX アプライアンスの間で、ポート 443 を開く必要があります。このポートは、ESXi ホストから OVF ファイルをダウンロードして展開するために必要です。
- 使用している vSphere Web Client のバージョンでサポートされている Web ブラウザは次のとおりです。詳細については、『vCenter Server およびホスト管理』ドキュメントの「vSphere Web Client の使用」を参照してください。

## NSX 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。

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

表 3. NSX for vSphere で必要になるポートとプロトコル

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
クライアント PC	NSX Manager	443	TCP	NSX Manager 管理インターフェイス	いいえ	はい	PAM 認証
クライアント PC	NSX Manager	443	TCP	NSX Manager VIB アクセス	いいえ	いいえ	PAM 認証
ESXi ホスト	vCenter Server	443	TCP	ESXi ホストの準備	いいえ	いいえ	
vCenter Server	ESXi ホスト	443	TCP	ESXi ホストの準備	いいえ	いいえ	
ESXi ホスト	NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	RabbitMQ ユーザー/パスワード
ESXi ホスト	NSX Controller	1234	TCP	ユーザー ワールド エージェント接続	いいえ	はい	
NSX Controller	NSX Controller	2878、 2888、 3888	TCP	コントローラ クラスタ - 状態同期	いいえ	はい	IPsec

表 3. NSX for vSphere で必要になるポートとプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
NSX Controller	NSX Controller	7777	TCP	内部コントローラ RPC ポート	いいえ	はい	IPsec
NSX Controller	NSX Controller	30865	TCP	コントローラ クラスター - 状態同期	いいえ	はい	IPsec
NSX Manager	NSX Controller	443	TCP	コントローラと Manager の通信	いいえ	はい	ユーザー/パスワード
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	いいえ	はい	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	いいえ	はい	
NSX Manager	ESXi ホスト	443	TCP	管理とプロビジョニング 接続	いいえ	はい	
NSX Manager	ESXi ホスト	902	TCP	管理とプロビジョニング 接続	いいえ	はい	
NSX Manager	DNS サーバ	53	TCP	DNS クライアント接続	いいえ	いいえ	
NSX Manager	DNS サーバ	53	UDP	DNS クライアント接続	いいえ	いいえ	
NSX Manager	Syslog サーバ	514	TCP	Syslog 接続	いいえ	いいえ	
NSX Manager	Syslog サーバ	514	UDP	Syslog 接続	いいえ	いいえ	
NSX Manager	NTP タイム サーバ	123	TCP	NTP クライアント接続	いいえ	はい	
NSX Manager	NTP タイム サーバ	123	UDP	NTP クライアント接続	いいえ	はい	
vCenter Server	NSX Manager	80	TCP	ホストの準備	いいえ	はい	
REST Client	NSX Manager	443	TCP	NSX Manager REST API	いいえ	はい	ユーザー/パスワード
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (NSX 6.2.3 より 前のデフォ ルト) または 4789 (NSX 6.2.3 以降の 新規インス トールのデ フォルト)	UDP	VTEP 間の転送ネット ワークのカプセル化	いいえ	はい	
ESXi ホスト	ESXi ホスト	6999	UDP	VLAN LIF 上の ARP	いいえ	はい	
ESXi ホスト	NSX Manager	8301, 8302	UDP	分散仮想スイッチ同期	いいえ	はい	
NSX Manager	ESXi ホスト	8301, 8302	UDP	分散仮想スイッチ同期	いいえ	はい	



表 3. NSX for vSphere で必要になるポートとプロトコル (続き)

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
ゲスト イントロ ベクション 仮想マ シン	NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	RabbitMQ ユー ザー/パスワード
プライマリ NSX Manager	セカンダリ NSX Manager	443	TCP	Cross-vCenter NSX ユニバーサル同期サー ビス	いいえ	はい	
プライマリ NSX Manager	vCenter Server	443	TCP	vSphere API	いいえ	はい	
セカンダリ NSX Manager	vCenter Server	443	TCP	vSphere API	いいえ	はい	
プライマリ NSX Manager	NSX ユニバーサル コントローラ クラ スタ	443	TCP	NSX Controller REST API	いいえ	はい	ユーザー/パスワード
セカンダリ NSX Manager	NSX ユニバーサル コントローラ クラ スタ	443	TCP	NSX Controller REST API	いいえ	はい	ユーザー/パスワード
ESXi ホスト	NSX ユニバーサル コントローラ クラ スタ	1234	TCP	NSX 制御プレーン プロ トコル	いいえ	はい	
ESXi ホスト	プライマリ NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	RabbitMQ ユー ザー/パスワード
ESXi ホスト	セカンダリ NSX Manager	5671	TCP	RabbitMQ	いいえ	はい	RabbitMQ ユー ザー/パスワード

# NSX のアップグレード

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 6.3.x へのアップグレード
- Cross-vCenter NSX 環境での NSX 6.3.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対して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 のアップグレード前にアンインストールしておきます。Data Security は、NSX 6.3.x でサポートされていません。[「NSX Data Security のアンインストール」](#)を参照してください。

- 4 ハードウェア ゲートウェイ（ハードウェア VTEP）が環境にインストールされている場合、NSX 6.3.0 および 6.3.1 へのアップグレードはブロックされます。アップグレードの方法については、VMware サポートにお問い合わせください。詳細については <https://kb.vmware.com/kb/2148511> を参照してください。NSX 6.3.2 へのアップグレードは可能です。
- 5 NSX 5.5 以前の NSX Edge アプライアンスの場合、NSX 6.x にアップグレードしてから、NSX 6.3.x にアップグレードします。
- 6 NSX 6.3.3 にアップグレードする場合、NSX Controller クラスタに 3 台のコントローラ ノードが含まれている必要があります。3 台より少ない場合は、アップグレードを開始する前にノードを追加する必要があります。コントローラ ノードの追加方法については、『NSX インストール ガイド』で「NSX Controller クラスタのデプロイ」を参照してください。
- 7 同じメンテナンス期間でアップグレードする NSX Manager を決定します。
  - Cross-vCenter NSX 環境の場合、同じメンテナンス期間内にプライマリ NSX Manager とすべてのセカンダリ NSX Manager を同じ NSX バージョンにアップグレードする必要があります。
  - 同じ SSO サーバを使用する vCenter Server システムに複数の NSX Manager が接続している場合、NSX Manager のバージョンのすべての組み合わせはサポートされません。サポートされる構成がメンテナンス期間の最後に残るように、NSX Manager のアップグレードをプランニングする必要があります。
    - 同じバージョンの NSX を使用している NSX Manager はすべてサポートされます。
    - 異なるバージョンの NSX を使用する NSX Manager がサポートされます。これは、1 つ以上の NSX Manager に NSX 6.4.0 以降がインストールされ、他のすべての NSX Manager に NSX 6.3.3 以降がインストールされている場合に適用されます。
- 8 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。
- 9 テクニカル サポート バンドルを作成します。
- 10 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。
- 11 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。
- 12 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。
- 13 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。
- 14 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 モデルが追加されました。

有効なサポート契約を締結しており、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、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 のライセンス エディションと関連機能の詳細については、<https://kb.vmware.com/kb/2145269> を参照してください。

## NSX アップグレードの運用上の影響

NSX のアップグレードに時間がかかる場合があります。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 コンポーネントの状況を理解することが重要です。

