

# vShield クイックスタートガイド

vShield Manager 5.0.1

vShield App 5.0.1

vShield Edge 5.0.1

vShield Endpoint 5.0.1

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、<http://www.vmware.com/jp/support/pubs> を参照してください。

JA-000839-00

**vmware**<sup>®</sup>

最新の技術ドキュメントは VMware の Web サイト (<http://www.vmware.com/jp/support/pubs/>) にあります  
VMware の Web サイトでは最新の製品アップデートも提供されています。

このドキュメントに関するご意見およびご感想がある場合は、[docfeedback@vmware.com](mailto:docfeedback@vmware.com) までお送りください。

Copyright © 2010 – 2012 VMware, Inc. 無断転載を禁ず。本製品は、米国著作権法および米国知的財産法ならびに国際著作権法および国際知的財産法により保護されています。VMware 製品には、<http://www.vmware.com/go/patents-jp> に列記されている 1 つ以上の特許が適用されます。

VMware は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。

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

**ヴァイムウェア株式会社**  
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)

# 目次

- 本書について 5
- 1 vShield への手引き 7
  - vShield コンポーネントの概要 7
  - 導入シナリオ 10
- 2 インストールの準備 13
  - システム要件 13
  - 導入にあたって考慮すべき事柄 14
- 3 vShield Manager のインストール 17
  - vShield Manager OVA ファイルの取得 17
  - vShield Manager 仮想アプライアンスのインストール 17
  - vShield Manager のネットワーク設定の構成 18
  - vShield Manager ユーザー インターフェイスへのログイン 19
  - vShield Manager と vCenter Server の同期 19
  - vSphere Client への vShield Manager プラグインの登録 20
  - vShield Manager ユーザー インターフェイスのデフォルトのアカウントのパスワードの変更 20
- 4 vShield Edge、vShield App、vShield Endpoint、および vShield Data Security のインストール 21
  - ライセンス付与された vShield コンポーネントの評価モードでの実行 21
  - vShield App、vShield Edge、vShield Endpoint および vShield Data Security のための仮想インフラストラクチャの準備 21
  - vShield Endpoint のインストール 25
  - vShield Data Security のインストール 27
- 5 vShield コンポーネントのアンインストール 29
  - vShield App 仮想アプライアンスのアンインストール 29
  - ポート グループからの vShield Edge のアンインストール 30
  - vShield Data Security 仮想マシンのアンインストール 30
  - vShield Endpoint モジュールのアンインストール 30
- 6 vShield のアップグレード 31
  - vShield Manager のアップグレード 31
  - vShield App のアップグレード 32
  - vShield Edge のアップグレード 32
  - vShield Endpoint のアップグレード 33
  - vShield Data Security のアップグレード 34
- 7 vShield のインストールの失敗 35

インデックス 37

# 本書について

---

このマニュアル、『vShield クイック スタート ガイド』では、vShield Manager ユーザー インターフェイス、vSphere Client プラグイン、コマンドライン インターフェイス (CLI) を使用して、VMware vShield™ システムをインストールして構成する方法について説明します。段階的な構成手順や推奨されるベスト プラクティスについても記載しています。

## 対象読者

本書は、VMware vCenter 環境で vShield をインストールまたは使用する方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、このマニュアルは VMware ESX、vCenter Server、vSphere Client を含む VMware Infrastructure 4.x についての知識も前提としています。

## VMware の技術ドキュメントの用語集

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

## 本書へのフィードバック

ドキュメントの向上にご協力ください。本書に関するコメントがございましたら、メールアドレス [docfeedback@vmware.com](mailto:docfeedback@vmware.com) までフィードバックをお寄せください。

## テクニカル サポートおよびエデュケーション リソース

ここでは、お客様にご利用いただけるテクニカル サポート リソースをご紹介します。本書およびその他の文書の最新バージョンは、<http://www.vmware.com/jp/support/pubs> でご覧いただけます。

### オンライン サポートおよび電話サポート

テクニカル サポート リクエストの提出や、製品および契約情報の確認、製品の登録をオンラインで行うには、<http://www.vmware.com/jp/support> をご覧ください。

該当するサポート契約を結んでいるお客様の場合、迅速な対応が必要な Severity1 の問題に関しては電話でのサポートをご利用ください。詳細は <http://www.vmware.com/support/japan.html> をご覧ください。

### サポート サービス

お客様のビジネス ニーズに適した各種サポートの詳細については、<http://www.vmware.com/jp/support/services> をご覧ください。

### VMware プロフェッショナル サービス

VMware 教育サービスのコースでは、広範なハンズオン ラボやケース スタディをご紹介します。また、業務の際のリファレンスとしてお使いいただける資料も提供しています。トレーニングは、オンサイト、講義形式、およびライブ オンラインで受講できます。オンサイトのパイロット プログラムと実装のベスト プラクティスでは、VMware

コンサルティング サービスにより、お客様の仮想環境の評価、計画、構築、管理に役立つ情報を提供しています。教育トレーニング、認定プログラム、およびコンサルティング サービスの情報については、<http://www.vmware.com/services> をご覧ください。

# vShield への手引き

---

この章では、インストールする VMware® vShield™ コンポーネントを紹介します。

この章では次のトピックについて説明します。

- [vShield コンポーネントの概要 \(P. 7\)](#)
- [導入シナリオ \(P. 10\)](#)

## vShield コンポーネントの概要

VMware vShield は VMware vCenter™ Server 統合のために作られたセキュリティ仮想アプライアンススイートです。vShield は外部からの攻撃や不正使用から仮想データセンターを守り、法的遵守の目的を達成するための、クリティカルセキュリティコンポーネントです。

vShield には仮想マシンを保護するために必要不可欠な仮想アプライアンスとサービスが含まれています。vShield はウェブベースのユーザーインターフェイス、vSphere Client プラグイン、コマンドラインインターフェイス (CLI)、そして REST API から設定可能です。

vCenter Server には vShield Manager が含まれます。以下の vShield パッケージでは各ライセンスが必要です：

- vShield App
- Data Security を含む vShield App
- vShield Edge
- vShield Endpoint

1 つの vShield Manager は、複数の vShield App、vShield Edge、vShield Endpoint、および vShield Data Security インスタンスを管理できます。

- [vShield Manager \(P. 8\)](#)

vShield Manager は、vShield の一元化されたネットワーク管理コンポーネントで、vCenter Server 環境内の ESX™ ホスト上に仮想アプライアンスとしてインストールされます。vShield Manager は vShield エージェントとは別の ESX ホスト上で実行できます。

- [vShield App \(P. 8\)](#)

vShield App はハイパーバイザーに基づくファイアウォールであり、仮想データセンター内のアプリケーションをネットワークを介した攻撃から保護します。組織は、仮想マシン間のネットワーク通信を監視して制御することができます。IP アドレスなどの物理構造だけでなく、VMware vCenter™ コンテナや vShield セキュリティグループなどの論理構造に基づく、アクセス制御ポリシーを作成できます。また、IP アドレスの柔軟な設定によって、同じ IP アドレスを複数のテナントゾーンで使用できるため、プロビジョニングが簡素化されます。

- **vShield Edge** (P. 9)

vShield Edge は、ポート グループ、vDS ポート グループ、または Cisco Nexus 1000V 内の仮想マシンを分離するためのネットワーク エッジ セキュリティとゲートウェイ サービスを提供します。vShield は分離されたスタブ ネットワークを、DHCP、VPN、NAT とロード バランシングを用いて共有された（アップリンクの）ネットワークへ接続します。よくある vShield Edge の導入には、vShield Edge が Virtual Datacenters (VDCs) のためにペリメータ セキュリティを提供する、DMZ、VPN エクストラネット、そしてマルチ テナントのクラウド環境などが含まれます。

