

# NSX for vShield Endpoint アップグレード ガイド

Update 5

変更日：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

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

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

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

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

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

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

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

# 内容

- 1 NSX for vShield Endpoint アップグレード ガイド 4
  - [サポート ドキュメント](#) 5
  - [NSX for vShield Endpoint のシステム要件](#) 5
  - [NSX で必要となるポートおよびプロトコル](#) 6
- 2 vCloud Networking and Security から NSX へのアップグレード 9
  - [vCloud Networking and Security から NSX for vShield Endpoint へのアップグレードの準備](#) 9
  - [vCloud Networking and Security 5.5.x から NSX 6.2.x for vShield Endpoint へのアップグレード](#) 17
- 3 NSX for vShield Endpoint でのパートナー サービスの使用 25
  - [NSX for vShield Endpoint のパートナー サービスのアップグレード](#) 25
  - [パートナー サービスの展開](#) 25
  - [NSX for vShield Endpoint での Service Composer の使用](#) 27

# NSX for vShield Endpoint アップグレードガイド

# 1

この NSX for vShield Endpoint アップグレードガイドでは、vSphere Web Client を使用して VMware® NSX™ 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、エンドポイント機能を使用する目的にのみ vCloud Networking and Security を使用するユーザー、およびアンチウイルスのオフロード用に vShield Endpoint を展開および管理するため、NSX へのアップグレードを計画しているユーザーを対象としています。本書に記載されている情報は、システム管理者としての経験があり、仮想マシンテクノロジーおよび仮想データセンターの操作に詳しい方を対象としています。また、本書は VMware ESXi、vCenter Server、vSphere Web Client を含む VMware vSphere 5.5 または 6.0 について理解していることを前提としています。

論理スイッチ、論理ルーター、Distributed Firewall または NSX Edge などの他の NSX の機能を使用する必要がある場合は、『NSX アップグレードガイド』を参照してください。

## VMware の技術ドキュメントの用語集

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

この章には、次のトピックが含まれています。

- サポート ドキュメント
- NSX for vShield Endpoint のシステム要件
- NSX で必要となるポートおよびプロトコル

## サポート ドキュメント

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

### リリース ノート

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

### 製品の相互運用性マトリックス

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

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

### 互換性ガイド

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

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

## NSX for vShield Endpoint のシステム要件

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

## ハードウェア

表 1-1. ハードウェア要件

アプライアンス	メモリ	vCPU	ディスク容量
NSX Manager	16 GB (NSX デプロイ環境のサイズ* によっては 24 GB)	4 (NSX デプロイ環境のサイズ* によっては 8)	60 GB
ゲスト イントロスペクション	1 GB	2	4 GB

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

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

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

## ソフトウェア

VMware 製品の次のバージョンをサポートしています。

- VMware vCenter Server 5.5U3 以降
- VMware vCenter Server 6.0U2 以降

## クライアントとユーザー アクセス

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

## NSX で必要となるポートおよびプロトコル

NSX が正常に機能するには、次のポートが開いている必要があります。

表 1-2. NSX で必要となるポートおよびプロトコル

送信元	宛先	ポート	プロトコル	目的	機密	TLS	認証
クライアント PC	NSX Manager	443	TCP	NSX Manager 管理インターフェイス	×	○	PAM 認証
クライアント PC	NSX Manager	80	TCP	NSX Manager VIB アクセス	×	×	PAM 認証
ESXi ホスト	vCenter Server	443	TCP	ESXi ホストの準備	×	×	
vCenter Server	ESXi ホスト	443	TCP	ESXi ホストの準備	×	×	
ESXi ホスト	NSX Manager	5671	TCP	RabbitMQ	×	○	RabbitMQ ユーザー/パスワード
ESXi ホスト	NSX Controller	1234	TCP	ユーザー ワールド エージェント接続	×	○	
NSX Controller	NSX Controller	2878、 2888、 3888	TCP	コントローラ クラスタ - 状態同期	×	○	IPsec