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 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で新しい機能が導入される場合、すべてのホストがアップグレードされるまで、これらの機能は使用できません。
- 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 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。ただし、分散ファイアウォールが有効になっている場合、異なる NSX バージョンを使用しているクラスタ間での仮想マシンの移行に制限があります。
  - 新しいバージョンの NSX を使用しているクラスタから古いバージョンの NSX を使用しているクラスタに仮想マシンを移行すると、仮想マシンのネットワーク接続が失われる可能性があります。
  - 古いバージョンの NSX を使用しているクラスタから、新しいバージョンの NSX を使用するクラスタへの仮想マシンの移行は、サポートされています。
- 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。

## 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。

## FIPS モードと NSX アップグレードについて

NSX 6.3.0 から、FIPS モードを有効にできます。FIPS モードにより、FIPS に準拠した暗号スイートが有効になります。



**警告：** NSX のバージョンを NSX 6.3.0 より前から NSX 6.3.0 以降にアップグレードする場合、アップグレードを完了してから FIPS モードを有効にしてください。アップグレードが完了する前に FIPS モードを有効にすると、アップグレード済みのコンポーネントとアップグレードされていないコンポーネント間の通信が中断します。

## NSX のアップグレードと FIPS のステータス

表 1-1. NSX 6.3.x にアップグレードした後の NSX コンポーネントにおける FIPS モードのステータス

NSX コンポーネント	FIPS モードのステータス
NSX Manager	NSX 6.3.x にアップグレードすると、NSX Manager アプライアンスで FIPS モードが利用可能になりますが、無効な状態です。すべての NSX コンポーネントのアップグレードが完了し、すべての NSX Edge アプライアンスで FIPS を有効にするまで、NSX Manager アプライアンスの FIPS モードは有効にしないでください。
NSX Controller クラスタ	NSX 6.3.x にアップグレードした後、NSX Controller クラスタは FIPS 対応となります。これを変更することはできません。
NSX ホスト クラスタ	NSX 6.3.x にアップグレードした後、NSX ホスト クラスタは FIPS 対応となります。これを変更することはできません。

表 1-1. NSX 6.3.x にアップグレードした後の NSX コンポーネントにおける FIPS モードのステータス (続き)

NSX コンポーネント	FIPS モードのステータス
NSX Edge	NSX 6.3.x にアップグレードすると、NSX Edge アプライアンスで FIPS モードが利用可能になりますが、無効な状態です。FIPS は、すべての NSX コンポーネントのアップグレードが完了するまで有効にしないでください。
ゲスト イントロスペクション サービス仮想マシン	NSX 6.3.x にアップグレードした後、ゲスト イントロスペクション サービス仮想マシンは FIPS 対応となります。これを変更することはできません。

## FIPS の有効化

NSX 6.3.x にアップグレードし、FIPS を有効にする場合、次の手順を実行する必要があります。

- 1 パートナー ソリューションが FIPS モード認定であることを確認します。  
<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security> にある『VMware 互換性ガイド』を参照してください。情報については、パートナーのドキュメントを確認してください。
- 2 NSX Manager を NSX 6.3.0 以降にアップグレードします。
- 3 NSX Controller クラスタを NSX 6.3.0 以降にアップグレードします。
- 4 NSX ワークロードを実行しているすべてのホスト クラスタを NSX 6.3.0 以降にアップグレードします。
- 5 すべての NSX Edge アプライアンスを NSX 6.3.0 以降にアップグレードします。
- 6 すべてのホスト クラスタにインストールされているゲスト イントロスペクションを NSX 6.3.0 以降にアップグレードします。
- 7 FIPS モードを NSX Edge アプライアンスで有効にします。『NSX 管理ガイド』の「NSX Edge での FIPS モードの変更」を参照してください。
- 8 FIPS モードを NSX Manager アプライアンスで有効にします。『NSX 管理ガイド』の「NSX Manager での FIPS モードと TLS 設定の変更」を参照してください。

## 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 は NSX 6.2.3 で廃止され、NSX 6.3.0 以降で削除されました。NSX 6.3.x にアップグレードする前に NSX Data Security をアンインストールする必要があります。

### 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。
- 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 Server 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 のバックアップとリストア

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。

### 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。

#### 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 (Backups & Restore)] 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 (Change)] 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 バックアップ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 (Transfer Protocol)] 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 (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。

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 (Filename Prefix)] 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。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。

---

**注:** バックアップディレクトリ内のファイル数は、100 個以下にする必要があります。ディレクトリ内のファイルの数が制限を超えると、警告メッセージが表示されます。

---

- 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 (Backup)] をクリックします。

新しいファイルが [バックアップ履歴 (Backup History)] 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 (Change)] をクリックします。

- a [バックアップ頻度 (Backup Frequency)] ドロップダウン メニューで、[時間単位 (Hourly)]、[日単位 (Daily)]、または [週単位 (Weekly)] 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 (Schedule)] 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 (Change)] 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、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 アドレス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をメモします。

### 手順

- 1 既存の NSX Manager アプライアンスのすべての設定をメモします。また、FTP サーバの設定も書き留めておきます。
- 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 FTP サーバ設定を追加します。

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)]、[ファイル名のプリフィックス (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。

[バックアップ履歴 (Backup History)] セクションにバックアップ フォルダが表示されます。

---

**注:** [バックアップ履歴 (Backup History)] セクションにバックアップ フォルダが表示されない場合は、FTP サーバ設定を確認します。FTP サーバに接続し、バックアップ フォルダを表示できるかどうかを確認してください。

---

- 6 [バックアップ履歴 (Backup History)] セクションで、リストアするバックアップ フォルダを選択し、[リストア (Restore)] をクリックします。

NSX Manager データのリストアが開始されます。

NSX の設定が NSX Manager にリストアされます。




**警告:** NSX Manager のバックアップをリストアした後、NSX Edge アプライアンスと論理スイッチを正常に動作させるため、追加のアクションが必要になる場合があります。[「NSX Edge の復旧」](#) および [「論理スイッチの非同期エラーの解決」](#) を参照してください。

---

## NSX Edge の復旧

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 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。

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 (Redeploy NSX Edge) (  ) 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 アプライアンス仮想マシンを再作成できます。『NSX 管理ガイド』の「NSX Edge の再デプロイ」を参照してください。



**警告:** NSX Manager のバックアップをリストアした後、NSX Edge アプライアンスを正常に動作させるため、追加のアクションが必要になる場合があります。

- 前回のバックアップ後に作成された Edge アプライアンスはリストア中に削除されません。仮想マシンは手動で削除する必要があります。
- 再デプロイしていない場合、前回のバックアップ後に削除された Edge アプライアンスはリストアされません。
- バックアップのリストア時に、バックアップに NSX Edge アプライアンスの設定場所と現在の場所が保存されていない場合、再デプロイ、高可用性の有効化または無効化などの操作が失敗します。アプライアンスの設定を編集し、有効な場所情報を指定する必要があります。PUT `/api/4.0/edges/{edgeId}/appliances` を使用して、アプライアンスの場所の設定を編集します。必要に応じて、<resourcePoolId>、<datastoreId>、<hostId>、<vmFolderId> を編集します。『NSX API ガイド』の「NSX Edge アプライアンスの設定の使用」を参照してください。

前回の NSX Manager のバックアップ後に次のいずれかの変更が行われると、リストアされた NSX Manager の設定と NSX Edge アプライアンスの現在の設定に差異が発生します。アプライアンスに対する変更を元に戻し、NSX Edge を正常に動作させるには、NSX Edge を[強制的に同期 (Force Sync)]する必要があります。『NSX 管理ガイド』の「NSX Edge と NSX Manager の強制同期」を参照してください。