- **vShield Endpoint** (P. 10)

vShield Endpoint は、アンチウイルスおよびアンチマルウェア エージェントの負荷を、VMware パートナーが提供する、専用のセキュアな仮想アプライアンスに移して軽くします。セキュアな仮想アプライアンスは（ゲスト仮想マシンとは異なり）オフラインになることはないので、アンチウイルス シグネチャを継続的に更新することができます。また、新しい仮想マシン（またはオフラインになっていた既存の仮想マシン）は、オンラインになった時点で、最も新しいアンチウイルス シグネチャにより即座に保護されます。

- **vShield Data Security** (P. 10)

vShield Data Security は、組織の仮想化されたクラウド環境内に格納されている機密データを表示できるようにします。vShield Data Security でアクセス違反が報告されるため、機密データの適切な保護や、世界各地の規制へのコンプライアンスの評価が可能になります。

## vShield Manager

vShield Manager は、vShield の一元化されたネットワーク管理コンポーネントで、vCenter Server 環境内の ESX™ ホスト上に仮想アプライアンスとしてインストールされます。vShield Manager は vShield エージェントとは別の ESX ホスト上で実行できます。

vShield Manager ユーザー インターフェイスまたは vSphere Client プラグイン、管理者インストール、構成、そして vShield コンポーネントの管理を使用します。vShield Manager ユーザー インターフェイスは vSphere Client インベントリ パネルのコピーを表示するために VMware Infrastructure SDK を活用し、また Hosts & Clusters と Networks ビューを含みます。

## vShield App

vShield App はハイパーバイザーに基づくファイアウォールであり、仮想データセンター内のアプリケーションをネットワークを介した攻撃から保護します。組織は、仮想マシン間のネットワーク通信を監視して制御することができます。IP アドレスなどの物理構造だけでなく、VMware vCenter™ コンテナや vShield セキュリティ グループなどの論理構造に基づく、アクセス制御ポリシーを作成できます。また、IP アドレスの柔軟な設定によって、同じ IP アドレスを複数のテナントゾーンで使用できるため、プロビジョニングが簡素化されます。

VMware vMotion が機能し、仮想マシンが ESX ホスト間で移動する際に仮想マシンの保護が維持されるようにするには、vShield App をクラスタ内のすべての ESX ホスト上にインストールする必要があります。既定では、vShield App 仮想アプライアンスを vMotion を使用して移動させることはできません。

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



## vShield Edge

vShield Edge は、ポート グループ、vDS ポート グループ、または Cisco Nexus 1000V 内の仮想マシンを分離するためのネットワーク エッジ セキュリティとゲートウェイ サービスを提供します。vShield は分離されたスタブ ネットワークを、DHCP、VPN、NAT とロード バランシングを用いて共有された（アップリンクの）ネットワークへ接続します。よくある vShield Edge の導入には、vShield Edge が Virtual Datacenters (VDCs) のためにペリメータ セキュリティを提供する、DMZ、VPN エクストラネット、そしてマルチ テナントのクラウド環境などが含まれます。

### 標準的な vShield Edge サービス（Cloud Director を含む）

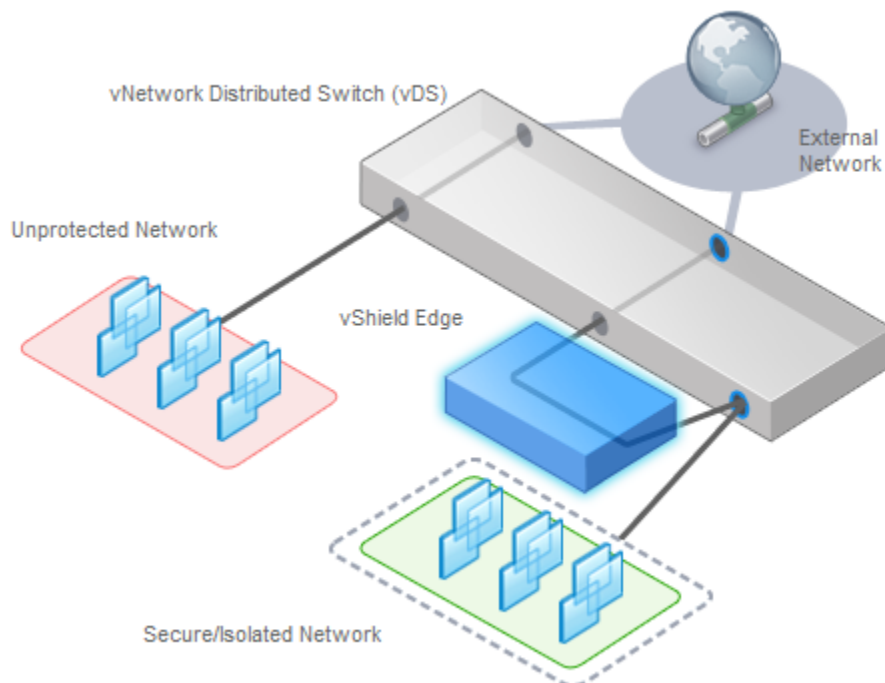
<b>ファイアウォール</b>	サポートするルールには、TCP、UDP、ICMP のステートフル インспекションのための、IP とポート レンジを用いた 5 個組みの IP 構成があります。
<b>ネットワーク アドレス変換</b>	送信元と送信先の IP アドレスや、TCP と UDP ポート変換のための管理を分離します。
<b>DHCP (Dynamic Host Configuration Protocol)</b>	IP プール、ゲートウェイ、DNS サーバ、検索ドメインの構成します。

### アドバンスド vShield Edge サービス

<b>サイト間 VPN (Virtual Private Network)</b>	全ての大手ファイアウォール ベンダーと相互運用できる、標準化された IPsec プロトコル設定を使用します。
<b>ロード バランシング</b>	シンプルで動的に構成できる仮想 IP アドレスとサーバ グループです。

vShield Edge は全てのサービスで Syslog のリモート サーバへのエクスポートをサポートしています。

図 1-1. vDS ポート グループの保護のためにインストールされた vShield Edge

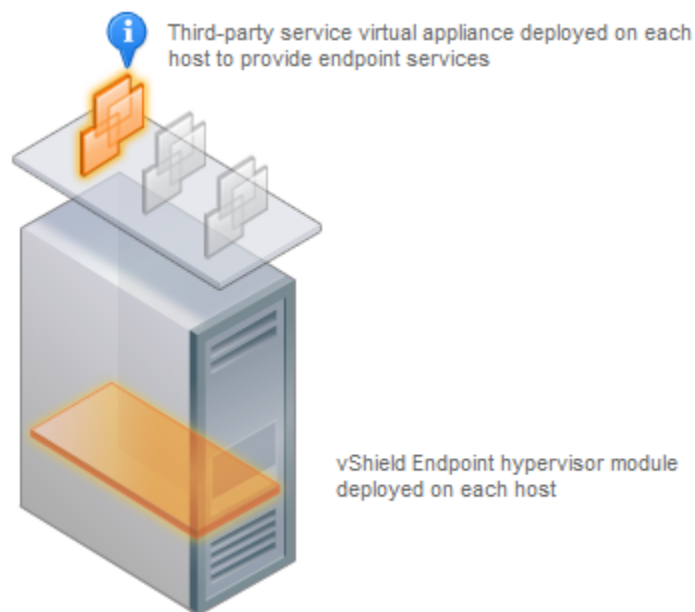


## vShield Endpoint

vShield Endpoint は、アンチウイルスおよびアンチマルウェア エージェントの負荷を、VMware パートナーが提供する、専用のセキュアな仮想アプライアンスに移して軽くします。セキュアな仮想アプライアンスは（ゲスト仮想マシンとは異なり）オフラインになることはないため、アンチウイルス シグネチャを継続的に更新することができ、ホスト上の仮想マシンに対して中断されることなく保護を提供することができます。また、新しい仮想マシン（またはオフラインになっていた既存の仮想マシン）は、オンラインになった時点で、最も新しいアンチウイルス シグネチャにより即座に保護されます。

vShield Endpoint はハイパーバイザー モジュールとして、また ESX ホスト上のサードパーティ アンチウイルス ベンダー（VMware パートナー）からのセキュリティ仮想アプライアンスとして、インストールされます。ハイパーバイザーは外部からゲスト仮想マシンをスキャンするので、各仮想マシンにエージェントをインストールする必要はありません。これにより、vShield Endpoint は、メモリ使用を最適化しながらリソースのボトルネックを避けることができます。