表 1-2. NSX で必要となるポートおよびプロトコル (続き)

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

表 1-2. NSX で必要となるポートおよびプロトコル (続き)

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

## Cross-vCenter NSX と拡張リンク モードのポート

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



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

## 2

この章には、次のトピックが含まれています。

- vCloud Networking and Security から NSX for vShield Endpoint へのアップグレードの準備
- vCloud Networking and Security 5.5.x から NSX 6.2.x for vShield Endpoint へのアップグレード

## vCloud Networking and Security から NSX for vShield Endpoint へのアップグレードの準備

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



**警告:** ダウングレードはサポートされない:

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

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

次のガイドラインは、アップグレード前のチェックリストとして使用できます。

- 1 vCloud Networking and Security のバージョンが 5.5 であることを確認します。このバージョンでない場合は、『vShield インストールとアップグレード ガイド』バージョン 5.5 を参照して、アップグレードの手順を確認してください。
- 2 必要なポートがすべて開いていることを確認します。「[NSX で必要となるポートおよびプロトコル](#)」を参照してください。
- 3 vCenter Server が NSX 6.2.x のシステム要件を満たしていることを確認します。「[NSX for vShield Endpoint のシステム要件](#)」を参照してください。
- 4 vSphere Distributed Switch のアップリンク ポート名情報を取得できることを確認します。<https://kb.vmware.com/kb/2129200> を参照してください。

- 5 vShield Endpoint パートナーのサービスを展開している場合は、アップグレードを行う前に互換性を確認します。
  - ほとんどの場合、パートナー ソリューションに影響を与えることなく、vCloud Networking and Security を NSX にアップグレードできます。ただし、アップグレードする NSX のバージョンと、パートナー ソリューションとの間に互換性がない場合、NSX をアップグレードする前に、パートナー ソリューションを互換性のあるバージョンにアップグレードする必要があります。
  - VMware 互換性ガイドでネットワークとセキュリティについて確認します。  
<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security> を参照してください。
  - パートナー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。
- 6 環境内に Data Security がある場合は、vShield Manager のアップグレード前にアンインストールしておきます。[「vShield Data Security のアンインストール」](#) を参照してください。
- 7 外部スイッチ プロバイダとして Cisco Nexus 1000V を使用している場合は、NSX にアップグレードする前に、これらのネットワークを vSphere Distributed Switch に移行する必要があります。NSX をインストールしたら、vSphere Distributed Switches を論理スイッチに移行できます。
- 8 vShield Manager、vCenter Server、およびその他の vCloud Networking and Security コンポーネントの最新のバックアップが作成済みであることを確認します。[「vCloud Networking and Security のバックアップとリストア」](#) を参照してください。
- 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。[「vShield Manager から NSX へのアップグレード バンドルのダウンロードと MD5 の確認」](#) を参照してください。
- 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、vCloud Networking and Security のコンポーネントとアプライアンスのパワーオフや削除を行わないでください。

## アップグレードによる vShield Endpoint の動作上の影響

vCloud Networking and Security のアップグレードには時間がかかる場合があります。アップグレード中の vCloud Networking and Security コンポーネントの動作状態を理解することが重要です。

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

- vShield Manager
- vShield Endpoint

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

## vCenter Server のアップグレード

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

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

## vShield Manager のアップグレード

アップグレード中：

- vShield Manager の設定はブロックされます。vShield API サービスは利用できません。vShield の設定は変更できません。既存の仮想マシンの接続は引き続き機能します。

アップグレード後：

- vShield と NSX の設定の変更はすべて許可されます。

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

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

アップグレード中：

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

アップグレード後：

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

## vShield Endpoint の動作状態の確認

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

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

アップグレード前のチェックリストとして次の手順を実行します。

#### 手順

- 1 管理者ユーザーの ID とパスワードを特定します。
- 2 正引きと逆引きの名前解決が、すべてのコンポーネントで動作していることを確認します。
- 3 すべての vSphere と vShield コンポーネントにログインできることを確認します。
- 4 vShield Manager、vCenter Server、および ESXi の現在のバージョンをメモします。
- 5 vShield 環境を視覚的に確認して、すべてのステータス インジケータが緑、正常、デプロイ済みの状態であることを確認します。
- 6 Syslog が設定されていることを確認します。
- 7 パートナー ソリューションが動作していることを確認します。