- NSX Edge ファイアウォールの preRules に対して、分散ファイアウォール経由で行われた変更
- オブジェクト メンバーシップのグループ化に対する変更

前回の NSX Manager のバックアップ後に次のいずれかの変更が行われると、リストアされた NSX Manager の設定と NSX Edge アプライアンスの現在の設定に差異が発生します。アプライアンスに対する変更を元に戻し、NSX Edge を正常に動作させるには、NSX Edge を[再デプロイ (Redeploy)]する必要があります。『NSX 管理ガイド』の「NSX Edge の再デプロイ」を参照してください。

- Edge アプライアンスの設定に対する変更：
  - 高可用性の有効化または無効化
  - アプライアンスの状態の変更 (デプロイ済みからデプロイ解除済み)
  - アプライアンスの状態の変更 (デプロイ解除済みからデプロイ済み)
  - リソースの予約設定の変更
- Edge アプライアンスの vNIC の設定の変更：
  - vNIC の追加、削除または切断
  - ポート グループ
  - トランク ポート
  - フェンス パラメータ
  - シェーピング ポリシー



## 論理スイッチの非同期エラーの解決

NSX Manager のバックアップの作成からリストアまでの間に論理スイッチの変更が発生すると、論理スイッチが同期なし状態をレポートする場合があります。

### 手順

- 1 vSphere Web Client にログインします。
- 2 [ネットワークとセキュリティ (Networking & Security)] - [論理スイッチ (Logical Switches)] の順に移動します。
- 3 [同期なし (Out of sync)] リンクが表示されている場合には、このリンクをクリックします。
- 4 [解決 (Resolve)] をクリックし、不足しているバックアップ ポート グループを論理スイッチに再作成します。

## vSphere Distributed Switch のバックアップ

vSphere Distributed Switch 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。

vSphere Distributed Switch 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。

VXLAN のクラスタを準備する前に、vSphere Distributed Switch の設定をエクスポートすることをおすすめします。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-vcserver-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>

## アップグレードで作成された NSX Manager のバックアップの管理

NSX Manager を NSX 6.3.6 にアップグレードすると、アップグレード中にバックアップが作成され、ローカルに保存されます。このバックアップをリストアする場合は、VMware サポートにお問い合わせください。この自動バックアップは、定期的なバックアップが失敗した場合のフェイルセーフとなります。

NSX Manager のアップグレードに成功すると、特権（有効）モードで使用できる新しいコマンドが追加されます。これらのコマンドは、バックアップ ファイルの管理に使用します。これらのコマンドを実行すると、バックアップ ファイルの一覧表示、コピー、削除を行うことができます。

バックアップ ファイルを削除しない場合、次のアップグレードまでバックアップ ファイルは同じ場所に残ります。次回アップグレードが開始されると、バックアップ ファイルが削除され、新しいバックアップが作成されます。

## show backup

バックアップ ファイルを一覧表示します。

```
nsxmgr-01a.corp.local# show backup
total 3040
-rw-r--r-- 1 root root 3102752 Mar 23 01:12 backup_file
-rw-r--r-- 1 root root      230 Mar 23 01:12 backup_metadata
```

## export backup

バックアップ ファイルを別の場所にコピーします。

```
nsxmgr-01a.corp.local# export backup scp root@backup-server:/backups
Exporting...
Password:
backup_file                100% 3030KB   19.8MB/s   00:00
backup_metadata            100%   230     27.3KB/s   00:00
nsxmgr-01a.corp.local#
```

## delete backup

バックアップ ファイルを削除します。バックアップ ファイルは、不要になった場合にのみ削除してください。

```
nsxmgr-01a.corp.local# delete backup
Do you want to delete the backup files (y|N)y
nsxmgr-01a.corp.local#
```

## 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の変更されることがあります。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 6.3.x へのアップグレード

NSX 6.3.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 (注を参照)
- 5 ゲスト イントロスペクション

---

**注:** 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。ただし、分散論理ルーターのアップグレードは、NSX Controller クラスタおよびホスト クラスタのアップグレードが完了するまで実行できません。アップグレードの依存関係の詳細については、「[NSX アップグレードの運用上の影響](#)」を参照してください。

---

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。

## 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 のカスタマー エクスペリエンス向上プログラム (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 のカスタマー エクスペリエンス向上プログラムのセクションを参照してください。

NSX 6.3.0 以降からアップグレードする場合、アップグレード バンドルのアップロードとアップグレードの開始は別々に実行できます。以前にアップロードされたアップグレード バンドルからアップグレードを開始するには、[ホーム (Home)] - [アップグレード (Upgrade)] の順に移動し、[アップグレードを開始 (Begin Upgrade)] をクリックします。

NSX Manager を NSX 6.3.6 にアップグレードすると、アップグレード中にバックアップが自動的に作成され、ローカルに保存されます。これらのバックアップ ファイルの管理方法については、「[アップグレードで作成された NSX Manager のバックアップの管理](#)」を参照してください。

- アップグレードで自動バックアップの作成に失敗すると、アップグレードが停止します。サポートが必要な場合は、VMware サポートにお問い合わせください。
- 自動バックアップは、定期的なバックアップに失敗した場合のフェイルセーフとなります。
  - アップグレードの前に、NSX Manager の定期的なバックアップを必ず行ってください。詳細については「[NSX Manager データのバックアップ](#)」を参照してください。このバックアップは、VMware サポートを利用せずにリストアできます。
  - 自動バックアップのリストアが必要な場合は、VMware サポートにお問い合わせください。

### 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** を実行して、ファイル システムの使用量を表示します。
  - b 使用率が 100% の場合は、特権（有効）モードに切り替えて **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。
- アップグレードの前に、NSX Manager 仮想アプライアンスの予約済みメモリが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。
- 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。Data Security は、NSX 6.3.x から削除されています。
- 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。
- 同じメンテナンス期間内に、Cross-vCenter NSX 環境のすべての NSX Manager をアップグレードする必要があります。
- 同じメンテナンス期間でアップグレードする NSX Manager を決定します。
  - Cross-vCenter NSX 環境の場合、同じメンテナンス期間内にプライマリ NSX Manager とすべてのセカンダリ NSX Manager を同じ NSX バージョンにアップグレードする必要があります。
  - 同じ SSO サーバを使用する vCenter Server システムに複数の NSX Manager が接続している場合、NSX Manager のバージョンのすべての組み合わせはサポートされません。サポートされる構成がメンテナンス期間の最後に残るように、NSX Manager のアップグレードをプランニングする必要があります。
    - 同じバージョンの NSX を使用している NSX Manager はすべてサポートされます。
    - 異なるバージョンの NSX を使用する NSX Manager がサポートされます。これは、1 つ以上の NSX Manager に NSX 6.4.0 以降がインストールされ、他のすべての NSX Manager に NSX 6.3.3 以降がインストールされている場合に適用されます。

## 手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 ホーム ページで、[アップグレード (Upgrade)] をクリックします。
- 3 [アップグレード (Upgrade)] をクリックし、[ファイルを選択 (Choose File)] をクリックして **VMware-NSX-Manager-upgrade-bundle-<releaseNumber>-<NSXbuildNumber>.tar.gz** ファイルを選択します。[続行 (Continue)] 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 アップグレードを後で開始する場合は、[アップグレード] ダイアログ ボックスで [閉じる (Close)] をクリックします。  
アップグレードを開始する準備ができたなら、[ホーム (Home)] - [アップグレード (Upgrade)] の順に移動し、[アップグレードを開始 (Begin Upgrade)] をクリックします。
- 5 [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選択し、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加するかどうかを選択します。[アップグレード (Upgrade)] 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。