図 1-2. ESX ホスト上にインストールされた vShield Endpoint



## vShield Data Security

vShield Data Security は、組織の仮想化されたクラウド環境内に格納されている機密データを表示できるようにします。vShield Data Security でアクセス違反が報告されるため、機密データの適切な保護や、世界各地の規制へのコンプライアンスの評価が可能になります。

## 導入シナリオ

vShield を用いて、様々な仮想マシンの導入のためのセキュアなゾーンを構築できます。特定のアプライアンス、ネットワーク セグメンテーション、またはカスタマイズされた法的遵守要因に合わせて、仮想マシンを分離できます。ゾーニング ポリシーを規定した後は、その各ゾーンへのアクセス ルールを強化するために vShield を導入できます。

- [DMZ の保護](#) (P. 11)

DMZ は混合信頼ゾーンです。クライアントはウェブや E メールサービスのためにインターネットから入り、DMZ 内のサービスは内部ネットワークの内側のサービスへのアクセス許可を要求します。

- **内部ネットワークの分離と保護 (P. 11)**

vShield Edge を使用して、内部ネットワークを外部ネットワークから分離することができます。vShield Edge はポート グループ内の仮想マシンを保護するためにペリメータ ファイアウォール保護とエッジ サービスを提供し、DHCP、NAT、VPN 経由での外部ネットワークへの通信を可能にします。

- **クラスタ内での仮想マシンの保護 (P. 12)**

vShield App を使用してクラスタ内の仮想マシンを保護することができます。

- **よくある vShield Edge の導入 (P. 12)**

NAT を使用してネットワーク トラフィックの出入りを許可して、vShield Edge を使ってスタブ ネットワークを分離できます。内部スタブ ネットワークを導入する場合は、vShield Edge の VPN トンネル経由での LAN 間暗号化を用いてネットワーク間の通信を保護することができます。

- **よくある vShield App の導入 (P. 12)**

vShield App を用いて vDC 内のセキュリティ ゾーンを作成できます。vCenter コンテナまたは Security Groups に対してファイアウォール ポリシーを適用することができます。Security Groups は vShield Manager ユーザー インターフェイスを使って作成できるカスタマイズ可能なコンテナです。コンテナ ベースのポリシーにより混合信頼ゾーン クラスタを物理的な外部ファイアウォールの必要なしに作成することができます。

## DMZ の保護

DMZ は混合信頼ゾーンです。クライアントはウェブや E メールサービスのためにインターネットから入り、DMZ 内のサービスは内部ネットワークの内側のサービスへのアクセス許可を要求します。

DMZ 仮想マシンをポート グループ内に設置し、ポート グループを vShield Edge で保護することができます。vShield Edge はファイアウォール、NAT、VPN や、DMZ サービスを保護するためのロードバランシングなどのアクセス サービスを提供します。

内部サービスが必要な DMZ サービスのよくある例が Microsoft Exchange です。Microsoft Outlook Web Access (OWA) は通常 DMZ クラスタの中に置かれますが、Microsoft Exchange のバックエンドは内部クラスタの中に置かれます。内部クラスタ上では、DMZ からの決まった送信元/先パラメータを用いて特定することにより、Exchange 関連のリクエストのみを受け付けるファイアウォール ルールを作成することができます。DMZ クラスタからは、外部からの DMZ へのアクセスを HTTP、FTP、または SMTP を用いて特定の送信先へのみ許可するというルールを作成できます。

## 内部ネットワークの分離と保護

vShield Edge を使用して、内部ネットワークを外部ネットワークから分離することができます。vShield Edge はポート グループ内の仮想マシンを保護するためにペリメータ ファイアウォール保護とエッジ サービスを提供し、DHCP、NAT、VPN 経由での外部ネットワークへの通信を可能にします。

保護されたポート グループ内では、各 ESX ホスト上の vShield App インスタンスをインストールできます。vDS は ESX ホストをカバーし内部ネットワーク内の仮想マシン間通信を保護します。

VLAN タグをセグメント トラフィック用に最適化すれば、App ファイアウォールを用いてさらに効果的なアクセス ポリシーを作成できます。物理的なファイアウォールの代わりに App ファイアウォールを用いることで、共有された ESX クラスタ内の信頼ゾーンを閉じたり混合させたりできます。これにより、分離され断片化したクラスタになる代わりに、理想的な最適化と DRS と HA などの機能からの統合が得られます。全体として、単一のプールとしての ESX 導入は個別に管理されたプールよりも簡単に管理できます。

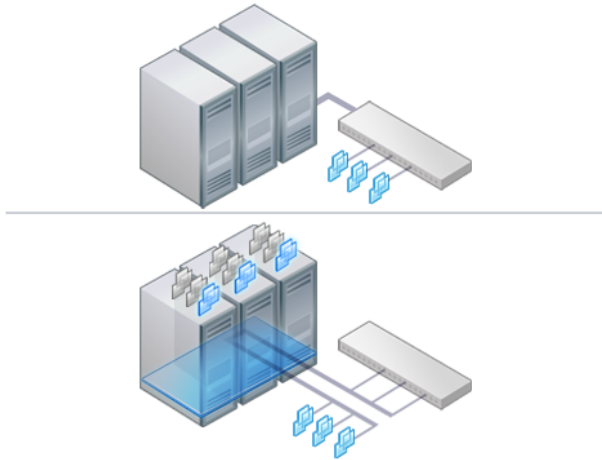
例えば、VLAN を論理的、組織的、またはネットワーク境界をベースとして仮想マシン ゾーンを分割し、使うことができます。Virtual Infrastructure SDK を活用することで、vShield Manager インベントリ パネルが Networks ビューの下に現在の VLAN ネットワークを表示します。各 VLAN ネットワークの仮想マシンへのアクセス ルールを設定し、タグのないトラフィックをこれらの仮想マシンへ選り分けておくことができます。

## クラスタ内での仮想マシンの保護

vShield App を使用してクラスタ内の仮想マシンを保護することができます。

図 1-3 では、vShield App インスタンスはクラスタ内の各 ESX にインストールされています。仮想マシンは vMotion™ または DRS 経由でクラスタ内の ESX ホスト間を移動する際保護されます。各 vApp はすべての転送ステータスを共有し、維持します。

図 1-3. クラスタ内の各 ESX ホストにインストールされた vShield App インスタンス



## よくある vShield Edge の導入

NAT を使用してネットワーク トラフィックの出入りを許可して、vShield Edge を使ってスタブ ネットワークを分離できます。内部スタブ ネットワークを導入する場合は、vShield Edge の VPN トンネル経由での LAN 間暗号化を用いてネットワーク間の通信を保護することができます。

vShield Edge は VMware Cloud Director 内のセルフ サービス アプリケーションとして導入することができます。

## よくある vShield App の導入

vShield App を用いて vDC 内のセキュリティ ゾーンを作成できます。vCenter コンテナまたは Security Groups に対してファイアウォール ポリシーを適用することができます。Security Groups は vShield Manager ユーザー インターフェイスを使って作成できるカスタマイズ可能なコンテナです。コンテナ ベースのポリシーにより混合信頼ゾーン クラスタを物理的な外部ファイアウォールの必要なしに作成することができます。

vDC を使用しない導入の場合は、信頼ゾーンの作成とアクセス ポリシーの強化のために vShield App の Security Groups 機能を使用してください。