たとえば、EICAR Standard Anti-Virus Test File (<http://www.eicar.org/86-0-Intended-use.html>) を使用してアンチウイルスの機能をテストできます。

- 8 (オプション) テスト環境がある場合は、本番環境をアップグレードする前に、アップグレードとアップグレード後の機能をテストします。

## ローカル管理者ユーザーの CLI 管理者ユーザーへの移行

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

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

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

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

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

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

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

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

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

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

たとえば、curl を使用して、次のように指定します。

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

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

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

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

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

たとえば、curl を使用して、次のように指定します。

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

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

たとえば、curl を使用して、次のように指定します。

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

- CLI ユーザー admin に super\_user ロールを追加します。

たとえば、curl を使用して、次のように指定します。

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

## vShield Data Security のアンインストール

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

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

### 手順

- 1 vShield Manager 5.5 のインベントリ パネルから、[Datacenters] フォルダを展開し、vShield Data Security がインストールされているホストに移動します。
- 2 vShield Data Security がインストールされている各ホストで、次の手順を完了して、アンインストールします。
  - a ホストをクリックして、[vShield ホスト準備] ペインの [サマリ (Summary)] タブで、vShield Data Security の [アンインストール (Uninstall)] リンクをクリックします。
  - b [アンインストールするサービスを選択します] ペインで、vShield Data Security が選択されていることを確認し、[アンインストール (Uninstall)] ボタンをクリックします。

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

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

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

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

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

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

次の場合にバックアップを作成することをお勧めします。

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

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

## vShield Manager データのオン デマンド バックアップ

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

### 手順

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

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

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

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

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

14 [バックアップ (Backup)] をクリックします。

完了すると、バックアップはこのフォームの下テーブルに表示されます。

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

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

## vSphere Distributed Switch のバックアップ

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

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

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

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

## vCenter Server のバックアップ

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

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

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

vCenter Server 5.5 に役立つリンク：

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

vCenter Server 6.0 に役立つリンク：

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



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

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

### 前提条件

MD5 チェックサム ツールを用意します。

### 手順

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

- 2 アップグレード バンドルのファイル名の最後が tar.gz になっていることを確認します。

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

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

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

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

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

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

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

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

- 1 vShield Manager から NSX Manager へ

## 2 vShield Endpoint から NSX ゲスト イントロスペクションへ

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

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



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

#### 前提条件

- [\[vCloud Networking and Security から NSX for vShield Endpoint へのアップグレードの準備\]](#) に記載されているアップグレード準備タスクがすべて完了していることを確認します。
- NSX Manager へのアップグレードに必要なディスク容量が vShield Manager にあることを確認します。 [\[NSX for vShield Endpoint のシステム要件\]](#) を参照してください。
- NSX 6.2.x にアップグレードする前に、vShield Manager 仮想アプライアンスの予約済みメモリを 16 GB 以上に増加し、仮想 CPU を 4 個割り当てます。