---

**注:** [アップグレード] ダイアログ ボックスに、自動バックアップが行われたことを示すメッセージが表示されます。

---

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。

- 6 NSX Manager 仮想アプライアンスに再びログインし、ホーム ページから [アップグレード (Upgrade)] をクリックします。アップグレードの状態が [完了 (Complete)] になっていることと、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

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、メンテナンス時間枠内に実施することをお勧めします。

NSX Controller 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 台ずつ実行されます。アップグレードの進行中は、[アップグレードを利用可能 (Upgrade Available)] 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。

**重要:** NSX 6.3.3 では、NSX Controller の基盤となるオペレーティング システムが変わります。NSX 6.3.2 以前から NSX 6.3.3 以降にアップグレードする場合、インプレース アップグレードは実行されません。既存のコントローラ が 1 度に 1 つずつ削除され、同じ IP アドレスを使用して新しい Photon OS ベースのコントローラが展開されます。

コントローラを削除すると、関連する DRS の非アフィニティ ルールも削除されます。新しいコントローラ仮想マシンが同じホストに配置されないように、vCenter Server で新しい非アフィニティ ルールを作成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 (Hosts and Clusters)] ビューで、コントローラを右クリックし、[パワー (Power)] > [リセット (Reset)] の順に選択します。
- 有効な NSX Controller 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 control-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 Controller 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。
- NSX 6.3.3 にアップグレードする場合、NSX Controller クラスタに 3 台のコントローラ ノードが含まれている必要があります。3 台より少ない場合は、アップグレードを開始する前にノードを追加する必要があります。コントローラ ノードの追加方法については、『NSX インストール ガイド』で「NSX Controller クラスタのデプロイ」を参照してください。

#### 手順

- ◆ [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] の順に移動し、[管理 (Management)] 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 (Controller Cluster Status)] 列で [アップグレードを利用可能 (Upgrade Available)] をクリックします。

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 (Controller Cluster Status)] 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 (Downloading upgrade file)] 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 (In progress)] 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 (Complete)] と表示され、この列は表示されなくなります。
- NSX Controller ノード セクションの [ステータス (Status)] 列に、それぞれのコントローラのステータスが表示されます。アップグレード前の場合、元の NSX のバージョンに応じて [接続済み (Connected)] または [標準 (Normal)] 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 (Disconnected)] 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 [接続済み (Connected)] になります。
- NSX Controller ノード セクションの [アップグレード ステータス (Upgrade Status)] 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 (Downloading upgrade file)] と表示され、次に [アップグレードが進行中です (Upgrade in progress)] となり、その後 [再起動中です (Rebooting)] 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 (Upgraded)] と表示されます。

---

**注:** NSX 6.3.2 以前から NSX 6.3.3 以降にアップデートする場合、ステータスが [アップグレード ファイルをダウンロード中です (Downloading upgrade file)] ではなく、[アップグレードを待機しています (Queued For Upgrade)] になります。

---

アップグレードが完了すると、NSX Controller 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 (Software Version)] 列に、[6.3.]<buildNumber> と表示されます。[show control-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 Controller 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 (Upgrade Status)] 列に [失敗 (Failed)] 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 (Upgrade Available)] 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 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。別のコントローラを作成する手順については、『NSX トラブルシューティング ガイド』の「NSX Controller の再デプロイ」を参照してください。

#### 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 のアップグレード後に、環境内の適切なクラスタをアップデートできます。

ホスト クラスタをアップグレードすると、NSX VIB もアップグレードされます。

アップグレード前のバージョンが NSX 6.2.x 以前、または ESXi 5.5 がインストールされた NSX 6.3.0 以降の場合は、アップグレードを完了するためにホストを再起動する必要があります。

- クラスタで DRS が有効になっている場合、[すべてを解決 (Resolve all)] をクリックすると、DRS は、仮想マシンを継続して実行可能な制御された方法でホストの再起動を試みます。仮想マシンはクラスタ内の別のホストに移動され、ホストはメンテナンス モードに移行して再起動されます。
- クラスタで DRS が有効になっていない場合は、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。[すべてを解決 (Resolve all)] をクリックすると、ホストはメンテナンス モードに移行して再起動されます。

アップグレード前のバージョンが、ESXi 6.0 以降がインストールされた NSX 6.3.0 以降の場合は、アップグレードを完了するため、ホストをメンテナンス モードに移行する必要があります。再起動は不要です。

- クラスタで DRS が有効になっている場合、[すべてを解決 (Resolve all)] をクリックすると、DRS は、仮想マシンを継続して実行可能な制御された方法で、ホストのメンテナンス モードへの移行を試みます。仮想マシンはクラスタ内の別のホストに移動され、ホストはメンテナンス モードに移行します。

- クラスタで DRS が有効になっていない場合は、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。アップグレードを完了するためには、ホストを手動でメンテナンス モードに移行させる必要があります。

NSX 6.3.5 以降では、[ホストの準備 (Host Preparation)] タブで ESX Agent Manager (EAM) のステータスを確認できます。

#### 前提条件

- NSX Manager と NSX Controller クラスタをアップグレードします。
- NSX Manager のアップグレード後、ホスト クラスタをアップグレードする前に、vSphere Web Client からログアウトしてから、再度ログインします。
- 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。
- 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。
- 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。

VIB は、ESXi と NSX のバージョンによって異なるため、アップグレードで変わる可能性があります。現在インストールされている VIB のバージョンを記録します。

ESXi バージョン	NSX バージョン	インストールされている VIB
5.5	6.1.x、6.2.x または 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 以降	6.3.2 以前	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 以降	6.3.3 以降	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

**注:** NSX の一部のバージョンには、アップグレードで削除される VIB があります。

- 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 が含まれています。

#### 手順

- 1 vSphere Web Client で [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール手順 (Installation)] 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。

#### NSX Component Installation on Hosts

##### Actions

Clusters & Hosts	Installation Status	Firewall	VXLAN
▶ Compute Cluster A	✓ 6.2.0 Upgrade available	✓ Enabled	✓ Configured
▶ Management & Edge Cluster	✓ 6.2.0 Upgrade available	✓ Enabled	✓ Configured

[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。

- 5 DRS が無効になっている状態で [解決 (Resolve)] アクションが失敗しており、ESXi 6.0 以降 と NSX 6.3.0 以降 を共にアップグレードしている場合、アップグレードを完了するには、ホストを手動でメンテナンス モードに移行させる必要があります。

a 回避したホストをメンテナンス モードに設定します。

b [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。

アップグレードは、ホストがメンテナンス モードに移行すると自動的に開始されます。[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。ステータスが **[インストールしています]** にならない場合は、ページを更新してください。

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。

c ホストのメンテナンス モードを解除します。

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** コマンドを実行します。VIB が正しいバージョンに更新されたことを確認します。

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。

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

[\[NSX Edge のアップグレード\]](#)