Service Provider Admin は内部ネットワークのすべてのゲスト仮想マシンに適用する、幅広いファイアウォール ポリシー賦課に vShield App を使用できます。例えば、すべてのゲスト仮想マシンの第二 vNIC にファイアウォール ポリシーを設け、ストレージ サーバーへのアクセスを許可しつつ、他のすべての仮想マシンからの仮想マシンへのアドレス指定をブロックするという事もできます。

## インストールの準備

この章では、vShield のインストールを成功させるための必要条件について紹介します。

この章では次のトピックについて説明します。

- システム要件 (P. 13)
- 導入にあたって考慮すべき事柄 (P. 14)

### システム要件

vShield を vCenter Server 環境にインストールする前に、ネットワーク構成とリソースを考慮してください。1 つの vCenter Server につき 1 つの vShield Manager、1 つの ESX™ ホストにつき 1 つの vShield App または vShield Endpoint、1 つのポート グループにつき 1 つの vShield Edge をインストールできます。

### ハードウェア

表 2-1. ハードウェア要件

コンポーネント	最小
メモリ	vShield の全コンポーネント用に 8GB
ディスク スペース	<ul style="list-style-type: none"> <li>■ vShield Manager 用に 8GB</li> <li>■ ESX ホスト・vShield App につき 5GB</li> <li>■ vShield Edge につき 200MB</li> <li>■ vShield Data Security 用に、ESX ホストにつき 6GB</li> </ul>
NIC	vShield の全コンポーネント用に、ESX ホスト上の 2 ギガビットの NIC

### 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) の製品の相互運用性マトリクスを参照してください。

VMware 製品には最小必要バージョンがあります。

- VMware vCenter Server 4.0 Update 2 またはそれ以降
- 各サーバーに VMware ESX 4.0 Update 2 またはそれ以降

**注意** vShield Endpoint および vShield Data Security には、ESXi 5.0 Patch 1 およびそれ以降、または ESXi 4.1 Patch 3 およびそれ以降が必要です。

- VMware Tools

vShield Endpoint および vShield Data Security 用には、仮想マシンのハードウェア バージョンを 7 または 8 にアップグレードし、ESXi 5.0 Patch 1 とともにリリースされている VMware Tools 8.6.0 をインストールする必要があります。詳細は「[ゲスト仮想マシンへの VMware Tools のインストール \(P. 26\)](#)」を参照してください。

- VMware vCloud Director 1.0 またはそれ以降
- VMware View 4.5 またはそれ以降

## クライアントとユーザー アクセス

- VMware vSphere Client がインストールされた PC

---

**注意** vSphere インベントリに名前が ESX ホストを追加した場合は、DNS 名が提供されていることを確認してください。DNS 名が提供されていない場合は、vShield Manager が IP アドレスを解決できません。

---

- 仮想マシンを追加、電源オンする許可
- 仮想マシンのファイルを保存してあ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できるアカウント許可
- vShield Manager ユーザー インターフェイスにアクセスするためのウェブ ブラウザのクッキーの有効化
- ESX ホストからアクセス可能な vShield Manager ポート 443。このポートは、ESX ホストから OVF ファイルをダウンロードして導入するために必要です。
- 以下のサポートするウェブ ブラウザのうちいずれかを用いての vShield Manager への接続：
  - Internet Explorer 6.x かそれ以降
  - Mozilla Firefox 1.x かそれ以降
  - Safari 1.x か 2.x

## 導入にあたって考慮すべき事柄

vShield コンポーネントを導入する前に、以下の推奨と制限を考慮してください。

- [vShield Protection のための仮想マシンの用意 \(P. 15\)](#)  
vShield で仮想マシンをどのように保護するか決定する必要があります。ベスト プラクティスとして、vShield App、vShield Endpoint、および vShield Data Security 用のリソース プール内のすべての ESX ホストを、使用する vShield コンポーネントに合わせて準備しておいてください。また、仮想マシンをハードウェア バージョン 7 または 8 にアップグレードしておく必要もあります。
- [vShield Manager のアップタイム \(P. 15\)](#)  
vShield Manager は、度重なる再起動やメンテナンス モードでの運用などのダウンタイムに影響されない ESX ホスト上で運用する必要があります。vShield Manager の耐性を高めるためには HA や DRS が使用できます。vShield Manager の搭載された ESX ホストにダウンタイムが予想される場合は、vShield Manager 仮想アプライアンスを他の ESX ホストに vMotion します。このため、ESX ホストは 1 台以上設置することが推奨されます。
- [vShield コンポーネント間の通信 \(P. 15\)](#)  
vShield コンポーネントの管理インターフェイスは、vSphere 管理ネットワークなどの一般的なネットワーク上に置いてください。vShield Manager は、vCenter Server、vShield App および vShield Edge インスタンス、vShield Endpoint モジュール、および vShield Data Security 仮想マシンと接続できることを必要とします。vShield コンポーネントは、ルーター接続上でも、また異なる LAN でも通信できます。
- [vShield 仮想マシンの堅牢化 \(P. 15\)](#)  
vShield Manager と他の vShield コンポーネントにはウェブ ベースでのユーザー インターフェイス、コマンドライン インターフェイス、REST API を用いてアクセスできます。vShield にはこれらのアクセス オプションのための既定のログイン証明書が含まれます。各 vShield 仮想マシンのインストール後、既定のログイン信用書を変更することによりアクセスを堅牢化することができます。vShield Data Security には既定のログイン証明書が含まれない点に注意してください。

## vShield Protection のための仮想マシンの用意

vShield で仮想マシンをどのように保護するか決定する必要があります。ベスト プラクティスとして、vShield App、vShield Endpoint、および vShield Data Security 用のリソース プール内のすべての ESX ホストを、使用する vShield コンポーネントに合わせて準備しておいてください。また、仮想マシンをハードウェア バージョン 7 または 8 にアップグレードしておく必要もあります。

以下の質問について考慮してください：

### どのように仮想マシンをグループ化するか？

セキュリティとアクセス ルール設定を簡単にするためには、機能、部門、あるいはその他の組織の必要により仮想マシンのグループ化するために仮想マシンを vDS 上のポート グループや別の ESX ホストに移動することを考える必要があります。外部ネットワークから仮想マシンを分離するためにすべてのポート グループのペリメータに vShield Edge をインストールすることができます。ESX ホスト上に vShield App をインストールし、リソースの重要度によりルールを強化するためにコンテナ リソース毎にファイアウォール ポリシーを設定できます。

### 仮想マシンを他の ESX ホストに vMotion で移動した場合、仮想マシンは引き続き保護されるのか？

はい、リソース プール内でホストが準備されていれば、セキュリティの状態を弱めることなく、ホスト間でマシンを移動することができます。ESX ホストを準備する方法の詳細については、[すべてのESXホストの準備\(P.22\)](#) を参照してください。

## vShield Manager のアップタイム

vShield Manager は、度重なる再起動やメンテナンス モードでの運用などのダウンタイムに影響されない ESX ホスト上で運用する必要があります。vShield Manager の耐性を高めるためには HA や DRS が使用できます。vShield Manager の搭載された ESX ホストにダウンタイムが予想される場合は、vShield Manager 仮想アプライアンスを他の ESX ホストに vMotion します。このため、ESX ホストは 1 台以上設置することが推奨されます。