[\[NSX for vShield Endpoint のシステム要件\]](#) を参照してください。

#### 手順

- 1 vShield Manager から参照できる場所に NSX のアップグレード バンドルをダウンロードします。アップグレード バンドル ファイルは、**VMware-vShield-Manager-upgrade-bundle-to-NSX-<release>-<buildNumber>.tar.gz** のような名前になっています。
- 2 vShield Manager 5.5 インベントリ パネルから [設定とレポート] をクリックします。
- 3 [アップデート] タブ、[アップグレード バンドルのアップロード] の順にクリックします。
- 4 [ファイルを選択] を選択し、**VMware-vShield-Manager-upgrade-bundle-to-NSX-<release>-<buildNumber>.tar.gz** ファイルを選択して、[開く] をクリックします。
- 5 [ファイルのアップロード] をクリックします。  
ファイルのアップロードには数分かかります。
- 6 [インストール] をクリックして、アップグレード プロセスを開始します。
- 7 [インストールの確認] をクリックします。アップグレード プロセスによって vShield Manager が再起動されるため、vShield Manager ユーザー インターフェイスへの接続が失われる可能性があります。その他の vShield コンポーネントは再起動されません。
- 8 再起動後、Web ブラウザ ウィンドウを開き、https://10.10.10.10 のように IP アドレスを入力して、NSX Manager 仮想マシンにログインします。アップグレードされた NSX Manager の IP アドレスは、vShield Manager と同じです。  
[サマリ] タブにインストールした NSX Manager のバージョンが表示されます。
- 9 [ホーム] - [vCenter Server 登録の管理] の順に移動し、vCenter Server のステータスが **接続中** であることを確認します。

- 10 vSphere Web Client にアクセスしている既存のブラウザ セッションを閉じます。数分待ち、ブラウザ キャッシュをクリアしてから vSphere Web Client に再ログインします。
- 11 vShield Manager で SSH が有効になっていた場合は、アップグレード後に NSX Manager で有効にする必要があります。NSX Manager 仮想アプライアンスにログインし、[サマリの表示] をクリックします。[システム レベルのコンポーネント] で、SSH サービスの [開始] をクリックします。

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

vCloud Networking and Security のパスワード

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

NSX にアップグレードした後のパスワード

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

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

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

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

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

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

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

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

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

## 次のステップ

NSX Manager のバックアップを作成します。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。[「NSX Manager データの vShield Endpoint 用バックアップ」](#) を参照してください。

## NSX Manager データの vShield Endpoint 用バックアップ

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

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

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

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

## 手順

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

- e [バックアップディレクトリ] フィールドに、バックアップの保存先の絶対パスを入力します。

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

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

- f [ファイル名のプリフィックス] に文字列を入力します。

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

- g パス フレーズを入力してバックアップを保護します。

このパス フレーズはバックアップをリストアするために必要となります。

- h [OK] をクリックします。

次はその例です。

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

新しいファイルが [バックアップ履歴] に追加されます。

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

The screenshot shows a dialog box titled "Create or Schedule Backup". It contains four dropdown menus: "Backup Frequency" set to "Weekly", "Day of week" set to "Friday", "Hour of day" set to "15", and "Minute" set to "45". At the bottom of the dialog are three buttons: "Turn OFF", "Modify", and "Cancel".

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

#### 次のステップ

vShield Endpoint をアップグレードします。[「NSX for vShield Endpoint のゲスト イントロスペクションへのアップグレード」](#) を参照してください。

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

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

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

#### 前提条件

NSX Manager が 6.2.x にアップグレードされたことを確認します。

## 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 'Service Deployments' tab in the NSX Manager interface. The 'Installation Status' column for the 'Guest Introspection' service shows 'Succeeded' and 'Upgrade Available'. The 'Service Status' column shows 'Up'. The 'Cluster' column shows 'Comp...'. The 'Datastore' column shows 'ds-site...'. The 'Port Group' column shows 'vds-sit...'. The 'IP Address Range' column 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。

The screenshot shows the 'Confirm Upgrade' dialog box for the 'Guest Introspection' service. The 'Datastore' is set to 'ds-site-a-nfs01', the 'Network' is set to 'vds-site-a\_Management...', and the 'IP assignment' is set to 'GI Pool'. The 'Specify schedule' section has 'Upgrade now' selected. The 'OK' and 'Cancel' buttons are at the bottom.