## NSX Edge のアップグレード

アップグレード プロセスでは、新しい Edge 仮想アプライアンスが既存のアプライアンス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 がアップグレードされていることを確認します。
- 分散論理ルーターをアップグレードする前に、NSX Controller クラスタおよびホストの準備が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、適切なサイズの NSX Edge アプライアンスを 2 台準備し、2 台ともパワーオン状態にします。
  - 高可用性 (HA) 構成の NSX Edge インスタンスの場合は、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 Edge アプライアンス用に設定した場所と実際の配置場所にリストされたホスト クラスタが、NSX 用に準備されていることと、メッセージング インフラストラクチャのステータスが**正常**であることを確認する必要があります。NSX Edge アプライアンスの作成後にクラスタが削除された場合など、設定した場所が使用できない場合には、実際の配置場所のみを確認します。
  - GET `https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances` API 要求を使用して、最初に設定した場所の ID (<configuredResourcePool > id>) と現在の場所 (<resourcePoolId>) を確認します。
  - GET `https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}` API 要求を使用して、これらのクラスタのホスト準備ステータスとメッセージング インフラストラクチャのステータスを検索します。<resourceId> は、前の手順で確認した NSX Edge アプライアンス設定場所と実際の配置場所を表す ID です。
    - 応答本文の `com.vmware.vshield.vsm.nwfabric.hostPrep` の <featureId> に対応するステータスを確認します。ステータスは**正常**である必要があります。

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- 応答本文の `com.vmware.vshield.vsm.messagingInfra` の `<featureId>` に対応するステータスを確認します。ステータスは**正常**である必要があります。

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- 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 ガイド』の「NSX アップグレードの運用上の影響」を参照してください。
- アップグレード前のバージョンが NSX 6.0.x で、NSX Edge で L2 VPN が有効になっている場合は、L2 VPN の設定を削除してからアップグレードを行う必要があります。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 で、[Networking and Security (Networking & Security)] - [NSX Edge (NSX Edges)] の順に選択します。
- 2 各 NSX Edge インスタンスで、[アクション (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

vSphere HA が有効で Edge が展開されているクラスタでは、NSX Edge の 6.2.4 以前のバージョンを 6.2.5 以降にアップグレードした後、vSphere の [仮想マシンの起動] を無効にする必要があります。無効にするには、vSphere Web Client を開いて、NSX Edge 仮想マシンが配置されている ESXi ホストを検索します。[管理 (Manage)] - [設定 (Settings)] の順にクリックして、[仮想マシン] で [仮想マシンの起動/シャットダウン] を選択し、[編集 (Edit)] をクリックして、仮想マシンが手動モードであること（つまり、自動起動/シャットダウン リストに追加されていないこと）を確認します。

## 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 をアップグレードします。

### 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 are tabs: 'Installation', 'Management', 'Host Preparation', 'Logical Network Preparation', and 'Service Deployments'. The 'Service Deployments' tab is selected. Below the tabs, there is a dropdown menu for 'NSX Manager' showing '192.168.110.15 (Role: Primary)'. Below that, there is 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, there is a table with 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'. The 'Installation Status' column shows 'Succeeded' and 'Upgrade Available' (indicated by a blue arrow icon). The 'Service Status' column shows 'Up' (indicated by a green checkmark icon). 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

一部の NSX サービスは直接アップグレードをサポートしていません。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 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 6.3.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