## vShield コンポーネント間の通信

vShield コンポーネントの管理インターフェイスは、vSphere 管理ネットワークなどの一般的なネットワーク上に置いてください。vShield Manager は、vCenter Server、vShield App および vShield Edge インスタンス、vShield Endpoint モジュール、および vShield Data Security 仮想マシンと接続できることを必要とします。vShield コンポーネントは、ルーター接続上でも、また異なる LAN でも通信できます。

VMware では、vShield Manager の管理下にある環境とは異なる vCenter 環境に vShield Manager をインストールすることをお勧めしています。それぞれの vShield Manager が 1 つの vCenter Server 環境を管理します。



**注意** vCenter は、それを管理している vShield App の保護下にあるホスト上では動作しないという点を確認してください。

## vShield 仮想マシンの堅牢化

vShield Manager と他の vShield コンポーネントにはウェブ ベースでのユーザー インターフェイス、コマンドライン インターフェイス、REST API を用いてアクセスできます。vShield にはこれらのアクセス オプションのための既定のログイン証明書が含まれます。各 vShield 仮想マシンのインストール後、既定のログイン信用書を変更することによりアクセスを堅牢化することができます。vShield Data Security には既定のログイン証明書が含まれない点に注意してください。

- [vShield Manager ユーザー インターフェイス \(P. 16\)](#)

ウェブ ブラウザのウィンドウを開き、vShield Manager の管理ポートの IP アドレスに進むことにより vShield Manager ユーザー インターフェイスにアクセスできます。



- [コマンドライン インターフェイス \(P. 16\)](#)

vSphere Client コンソール セッション経由でコマンドライン インターフェイスを使用し、vShield Manager、vShield App、vShield Edge 仮想アプライアンスにアクセスできます。vShield Endpoint 仮想アプライアンスにアクセスする方法については、アンチウイルス ソリューション プロバイダーから提供された説明書を参照してください。コマンドライン インターフェイスから vShield Data Security 仮想マシンにアクセスすることはできません。

- [REST リクエスト \(P. 16\)](#)

すべての REST API リクエストは vShield Manager の確認を要求します。

## vShield Manager ユーザー インターフェイス

ウェブ ブラウザのウィンドウを開き、vShield Manager の管理ポートの IP アドレスに進むことにより vShield Manager ユーザー インターフェイスにアクセスできます。

既定のユーザー アカウント、管理者は vShield Manager へのグローバルアクセス権限を持っています。最初のログインの後、管理者ユーザー アカウントの既定パスワードを変更してください。[「vShield Manager ユーザー インターフェイスのデフォルトのアカウントのパスワードの変更 \(P. 20\)」](#)を参照してください。

## コマンドライン インターフェイス

vSphere Client コンソール セッション経由でコマンドライン インターフェイスを使用し、vShield Manager、vShield App、vShield Edge 仮想アプライアンスにアクセスできます。vShield Endpoint 仮想アプライアンスにアクセスする方法については、アンチウイルス ソリューション プロバイダーから提供された説明書を参照してください。コマンドライン インターフェイスから vShield Data Security 仮想マシンにアクセスすることはできません。

各仮想アプライアンスは vShield Manager ユーザー インターフェイス と同様、既定のユーザー名 (**admin**) とパスワード (**default**) の組み合わせを使います。Enabled モードに入るにもパスワード **default** を使います。

CLI の堅牢化について詳しくは、vShield コマンドライン インターフェイス リファレンスを参照してください。

## REST リクエスト

すべての REST API リクエストは vShield Manager の確認を要求します。

Base 64 エンコーディングを使用すれば、ユーザー名:パスワードというフォーマットで、ユーザー名とパスワードの組み合わせを識別することができます。リクエストを実行するには特権のアクセス権で vShield Manager ユーザー インターフェイス アカウント (ユーザー名とパスワード) を使用する必要があります。REST API リクエストの確認の詳細については、vShield API プログラミング ガイドを参照してください。



## vShield Manager のインストール

---

VMware vShield は vCenter Server 仮想インフラストラクチャを保護するために、ファイアウォール保護、トラフィック分析、ネットワーク ペリメータ サービスを提供します。vShield 仮想アプライアンスのインストールはほとんどの仮想データセンターで自動化されています。

vShield Manager は vShield の集中管理コンポーネントです。vShield Manager は vShield App、vShield Endpoint、vShield Edge インスタンスを監視し、構成を適用するのに用いられます。vShield Manager は ESX ホスト上で仮想アプライアンスとして稼働します。

VMware vShield は VMware ESX 4.0 と 4.1 に含まれています。基本的な VMware vShield パッケージには vShield Manager と vShield App が含まれます。トラフィックを IP アドレス間の通信ベースで監視するための vShield App ファイアウォール ルールのセットを構成できます。

vShield Manager は複数の段階を経てのインストールします。vShield Manager のインストールを成功させるには下記の手順通りに進める必要があります。

vShield App、vShield Endpoint、vShield Edge のライセンスを取得して、ネットワーク セキュリティを強化することができます。

この章では次のトピックについて説明します。

- [vShield Manager OVA ファイルの取得 \(P. 17\)](#)
- [vShield Manager 仮想アプライアンスのインストール \(P. 17\)](#)
- [vShield Manager のネットワーク設定の構成 \(P. 18\)](#)
- [vShield Manager ユーザー インターフェイスへのログイン \(P. 19\)](#)
- [vShield Manager と vCenter Server の同期 \(P. 19\)](#)
- [vSphere Client への vShield Manager プラグインの登録 \(P. 20\)](#)
- [vShield Manager ユーザー インターフェイスのデフォルトのアカウントのパスワードの変更 \(P. 20\)](#)

### vShield Manager OVA ファイルの取得

vShield Manager 仮想マシンは OVA (Open Virtualization Appliance) としてパッケージされており、vSphere Client を使ってデータストアと仮想マシン インベントリに vShield Manager をインポートすることができます。

### vShield Manager 仮想アプライアンスのインストール

DRS により構成されたクラスタ内の ESX ホスト上に vShield Manager 仮想マシンをインストールします。

vShield 5.0 およびそれ以降では、vShield Manager との相互運用性を保つ vCenter とは異なる vCenter に vShield Manager をインストールできます。1 つの vShield Manager は 1 つの vCenter Server 環境をサービスします。

vShield Manager 仮想マシン インストールには VMware Tools が含まれます。vShield Manager 上で VMware Tools をアップグレードしたり、インストールしたりしないでください。

#### 手順

- 1 vSphere Client にログインします。
  - 2 vShield Manager の管理インターフェイスのホームとなるポート グループを作成します。  
vShield Manager 管理インターフェイスは、vShield Edge、vShield App、vShield Endpoint インスタンスのすべての機能からアクセス可能である必要があります。
- 
- 注意** vShield Manager 管理インターフェイスを Service Console と VMkernel と同じポート グループに保存しないでください。
- 
- 3 [File] - [Deploy OVF Template] を選択します。
  - 4 [Deploy from file] をクリックし、[Browse] をクリックして、PC 内の vShield Manager OVA ファイルが含まれているフォルダを指定します。
  - 5 インストールを終了します。  
vShield Manager がインベントリ内に仮想マシンとしてインストールされました。
  - 6 vShield Manager 仮想マシンの電源をオンにします。

## vShield Manager のネットワーク設定の構成

IP アドレスの設定、デフォルト ゲートウェイの指定、DNS 設定には vShield Manager のコマンドライン インターフェイス (CLI) を使用する必要があります。

vShield Manager が IP アドレスとホスト名解決のための DNS Server を 2 つまで指定できます。ESX ホストが、IP アドレスではなくホスト名を使って vCenter Server に追加された場合、DNS は必要となります。

#### 手順

- 1 vShield Manager 仮想マシンを右クリックし、[Open Console] をクリックして vShield Manager のコマンドライン インターフェイス (CLI) を起動します。  
起動プロセスに数分かかることがあります。
- 2 **manager login** プロンプトが表示された後、既定のユーザー名 **admin** とパスワード **default** を用いて CLI にログインします。
- 3 パスワード **default** で Enabled モードに入ります。  
**manager> enable Password:**  
**manager#**
- 4 **setup** コマンドを実行して、[CLI setup] ウィザードを起動します。  
[CLI setup] ウィザードで、vShield Manager 管理インターフェイス用の IP アドレスと、デフォルト ネットワーク ゲートウェイを識別するための IP アドレスを割り当てます。管理インターフェイスの IP アドレスは、すべてのインストールされた vShield App、vShield Edge、vShield Endpoint インスタンス、さらにシステム管理用のウェブ ブラウザからもアクセス可能でなければなりません。  
**manager# setup**

Use CTRL-D to abort configuration dialog at any prompt.  
Default settings are in square brackets '['].