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

## 次のステップ

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

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

## 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 for vShield Endpoint でのパートナー サービスの使用

# 3

ゲスト イントロスペクションによって、NSX のデプロイ環境でパートナー サービスを使用できるようになります。  
この章には、次のトピックが含まれています。

- [NSX for vShield Endpoint のパートナー サービスのアップグレード](#)
- [パートナー サービスの展開](#)
- [NSX for vShield Endpoint での Service Composer の使用](#)

## NSX for vShield Endpoint のパートナー サービスのアップグレード

vCloud Networking and Security から NSX にアップグレードした後に、パートナー サービスのアップグレードが必要になるか、推奨される場合があります。

### 前提条件

互換性およびアップグレードの詳細については、パートナー サービスのドキュメントを参照してください。

### 手順

- 1 パートナー管理ソリューションをアップグレードします。
- 2 ベンダーのコンソール上の NSX Manager を使用して、パートナー サービスを登録します。  
操作手順についてはパートナー サービスのドキュメントを参照してください。
- 3 古いパートナー サービス仮想マシンをパワーオフして削除します。

### 次のステップ

[「パートナー サービスの展開」](#)

## パートナー サービスの展開

パートナー ソリューションにホスト常駐型の仮想アプライアンスが含まれる場合は、ソリューションを NSX Manager で登録した後にサービスを展開できます。


### 前提条件

次のように設定されていることを確認します。

- パートナー ソリューションは、NSX Manager を使用して登録されます。

- NSX Manager から、パートナー ソリューションの管理コンソールにアクセスできます。

#### 手順

- 1 [Networking and Security] をクリックし、[インストール手順] をクリックします。
- 2 [サービス デプロイ] タブをクリックし、[新しいサービスのデプロイ] (  ) アイコンをクリックします。
- 3 [ネットワークおよびセキュリティ サービスのデプロイ] ダイアログ ボックスで、適切なソリューションを選択します。
- 4 [スケジュールを指定する] (ダイアログ ボックス下部) で、[今すぐデプロイする] を選択してソリューションをすぐにデプロイするか、デプロイの日付と時間を選択します。
- 5 [次へ] をクリックします。
- 6 ソリューションをデプロイするデータセンターおよびクラスタを選択し、[次へ] をクリックします。
- 7 ソリューション サービス仮想マシン ストレージを追加するデータストアを選択するか、[ホスト上が指定済み] を選択します。

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

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

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

ネットワークが [ホスト上が指定済み] に設定されている場合、使用するネットワークは、クラスタの各ホストの [エージェント仮想マシンの設定] > [ネットワーク] プロパティで指定されている必要があります。vSphere API/SDK のドキュメントを参照してください。

エージェント仮想マシンをクラスタに追加する前に、ホストでエージェント仮想マシンのネットワーク プロパティを設定する必要があります。[管理] - [設定] - [エージェント仮想マシン設定] - [ネットワーク] の順に移動し、[編集] をクリックして、エージェント仮想マシンのネットワークを設定します。

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

- 9 [IP 割り当て] で、次のいずれかを選択します。

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

- 10 [次へ] をクリックし、[設定内容の確認] ページで [終了] をクリックします。
- 11 [インストールの状態] に [成功] と表示されるまで、デプロイを監視します。ステータスに [失敗] と表示された場合は、[失敗] の横にあるアイコンをクリックして、エラーを解決するための操作を実行します。

#### 次のステップ

NSX ユーザー インターフェイスまたは NSX API を介してパートナー サービスを使用できるようになりました。

## NSX for vShield Endpoint での Service Composer の使用

Service Composer では、ネットワークおよびセキュリティ サービスを仮想インフラストラクチャ内のアプリケーションにプロビジョニングして割り当てることができます。

Service Composer を使用すると、セキュリティ グループやセキュリティ ポリシーを作成できます。セキュリティ グループには、グループ メンバーの静的および動的な定義を含めることができます。セキュリティ ポリシーは、セキュリティ グループにサービスを適用します。

詳細情報や手順については、『NSX 管理ガイド』の Service Composer の説明を参照してください。