NSX 6.0.x がインストールされている NSX Edge に L2 VPN がインストールされている場合、NSX Edge のアップグレードはサポートされません。L2 VPN の設定は、NSX Edge をアップグレードする前に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
```

## Cross-vCenter NSX 環境での NSX 6.3.x へのアップグレード

Cross-vCenter 環境で NSX 6.3.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り再開する場合、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 環境でのプライマリ 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。



**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。

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。

アップグレード中に、NSX のカスタマー エクスペリエンス向上プログラム (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 のカスタマー エクスペリエンス向上プログラムのセクションを参照してください。

NSX 6.3.0 以降からアップグレードする場合、アップグレード バンドルのアップロードとアップグレードの開始は別々に実行できます。以前にアップロードされたアップグレード バンドルからアップグレードを開始するには、[ホーム (Home)] - [アップグレード (Upgrade)] の順に移動し、[アップグレードを開始 (Begin Upgrade)] をクリックします。

NSX Manager を NSX 6.3.6 にアップグレードすると、アップグレード中にバックアップが自動的に作成され、ローカルに保存されます。これらのバックアップ ファイルの管理方法については、[「アップグレードで作成された NSX Manager のバックアップの管理」](#)を参照してください。

- アップグレードで自動バックアップの作成に失敗すると、アップグレードが停止します。サポートが必要な場合は、VMware サポートにお問い合わせください。
- 自動バックアップは、定期的なバックアップに失敗した場合のフェイルセーフとなります。
  - アップグレードの前に、NSX Manager の定期的なバックアップを必ず行ってください。詳細については [「NSX Manager データのバックアップ」](#) を参照してください。このバックアップは、VMware サポートを利用せずにリストアできます。
  - 自動バックアップのリストアが必要な場合は、VMware サポートにお問い合わせください。

## 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** を実行して、ファイルシステムの使用量を表示します。
  - b 使用率が 100% の場合は、特権（有効）モードに切り替えて **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。
- アップグレードの前に、NSX Manager 仮想アプライアンスの予約済みメモリが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。
- 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。Data Security は、NSX 6.3.x から削除されています。
- 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。
- 同じメンテナンス期間内に、Cross-vCenter NSX 環境のすべての NSX Manager をアップグレードする必要があります。
- 同じメンテナンス期間でアップグレードする NSX Manager を決定します。
  - Cross-vCenter NSX 環境の場合、同じメンテナンス期間内にプライマリ NSX Manager とすべてのセカンダリ NSX Manager を同じ NSX バージョンにアップグレードする必要があります。
  - 同じ SSO サーバを使用する vCenter Server システムに複数の NSX Manager が接続している場合、NSX Manager のバージョンのすべての組み合わせはサポートされません。サポートされる構成がメンテナンス期間の最後に残るように、NSX Manager のアップグレードをプランニングする必要があります。
    - 同じバージョンの NSX を使用している NSX Manager はすべてサポートされます。
    - 異なるバージョンの NSX を使用する NSX Manager がサポートされます。これは、1 つ以上の NSX Manager に NSX 6.4.0 以降がインストールされ、他のすべての NSX Manager に NSX 6.3.3 以降がインストールされている場合に適用されます。

## 手順

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

- 3 [アップグレード (Upgrade)] をクリックし、[ファイルを選択 (Choose File)] をクリックして **VMware-NSX-Manager-upgrade-bundle-<releaseNumber>-<NSXbuildNumber>.tar.gz** ファイルを選択します。[続行 (Continue)] 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 アップグレードを後で開始する場合は、[アップグレード] ダイアログ ボックスで [閉じる (Close)] をクリックします。

アップグレードを開始する準備ができたなら、[ホーム (Home)] - [アップグレード (Upgrade)] の順に移動し、[アップグレードを開始 (Begin Upgrade)] をクリックします。

- 5 [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選択し、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加するかどうかを選択します。[アップグレード (Upgrade)] 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。

---

**注:** [アップグレード] ダイアログ ボックスに、自動バックアップが行われたことを示すメッセージが表示されます。

---

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。

- 6 NSX Manager 仮想アプライアンスに再びログインし、ホーム ページから [アップグレード (Upgrade)] をクリックします。アップグレードの状態が [完了 (Complete)] になっていることと、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 (Installation)] - [管理 (Management)] 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 環境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、この手順を繰り返します。

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。

アップグレード中に、NSX のカスタマー エクスペリエンス向上プログラム (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 のカスタマー エクスペリエンス向上プログラムのセクションを参照してください。

NSX 6.3.0 以降からアップグレードする場合、アップグレード バンドルのアップロードとアップグレードの開始は別々に実行できます。以前にアップロードされたアップグレード バンドルからアップグレードを開始するには、[ホーム (Home)] - [アップグレード (Upgrade)] の順に移動し、[アップグレードを開始 (Begin Upgrade)] をクリックします。

NSX Manager を NSX 6.3.6 にアップグレードすると、アップグレード中にバックアップが自動的に作成され、ローカルに保存されます。これらのバックアップ ファイルの管理方法については、[\[アップグレードで作成された NSX Manager のバックアップの管理\]](#) を参照してください。

- アップグレードで自動バックアップの作成に失敗すると、アップグレードが停止します。サポートが必要な場合は、VMware サポートにお問い合わせください。
- 自動バックアップは、定期的なバックアップに失敗した場合のフェイルセーフとなります。
  - アップグレードの前に、NSX Manager の定期的なバックアップを必ず行ってください。詳細については [\[NSX Manager データのバックアップ\]](#) を参照してください。このバックアップは、VMware サポートを利用せずにリストアできます。

- 自動バックアップのリストアが必要な場合は、VMware サポートにお問い合わせください。

#### 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。
  - NSX Manager にログインし、**show filesystems** を実行して、ファイルシステムの使用量を表示します。
  - 使用率が 100% の場合は、特権（有効）モードに切り替えて **purge log manager** コマンドと **purge log system** コマンドを実行します。
  - 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。
- アップグレードの前に、NSX Manager 仮想アプライアンスの予約済みメモリが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。
- 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。Data Security は、NSX 6.3.x から削除されています。
- 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。
- 同じメンテナンス期間内に、Cross-vCenter NSX 環境のすべての NSX Manager をアップグレードする必要があります。
- 同じメンテナンス期間でアップグレードする NSX Manager を決定します。
  - Cross-vCenter NSX 環境の場合、同じメンテナンス期間内にプライマリ NSX Manager とすべてのセカンダリ NSX Manager を同じ NSX バージョンにアップグレードする必要があります。
  - 同じ SSO サーバを使用する vCenter Server システムに複数の NSX Manager が接続している場合、NSX Manager のバージョンのすべての組み合わせはサポートされません。サポートされる構成がメンテナンス期間の最後に残るように、NSX Manager のアップグレードをプランニングする必要があります。
    - 同じバージョンの NSX を使用している NSX Manager はすべてサポートされます。
    - 異なるバージョンの NSX を使用する NSX Manager がサポートされます。これは、1 つ以上の NSX Manager に NSX 6.4.0 以降がインストールされ、他のすべての NSX Manager に NSX 6.3.3 以降がインストールされている場合に適用されます。

## 手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 ホーム ページで、[アップグレード (Upgrade)] をクリックします。
- 3 [アップグレード (Upgrade)] をクリックし、[ファイルを選択 (Choose File)] をクリックして **VMware-NSX-Manager-upgrade-bundle-<releaseNumber>-<NSXbuildNumber>.tar.gz** ファイルを選択します。[続行 (Continue)] 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 アップグレードを後で開始する場合は、[アップグレード] ダイアログ ボックスで [閉じる (Close)] をクリックします。

アップグレードを開始する準備ができたなら、[ホーム (Home)] - [アップグレード (Upgrade)] の順に移動し、[アップグレードを開始 (Begin Upgrade)] をクリックします。

- 5 [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選択し、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加するかどうかを選択します。[アップグレード (Upgrade)] 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。

---

**注:** [アップグレード] ダイアログ ボックスに、自動バックアップが行われたことを示すメッセージが表示されません。

---

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。

- 6 NSX Manager 仮想アプライアンスに再びログインし、ホーム ページから [アップグレード (Upgrade)] をクリックします。アップグレードの状態が [完了 (Complete)] になっていることと、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、メンテナンス時間枠内に実施することをお勧めします。

NSX Controller 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 台ずつ実行されます。アップグレードの進行中は、[アップグレードを利用可能 (Upgrade Available)] 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。

**重要:** NSX 6.3.3 では、NSX Controller の基盤となるオペレーティング システムが変わります。NSX 6.3.2 以前から NSX 6.3.3 以降にアップグレードする場合、インプレース アップグレードは実行されません。既存のコントローラが 1 度に 1 つずつ削除され、同じ IP アドレスを使用して新しい Photon OS ベースのコントローラが展開されます。

コントローラを削除すると、関連する DRS の非アフィニティ ルールも削除されます。新しいコントローラ仮想マシンが同じホストに配置されないように、vCenter Server で新しい非アフィニティ ルールを作成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 (Hosts and Clusters)] ビューで、コントローラを右クリックし、[パワー (Power)] > [リセット (Reset)] の順に選択します。



- 有効な NSX Controller 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 control-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 Controller 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。
- NSX 6.3.3 にアップグレードする場合、NSX Controller クラスタに 3 台のコントローラ ノードが含まれている必要があります。3 台より少ない場合は、アップグレードを開始する前にノードを追加する必要があります。コントローラ ノードの追加方法については、『NSX インストール ガイド』で「NSX Controller クラスタのデプロイ」を参照してください。

## 手順

- ◆ [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール (Installation)] の順に移動し、[管理 (Management)] 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 (Controller Cluster Status)] 列で [アップグレードを利用可能 (Upgrade Available)] をクリックします。

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 (Controller Cluster Status)] 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 (Downloading upgrade file)] 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 (In progress)] 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、ステータスは [完了 (Complete)] と表示され、この列は表示されなくなります。
- NSX Controller ノード セクションの [ステータス (Status)] 列に、それぞれのコントローラのステータスが表示されます。アップグレード前の場合、元の NSX のバージョンに応じて [接続済み (Connected)] または [標準 (Normal)] 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 (Disconnected)] 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 [接続済み (Connected)] になります。
- NSX Controller ノード セクションの [アップグレード ステータス (Upgrade Status)] 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 (Downloading upgrade file)] と表示され、次に [アップグレードが進行中です (Upgrade in progress)] となり、その後 [再起動中です (Rebooting)] 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 (Upgraded)] と表示されます。

---