IP Address (A.B.C.D):

```
Subnet Mask (A.B.C.D):
Default gateway (A.B.C.D):
Primary DNS IP (A.B.C.D):
Secondary DNS IP (A.B.C.D):
Old configuration will be lost.
Do you want to save new configuration (y/[n]):
y
```

- 5 (オプション) 以前に vShield Manager のネットワーク設定を構成している場合は、システムを再起動する必要があります。
- 6 ログアウト後、既定のユーザー名 **admin** とパスワード **default** を用いて CLI にログインし直します。
- 7 ネットワーク接続を確認するためにデフォルト ゲートウェイに Ping を送信します。  
`manager> ping A.B.C.D`
- 8 PC から、IP アドレスが届いているかを確認するため vShield Manager へ Ping を送信します。

## vShield Manager ユーザー インターフェイスへのログイン

vShield Manager 仮想マシンのインストールと構成が済んだら、vShield Manager ユーザー インターフェイスへログインします。

### 手順

- 1 Web ブラウザ ウィンドウを開き、vShield Manager に割り当てた IP アドレスを入力します。  
vShield Manager ユーザー インターフェイスが SSL を用いてウェブ ブラウザのウィンドウで開きます。
- 2 セキュリティ証明書を受け入れます。

---

**注意** SSL 承認を認証に使用できます。vShield 管理ガイド を参照してください。

---

vShield Manager のログイン画面が表示されます。

- 3 既定のユーザー名 **admin** とパスワード **default** を用いて vShield Manager ユーザー インターフェイスにログインします。  
不正な使用を避けるため、最初のタスクの1つとしてデフォルトのパスワードを変更する必要があります。 [\[vShield Manager ユーザー インターフェイスのデフォルトのアカウントのパスワードの変更 \(P. 20\)\]](#) を参照してください。
- 4 [Log In] をクリックします。

## vShield Manager と vCenter Server の同期

vShield Manager ユーザー インターフェイスの VMware インフラストラクチャ インベントリを表示するために vCenter Server と同期します。

このタスクを完了するには vCenter Server の管理者権限でのユーザー アカウントが必要です。vCenter のパスワードに非 ASCII 文字が含まれている場合は、vShield Manager と vCenter Server の同期を行う前に修正する必要があります。

---

**注意** vShield Manager 仮想マシンは vShield Manager ユーザー インターフェイスのインベントリ パネルにリソースとして表示されません。[Settings & Reports] オブジェクトがインベントリ パネル内の vShield Manager 仮想マシンに相当します。

---

### 手順

- 1 vShield Manager にログインします。
- 2 vShield Manager インベントリ パネルから [Settings & Reports] をクリックします。
- 3 [Configuration] タブをクリックします。

- 4 [vCenter] タブをクリックします。
- 5 [IP address/Name] フィールドに vCenter Server の IP アドレスまたはホスト名を入力します。
- 6 [User Name] フィールドに vSphere Client ログイン ユーザー名を入力します。
- 7 [Password] フィールドに、そのユーザー名に対応するパスワードを入力します。
- 8 [Save] をクリックします。

## vSphere Client への vShield Manager プラグインの登録

[vSphere Plug-in] オプションでは、vShield Manager を vSphere Client プラグインとして登録します。プラグインが登録された後は、vShield のオプションのほとんどを vSphere Client から設定できます。

### 手順

- 1 vShield Manager インベントリ パネルから [Settings & Reports] をクリックします。
- 2 [Configuration] タブをクリックします。
- 3 [vSphere Plug-in] をクリックします。
- 4 [Register] をクリックします。

NAT 環境では、プラグイン スクリプトのダウンロード場所を修正しなければならない場合があります。デフォルトの vShield Manager のアドレスは、<vShield\_Manager\_IP> [:443] となっています。

- 5 vSphere Client にログインしている場合は、ログアウトします。
- 6 vSphere Client にログインします。
- 7 ESX ホストを選択します。
- 8 [vShield] タブがオプションとして表示されたことを確認します。

## vShield Manager ユーザー インターフェイスのデフォルトのアカウントのパスワードの変更

vShield Manager へのアクセスのセキュリティを強化するために、管理者アカウントのパスワードを変更できます。

### 手順

- 1 vShield Manager ユーザー インターフェイスへログインします。
- 2 vShield Manager インベントリ パネルから [Settings & Reports] をクリックします。
- 3 [Users] タブをクリックします。
- 4 管理者アカウントを選択します。
- 5 [Update User] をクリックします。
- 6 新しいパスワードを入力します。
- 7 [Retype Password] フィールドにパスワードをもう一度入力して確認します。
- 8 [OK] をクリックして、変更内容を保存します。

# vShield Edge、vShield App、vShield Endpoint、および vShield Data Security のインストール

# 4

vShield Manage のインストール後に、vShield App、vShield Endpoint、vShield Edge、および vShield Data Security の各コンポーネントをアクティベートするためのライセンスを取得できます。vShield Manager OVA パッケージにはアドオン コンポーネントをインストールするためのドライバーとファイルが含まれています。vShield App ライセンスがある場合には、vShield Endpoint コンポーネントも使用することができます。

この章では次のトピックについて説明します。

- [ライセンス付与された vShield コンポーネントの評価モードでの実行 \(P. 21\)](#)
- [vShield App、vShield Edge、vShield Endpoint および vShield Data Security のための仮想インフラストラクチャの準備 \(P. 21\)](#)
- [vShield Endpoint のインストール \(P. 25\)](#)
- [vShield Data Security のインストール \(P. 27\)](#)

## ライセンス付与された vShield コンポーネントの評価モードでの実行

vShield Edge、vShield App、vShield Endpoint を購入・アクティベーションする前に、これらのソフトウェアを評価モードでインストールし試用することができます。デモと評価目的で vShield Edge、vShield App、vShield Endpoint を評価モードでインストールした場合でも、インストール後すぐに完全に使用可能となります。ライセンス設定は必要なく、アクティベートした日から 60 日間全ての機能をお使いいただけます。

評価モードでの運用中、vShield コンポーネントはインスタンスの最大数をサポートします。

60 日の試用期間後は、ライセンスをご購入されないかぎり、vShield は使用できなくなります。例えば、vShield App や vShield Edge の仮想アプライアンスをオンにできなくなる、また仮想マシンを保護できなくなります。

60 日の試用期間後使用不可となる vShield App と vShield Edge の機能を、中断や機能のリストアをせずに使い続けるには、ご購入の vShield コンポーネントにあった機能をアクティベートするライセンスファイルを取得し、インストールする必要があります。

## vShield App、vShield Edge、vShield Endpoint および vShield Data Security のための仮想インフラストラクチャの準備

アドオン コンポーネントのインストールの前に、ESX ホストと vNetwork 環境の準備が必要です。vShield App、vShield Endpoint、および vShield Data Security 機能を ESX ホストにインストールします。vShield Edge をポートグループ、vNetwork Distributed Switch (vDS) ポートグループ、または Cisco Nexus 1000V にインストールします。

## vShield コンポーネント ライセンスのインストール

これらのコンポーネントをインストールする前に、必ず vShield Edge、vShield App、vShield Endpoint をインストールしてください。これらのライセンスは、vSphere Client を用いて vShield Manager のインストールが完了した後、インストールすることができます。vShield App ライセンスがある場合には、vShield Endpoint コンポーネントも使用することができます。

### 手順

- 1 vCenter Server システムに接続している vSphere Client ホストで、[Home] - [Licensing] を選択します。
- 2 レポートビューから [Asset] を選択します。
- 3 vShield の Asset を右クリックし、[Change license key] を選択します。
- 4 [Assign a new license key] を選択し、[Enter Key] をクリックします。
- 5 ライセンスキーとキー用のラベル（オプション）を入力し、[OK] をクリックします。
- 6 [OK] をクリックします。
- 7 このステップを、ライセンス取得済みの各 vShield コンポーネントに対し繰り返してください。

## すべての ESX ホストの準備

vShield アドオンを機能させるために、vCenter 環境内のすべての ESX ホストを準備してください。

vShield 仮想アプライアンスには VMware Tools が含まれます。vShield 仮想アプライアンス上の VMware Tools ソフトウェアを変更したり、アップグレードしたりしないでください。

---

**注意** vShield App で保護している場合、仮想マシンのネットワーク接続が中断されます。vCenter Server が仮想マシン上で動作している状態でネットワークから切り離されると、vShield App のインストール プロセスが完了せずに終了する場合があります。vShield App を VMware vCenter Server 仮想マシンと同じホスト上にインストールしないでください。

---

### 開始する前に

- 各 vShield App 仮想アプライアンスの管理（MGMT）ポートのための IP アドレスがあることを確認します。各 IP アドレスは vShield Manager からアクセス可能で、vCenter と ESX ホスト管理インターフェイスのために使用される管理ネットワーク上にある必要があります。
- vShield App を保存するためのローカル ストレージまたはネットワーク ストレージ。

### 手順

- 1 vSphere Client にログインします。
- 2 インベントリ ツリーから ESX ホストを選びます。
- 3 [vShield] タブをクリックします。
- 4 セキュリティ証明書を受け入れます。
- 5 [vShield App] サービスのために [Install] をクリックします。
- 6 vShield App では以下の情報を提供してください。

オプション	説明
[Datastore]	vShield App 仮想マシンファイルを保存したいデータストアを選択します。
[Management Port Group]	vShield App の管理インターフェイスをホストするためのポート グループを選択します。このポート グループは vShield Manager のポート グループへのアクセスが必要です。

オプション	説明
[IP Address]	vShield App の管理インターフェイスに割り当てる IP アドレスを入力します。
[Netmask]	割り当てた IP アドレスに関連する IP サブネット マスクを入力します。
[Default Gateway]	デフォルト ネットワーク ゲートウェイの IP アドレスを入力します。

7 [vShield Endpoint] チェックボックスを選択します。

8 [Install] をクリックします。

vSphere Client 画面の [最近のタスク] ペインから vShield App のインストールの進捗状況を確認できます。

9 全てのコンポーネントのインストール後、以下の手順を実行してください：

- vShield App：この段階で、vShield App のインストールは完了しています。データセンター、クラスタ、またはポート グループ コンテナ レベルで [vShield App] - [App Firewall] タブに進み、ファイアウォールのルールを構成します。各 vShield App は vShield Manager で設定されたグローバル ファイアウォールのルールを引き継ぎます。既定ではファイアウォールは全てのトラフィックが通過できる設定になっています。トラフィックを明示的にブロックするためにはブロックルールを設定しなければなりません。App Firewall ルールを設定するには、vShield 管理ガイドを参照してください。

**注意** ステートレス ESX 上に vShield App をインストールした場合は、ホストを再起動する前に「[ステートレス ESX ホストへの vShield App のインストール \(P. 23\)](#)」の手順に従ってください。



**注意** vCenter クライアントを通じてサービス仮想マシンを修正しないでください。これによって vShield Manager と vShield App との通信が切断され、ネットワークのセキュリティが損なわれる場合があります。

- vShield Endpoint：インストールを完了するには、「[vShield Endpoint のインストール \(P. 25\)](#)」を参照してください。
- vShield Data Security：インストールを完了するには、「[vShield Data Security のインストール \(P. 27\)](#)」を参照してください。

#### 次に進む前に

すべてのコンポーネントがインストールされたら、以下のタスクのいずれか 1 つを実行します。

- vShield App。この段階で、vShield App のインストールは完了しています。データセンター、クラスタ、またはポート グループ コンテナ レベルで [vShield App] - [App Firewall] タブを選択し、ファイアウォールのルールを構成します。各 vShield App は vShield Manager で設定されたグローバル ファイアウォールのルールを引き継ぎます。既定ではファイアウォールは全てのトラフィックが通過できる設定になっています。トラフィックを明示的にブロックするためにはブロックルールを設定しなければなりません。App Firewall ルールを設定するには、vShield 管理ガイドを参照してください。

**注意** ステートレス ESX server 上に vShield App をインストールした場合は、ホストを再起動する前に「[ステートレス ESX ホストへの vShield App のインストール \(P. 23\)](#)」の手順に従ってください。

- vShield Endpoint：インストールを完了するには、「[vShield Endpoint のインストール \(P. 25\)](#)」を参照してください。
- vShield Data Security：インストールを完了するには、「[vShield Data Security のインストール \(P. 27\)](#)」を参照してください。

## ステートレス ESX ホストへの vShield App のインストール

vShield App をステートレス ESX ホスト上にインストールする場合は、以下の手順を実行した後で vShield App をインストールした ESX ホストを再起動してください。

#### 開始する前に

- ステートレス ESX ホストへの vShield App のインストール。

- VIB によるホスト上のファイアウォール構成の変更が完了していることを確認します。
  - a vCenter クライアントで、インベントリ パネルからステートレス ESX ホストを選択します。
  - b [Configuration] タブをクリックします。
  - c ファイアウォール パネルの下の受信接続に DVFilter のエントリが表示されることを確認します。 DVFilter エントリが表示されない場合は、[Refresh] をクリックします。
- ホスト プロファイルを作成します。詳細については、『vSphere インストールおよびセットアップガイド』を参照してください。

#### 手順

- 1 ホスト プロファイルを編集します。
  - a vCenter クライアントで、[Home] - [Management] - [Host Profiles] を選択します。
  - b 編集するプロファイルを選択します。
  - c [Edit Host Profile] をクリックします。
  - d [Networking Configuration] - [Host Port Group] - [vmervice-vmknic-pg] - [IP address settings] - [How is IPv4 address determined] を選択します。
  - e IP アドレスに **169.254.1.1**、サブネット マスクに **255.255.255.0** と入力します。
  - f [Networking Configuration] - [Host Port Group] - [vmervice-vmknic-pg] - [Determine how MAC address for vmknic should be decided] を選択します。
  - g [User must explicitly choose the policy option] を選択します。
- 2 ホスト プロファイルを保存します。
- 3 ウェブブラウザで、<https://vsm-ip/bin/offline-bundles/VMware-vShield-fastpath-esx5x-5.0.1-556798.zip> と入力し、zip ファイルをダウンロードします。
- 4 手順 1 で作成したホスト プロファイルと 手順 3 でダウンロードしたオフライン バンドルを使用し、ステートレス ESX 構成をアップデートします。