**注:** NSX 6.3.2 以前から NSX 6.3.3 以降にアップデートする場合、ステータスが [アップグレード ファイルをダウンロード中です (Downloading upgrade file)] ではなく、[アップグレードを待機しています (Queued For Upgrade)] になります。

---

アップグレードが完了すると、NSX Controller 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 (Software Version)] 列に、[6.3]<buildNumber> と表示されます。[show control-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 Controller 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 (Upgrade Status)] 列に [失敗 (Failed)] 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 (Upgrade Available)] 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 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。別のコントローラを作成する手順については、『NSX トラブルシューティング ガイド』の「NSX Controller の再デプロイ」を参照してください。

#### 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 クラスタをアップデートする必要があります。

ホスト クラスタをアップグレードすると、NSX VIB もアップグレードされます。

アップグレード前のバージョンが NSX 6.2.x 以前、または ESXi 5.5 がインストールされた NSX 6.3.0 以降の場合は、アップグレードを完了するためにホストを再起動する必要があります。

- クラスタで DRS が有効になっている場合、[すべてを解決 (Resolve all)] をクリックすると、DRS は、仮想マシンを継続して実行可能な制御された方法でホストの再起動を試みます。仮想マシンはクラスタ内の別のホストに移動され、ホストはメンテナンス モードに移行して再起動されます。
- クラスタで DRS が有効になっていない場合は、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。[すべてを解決 (Resolve all)] をクリックすると、ホストはメンテナンス モードに移行して再起動されます。

アップグレード前のバージョンが、ESXi 6.0 以降がインストールされた NSX 6.3.0 以降の場合は、アップグレードを完了するため、ホストをメンテナンス モードに移行する必要があります。再起動は不要です。

- クラスタで DRS が有効になっている場合、[すべてを解決 (Resolve all)] をクリックすると、DRS は、仮想マシンを継続して実行可能な制御された方法で、ホストのメンテナンス モードへの移行を試みます。仮想マシンはクラスタ内の別のホストに移動され、ホストはメンテナンス モードに移行します。
- クラスタで DRS が有効になっていない場合は、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。アップグレードを完了するためには、ホストを手動でメンテナンス モードに移行させる必要があります。

NSX 6.3.5 以降では、[ホストの準備 (Host Preparation)] タブで ESX Agent Manager (EAM) のステータスを確認できます。

## 前提条件

- NSX Manager と NSX Controller クラスタをアップグレードします。
  - NSX Manager のアップグレード後、ホスト クラスタをアップグレードする前に、vSphere Web Client からログアウトしてから、再度ログインします。
  - 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。
  - 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。
  - 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。
- VIB は、ESXi と NSX のバージョンによって異なるため、アップグレードで変わる可能性があります。現在インストールされている VIB のバージョンを記録します。

ESXi バージョン	NSX バージョン	インストールされている VIB
5.5	6.1.x、6.2.x または 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 以降	6.3.2 以前	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 以降	6.3.3 以降	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

注: NSX の一部のバージョンには、アップグレードで削除される VIB があります。

- 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 が含まれています。

## 手順

- 1 vSphere Web Client で [ホーム (Home)] > [Networking and Security (Networking & Security)] > [インストール手順 (Installation)] 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。

### NSX Component Installation on Hosts

#### Actions

Clusters & Hosts	Installation Status	Firewall	VXLAN
▶ Compute Cluster A	✓ 6.2.0 Upgrade available	✓ Enabled	✓ Configured
▶ Management & Edge Cluster	✓ 6.2.0 Upgrade available	✓ Enabled	✓ Configured

[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。

- 5 DRS が無効になっている状態で [解決 (Resolve)] アクションが失敗しており、ESXi 6.0 以降 と NSX 6.3.0 以降 を共にアップグレードしている場合、アップグレードを完了するには、ホストを手動でメンテナンス モードに移行させる必要があります。

a 回避したホストをメンテナンス モードに設定します。

- b [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。

アップグレードは、ホストがメンテナンス モードに移行すると自動的に開始されます。[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。ステータスが **[インストールしています]** にならない場合は、ページを更新してください。

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。

- c ホストのメンテナンス モードを解除します。

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** コマンドを実行します。VIB が正しいバージョンに更新されたことを確認します。

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。

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

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

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

アップグレード プロセスでは、新しい Edge 仮想アプライアンスが既存のアプライアンス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。

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。

#### 前提条件

- NSX Manager がアップグレードされていることを確認します。
- 分散論理ルーターをアップグレードする前に、NSX Controller クラスタおよびホストの準備が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、適切なサイズの NSX Edge アプライアンスを 2 台準備し、2 台ともパワーオン状態にします。
  - 高可用性 (HA) 構成の NSX Edge インスタンスの場合は、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 Edge アプライアンス用に設定した場所と実際の配置場所にリストされたホスト クラスタが、NSX 用に準備されていることと、メッセージング インフラストラクチャのステータスが**正常**であることを確認する必要があります。NSX Edge アプライアンスの作成後にクラスタが削除された場合など、設定した場所が使用できない場合には、実際の配置場所のみを確認します。
  - GET `https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances` API 要求を使用して、最初に設定した場所の ID (`<configuredResourcePool > id>`) と現在の場所 (`<resourcePoolId>`) を確認します。
  - GET `https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}` API 要求を使用して、これらのクラスタのホスト準備ステータスとメッセージング インフラストラクチャのステータスを検索します。`<resourceId>` は、前の手順で確認した NSX Edge アプライアンス設定場所と実際の配置場所を表す ID です。
    - 応答本文の `com.vmware.vshield.vsm.nwfabric.hostPrep` の `<featureId>` に対応するステータスを確認します。ステータスは**正常**である必要があります。

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
```



```
<installed>true</installed>
<enabled>true</enabled>
<allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- 応答本文の `com.vmware.vshield.vsm.messagingInfra` の `<featureId>` に対応するステータスを確認します。ステータスは**正常**である必要があります。

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- 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 ガイド』の「NSX アップグレードの運用上の影響」を参照してください。
- アップグレード前のバージョンが NSX 6.0.x で、NSX Edge で L2 VPN が有効になっている場合は、L2 VPN の設定を削除してからアップグレードを行う必要があります。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 で、[Networking and Security (Networking & Security)] - [NSX Edge (NSX Edges)] の順に選択します。
- 2 各 NSX Edge インスタンスで、[アクション (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

vSphere HA が有効で Edge が展開されているクラスタでは、NSX Edge の 6.2.4 以前のバージョンを 6.2.5 以降にアップグレードした後、vSphere の [仮想マシンの起動] を無効にする必要があります。無効にするには、vSphere Web Client を開いて、NSX Edge 仮想マシンが配置されている ESXi ホストを検索します。[管理 (Manage)] - [設定 (Settings)] の順にクリックして、[仮想マシン] で [仮想マシンの起動/シャットダウン] を選択し、[編集 (Edit)] をクリックして、仮想マシンが手動モードであること（つまり、自動起動/シャットダウン リストに追加されていないこと）を確認します。



## 「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 をアップグレードします。

#### 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, the 'Installation' tab is selected, and within it, the 'Service Deployments' sub-tab is active. Below the tabs, the 'NSX Manager' dropdown shows '192.168.110.15 (Role: Primary)'. The main section is titled 'Network & Security Service Deployments' and contains a message: '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 (-), refreshing, and an upgrade arrow (⬆). A search filter is also present. The main table lists the services:

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

一部の NSX サービスは直接アップグレードをサポートしていません。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 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 6.3.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

NSX 6.0.x がインストールされている NSX Edge に L2 VPN がインストールされている場合、NSX Edge のアップグレードはサポートされません。L2 VPN の設定は、NSX Edge をアップグレードする前に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

## 2

NSX と vSphere のアップグレードが必要な場合、まず NSX のアップグレードを完了してから、vSphere のアップグレードを完了することをお勧めします。

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。

NSX 6.3.x がインストールされている場合、ESXi をアップグレードする方法は、アップグレード前後の ESXi のバージョンによって異なります。

表 2-1. NSX 6.3.x がインストールされている場合の ESXi のアップグレード方法

ホストのアップグレードのタイプ	ホストのメンテナンス モードの要件	ホストの再起動の要件
ESXi 5.5 から ESXi 6.0 へのアップグレード 「 <a href="#">NSX 環境での ESXi 6.0 へのアップグレード</a> 」を参照してください。	ESXi のアップグレードと、後続の NSX VIB のアップグレードが完了するまで、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。	ESXi のアップグレード時には再起動が必要です。後続の NSX VIB のアップグレード時にも再起動が必要です。
ESXi 5.5 から ESXi 6.5 へのアップグレード 「 <a href="#">NSX 環境での ESXi 6.5 へのアップグレード</a> 」を参照してください。	ESXi のアップグレード後に、ホストのメンテナンスモードを終了しても問題ありません。後続の NSX VIB のアップグレードが完了するまで、アップグレードされたホスト上の VXLAN を使用する vSphere Distributed Switch に、vMotion による仮想マシンの移行はブロックされます。	ESXi のアップグレード時には再起動が必要です。後続の NSX VIB のアップグレード時にも再起動が必要です。
ESXi 6.0 から ESXi 6.5 へのアップグレード 「 <a href="#">NSX 環境での ESXi 6.5 へのアップグレード</a> 」を参照してください。	ESXi のアップグレード後に、ホストのメンテナンスモードを終了しても問題ありません。後続の NSX VIB のアップグレードが完了するまで、アップグレードされたホスト上の VXLAN を使用する vSphere Distributed Switch に、vMotion による仮想マシンの移行はブロックされます。	ESXi のアップグレード時には再起動が必要です。後続の NSX VIB のアップグレード時に再起動は不要です。

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 6.0 へのアップグレード](#)
- [NSX 環境での ESXi 6.5 へのアップグレード](#)
- [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 6.0 へのアップグレード

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。

インストールされている NSX VIB は、ESXi と NSX のバージョンによって異なります。NSX 6.3.3 以降の環境で ESXi 5.5 から 6.0 にアップグレードすると、esx-vsip と esx-vxlan VIB が削除され、esx-nsxv VIB で置換されます。

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

**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** 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 6.0 と NSX 6.3.2 以前にアップグレードした場合：

```
[root@host-1:~] esxcli software vib list
...
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 6.0 と NSX 6.3.3 以降にアップグレードした場合：

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv      6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-08-10
...
```

## NSX 環境での ESXi 6.5 へのアップグレード

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。

NSX 6.3.x がインストールされている状態で ESXi 6.5 にアップグレードする場合、新しい NSX VIB がインストールされるまで、アップグレードされたホスト上の VXLAN を使用する vSphere Distributed Switch への、vMotion による仮想マシンの移行はブロックされます。

VMware では、NSX 6.3.x 環境でホストを ESXi 6.5 にアップグレードする場合は、vSphere Upgrade Manager を使用することをお勧めします。

ESXi のアップグレードに使用するメソッドに関係なく、次のワークフローに従う必要があります。一度に 1 台のホストに対し、次を実行します。

### 1 ESXi のアップグレード

ESXi のアップグレードが完了すると、ホストのメンテナンス モードは終了しますが、次の手順が完了するまで論理スイッチに接続している仮想マシンをホストに移行することはできません。

### 2 NSX VIB のアップグレード

VIB がアップグレードされ、ホストのメンテナンス モードが終了すると、論理スイッチに接続されている仮想マシンをホストに移行できます。

---

**重要:** 一度に 1 台のホストをアップグレードする必要があります。ESXi をアップグレードする際は、修正にクラスタまたはデータセンターを選択しないでください。

---

インストールされている NSX VIB は、ESXi と NSX のバージョンによって異なります。NSX 6.3.3 以降の環境で ESXi 5.5 から 6.5 にアップグレードすると、esx-vsip と esx-vxlan VIB が削除され、esx-nsxv VIB で置換されます。

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

#### 前提条件

- NSX 6.3.x がインストールされていることを確認します。
- 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。

**重要:** NSX 6.3.x は、ESXi 6.5 の初期リリースとは相互運用性がありません。NSX 6.3.0 との互換性を確保するためには、ESXi 6.5.0a 以降にアップグレードする必要があります。最新の相互運用性情報については、相互運用性マトリックスを確認してください。

- 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。
- vSphere Update Manager がインストールされ、設定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ーで、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。クラスター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ー (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、[Update Manager] - [<Update Manager オブジェクト> (<Update Manager Object>)] - [管理 (Manage)] の順に移動します。
- 2 「ホストのアップグレード イメージのインポートとホストのアップグレード ベースラインの作成」の手順に従って、ホストのアップグレード イメージをインポートし、ホストのアップグレード ベースラインを作成します。
  - a [ESXi イメージ (ESXi Images)] タブ選択し、[ESXi イメージのインポート (Import ESXi Image)] をクリックして、アップロードするイメージを参照します。
  - b [ホストのベースライン (Host Baselines)] タブ、[新規ベースライン (New Baseline)] の順にクリックします。新規ベースライン ウィザードを使用して新しいベースラインを作成し、ベースライン タイプとして [ホストのアップグレード (Host Upgrade)] を選択します。
- 3 一度に 1 台のホストをアップグレードします。ホストごとに次の手順を繰り返します。
  - a [ホストおよびクラスター (Hosts and Clusters)] に移動し、アップグレードするホストを選択します。クラスターまたはデータセンターを選択しないでください。
  - b ホストを右クリックし、[Update Manager] - [ベースラインの添付... (Attach Baseline...)] の順に選択します。ベースラインまたはベースライン グループの添付ウィザードを使用して、ベースラインを選択します。完全な手順については、vSphere のドキュメントの「オブジェクトへのベースラインおよびベースライン グループの添付」を参照してください。
  - c ホストを右クリックし、[Update Manager] - [修正... (Remediate...)] の順に選択します。修正ウィザードを使用して、ベースラインを選択します。完全な手順については、vSphere のドキュメントの「アップグレード ベースラインを基準にしたホストの修正」を参照してください。
  - d 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。
  - e アップグレードが完了したことを確認するには、ホストを右クリックし、[Update Manager] - [アップデートの有無のスキャン... (Scan for Updates...)] の順に選択します。[アップグレード (Upgrades)] チェックボックスをクリックして、アップグレード基準に準拠しているかどうかスキャンします。[コンプライアンス ステータス] が **準拠** になっていれば、アップグレードは完了しています。  
  
詳細な手順については、vSphere のドキュメントの「手動による ESXi ホストのスキャンの開始」を参照してください。
  - f [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。

- g ESXi をアップグレードしたホストを確認します。[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。

詳細を確認する場合は、[準備ができていません (Not Ready)] をクリックしてください。

- h ホストを選択し、[アクション (Actions)] - [解決 (Resolve)] の順にクリックすると、NSX VIB のインストールが始まります。

アップグレード前のバージョンが ESXi 5.5 で、クラスタで DRS が有効になっている場合、DRS は仮想マシンを継続して実行可能な制御された方法で、ホストの再起動を試みます。何らかの理由で DRS の操作が失敗した場合、[解決 (Resolve)] アクションは停止します。この場合、仮想マシンを手動で移動して、[解決 (Resolve)] アクションをもう一度実行するか、ホストを手動でメンテナンス モードに移行させて再起動する必要があります。

アップグレード前のバージョンが ESXi 6.0 で、クラスタで DRS が有効になっている場合、DRS は仮想マシンを継続して実行可能な制御された方法で、ホストのメンテナンス モードへの移行を試みます。何らかの理由で DRS の操作が失敗した場合、[解決 (Resolve)] アクションは停止します。この場合、仮想マシンを手動で移動して、[解決 (Resolve)] アクションをもう一度実行するか、ホストを手動でメンテナンス モードにする必要があります。

**重要:** アップグレード前のバージョンが ESXi 6.0 で、ホストを手動でメンテナンス モードに移行してホスト VIB をインストールする場合は、メンテナンス モードを解除する前に、ホスト VIB のインストールが完了したことを確認する必要があります。[ホストの準備 (Host Preparation)] には、インストールが完了している場合でも、[インストール ステータス] に **[インストールしています]** と表示されます。

- 1 vSphere Web Client の [最近のタスク] ペインで、すべてのインストール タスクが完了していることを確認します。
- 2 ホストのコマンドラインにアクセスし、**esxcli software vib list** コマンドを実行します。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 6.5 と NSX 6.3.2 以前にアップグレードした場合：

```
[root@host-1:~] esxcli software vib list
...
esx-vsip      6.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
esx-vxlan     6.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
...
```

ESXi 6.5 と NSX 6.3.3 以降にアップグレードした場合：

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv      6.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-08-10
...
```

## 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。