## vShield Edge のインストール

各 vShield Edge 仮想アプライアンスには外部と内部のネットワーク インターフェイスがあります。内部インターフェイスは保護されたポート グループに接続され、ポート グループ内の全ての保護された仮想マシンのためのゲートウェイとして機能します。内部インターフェイスに割り当てられたサブネットは RFC 1918 専用スペースにもなります。vShield Edge の外部インターフェイスは社内共有ネットワークやアクセス レイヤー ネットワーキングを提供するサービスにアクセスするアップリンク ポート グループに接続します。

各 vShield Edge には最低 1 つ、または外部インターフェイスの数だけ IP アドレスが必要です。ロードバランサー、サイト間 VPN、NAT サービスのための複数外部 IP アドレスは設定変更できます。内部インターフェイスは、他の vShield Edge の保護されたポート グループと重なり合う、プライベート IP アドレス ブロックを持つことができます。

vShield Edge はポート グループ、vDS ポート グループ、Cisco<sup>®</sup> Nexus 1000V ごとに 1 つインストールできます。

DRS と HA が有効の場合、vShield Edge は動的に移動されます。

#### 手順

- 1 vSphere Client にログインします。
- 2 [表示] - [インベントリ] - [ネットワーク] に進みます。
- 3 vDS 上でポート グループを作成します。  
このポート グループは内部ポート グループです。
- 4 テナントのゲスト仮想マシンを内部ポート グループに移動します。



- 5 新しい内部ポート グループを選択します。
- 6 [Edge] タブをクリックします。
- 7 [Network Interfaces] では以下の情報を入力してください。

オプション	説明
<b>外部</b>	
ポート グループ	vDS 内の外部ポート グループを選択します。このポート グループは物理 NIC をホームとし、外部ネットワークに接続されます。
IP アドレス	外部ポート グループの IP アドレスを入力します。
サブネットマスク	指定した外部 IP アドレスに関連する IP サブネットマスクを入力します。
デフォルト ゲートウェイ	デフォルト ネットワーク ゲートウェイの IP アドレスを入力します。
<b>内部</b>	
ポート グループ	選択された内部ポート グループです。
IP アドレス	内部ポート グループの IP アドレスを入力します。
サブネットマスク	指定した内部 IP アドレスに関連する IP サブネットマスクを入力します。

- 8 [Edge deployment resource selection] に以下の情報を入力します。

オプション	説明
[Resource Pool]	複数のリソース プールにまたがる dvPort Group 上に vShield Edge をインストールする場合は、vShield Edge を配置するリソース プールを選択します。選択したポート グループが 1 つのリソース プール上にある場合は、リソース プール IP が自動的に入力されます。
[Host]	複数のホストにまたがる dvPort Group 上に vShield Edge をインストールする場合は、データストアの置いてある ESX ホストを選択します。選択したポート グループが 1 つのホスト上にある場合は、ホスト IP が自動的に入力されます。
[Datastore]	vShield Edge 仮想マシンファイルを保存したいデータストアを選択します。

- 9 [Intstall] をクリックします。

インストール完了後、保護されたポート グループ内の仮想マシンを保護するためにサービスとファイアウォール ルールを設定します。vShield Edge を設定するには、vShield 管理ガイド を参照してください。



**注意** vCenter クライアントを介して vShield Edge 仮想マシンを修正すると vShield Edge と vShield Manager 間の通信が切れる恐れがあるため、vCenter クライアントを介して vShield Edge 仮想マシンを修正しないでください。vShield Edge 仮想マシンを削除するには、vShield Manager から vShield Edge をアンインストールします。

## vShield Endpoint のインストール

このインストール手順は下記のシステムが既にあるという前提に立っています：

- クラスターの各ホストに、サポートされているバージョンの vCenter Server および ESXi がインストールされているデータセンター。必要なバージョンの詳細については、[第2章「インストールの準備 \(P.13\)」](#) を参照してください。
- vShield Manager 5.0 がインストール済みで運用中。
- アンチウィルス ソリューション管理サーバーがインストール済みで運用中。

## vShield Endpoint インストール ワークフロー

vShield Endpoint のインストール用の ESX ホストの準備が完了したら、vShield Endpoint を次の段階に分けてインストールします。

- 1 アンチウイルス ソリューション プロバイダーから提供された説明書に従い各 ESX ホストにセキュリティ仮想マシン (SVM) を設置、設定します。
- 2 ESXi 5.0 Patch 1 とともにリリースされている VMware Tools 8.6.0 を、保護対象のすべての仮想マシンにインストールします。

vShield Endpoint ホスト コンポーネントは、ESX ホストに次の 2 つのファイアウォール ルールを追加します：

- vShield-Endpoint-Mux ルールは、ホスト コンポーネントとパートナー セキュリティ VM の間の通信のために、ポート 48651 から 48666 を開きます。
- vShield-Endpoint-Mux-Partners ルールは、ホスト コンポーネントのインストールのために、パートナーにより使用される可能性があります。これはデフォルトでは無効になっています。

## ゲスト仮想マシンへの VMware Tools のインストール

VMware Tools には、保護の対象となるそれぞれのゲスト仮想マシンにインストールする必要がある vShield Thin Agent が含まれています。VMware Tools がインストールされた仮想マシンは、セキュリティ ソリューションがインストールされた ESX ホスト上で起動されるたびに自動的に保護されます。つまり、保護された仮想マシンは、終了と起動の間常に、また vMotion がセキュリティ ソリューションのインストールされた別の ESX に移動した後でも、セキュリティ保護が保たれます。

### 開始する前に

ゲスト仮想マシンにはサポートされているバージョンの Windows がインストールされていることを確認してください。vShield Endpoint 5.0 では、以下の Windows オペレーティング システムがサポートされています。

- Windows Vista (32 bit)
- Windows 7 (32/64 bit)
- Windows XP (32 bit)
- Windows 2003 (32/64 bit)
- Windows 2003 R2 (32/64 bit)
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (64 bit)

### 手順

- 1 VMware Tools のインストールの種類を選択します。

ホストの ESX のバージョン	Action
ESX 5.0 Patch 1	Setup Type ウィザードが表示されるまで Installing and Configuring VMware Tools のインストール手順に従います。
ESX 4.1 Patch 3 またはそれ以降	Setup Type ウィザードが表示されるまでナレッジ ベースの記事 <a href="http://kb.vmware.com/kb/2008084">http://kb.vmware.com/kb/2008084</a> のインストール手順に従います。

- 2 Setup Type ウィザードで、次のいずれかのオプションを選択します。
  - 完全
  - カスタム
    - VMware Device Drivers リストから VMCI Driver を選択し、その後 vShield Driver を選択します。

## vShield Data Security のインストール

vShield Data Security のインストールは、vShield Endpoint のインストール後に行うのみ実行できます。

### 開始する前に

ホストおよびゲスト仮想マシンに vShield Endpoint がインストールされていることを確認します。

### 手順

- 1 vSphere Client にログインします。
- 2 インベントリ ツリーから ESX ホストを選びます。
- 3 [vShield] タブをクリックします。
- 4 vShield Data Security の横にある [Install] をクリックします。
- 5 [vShield Data Security] チェックボックスを選択します。
- 6 vShield Data Security で以下の情報を入力します。

オプション	説明
[Datastore]	vShield Data Security サービス仮想マシンを追加するデータセンターを選択します。
[Management Port Group]	vShield Data Security の管理インターフェイスをホストするためのポート グループを選択します。このポート グループは vShield Manager のポート グループへのアクセスが必要です。

- 7 固定 IP を構成する場合は、[Configure static IP for management interface] チェックボックスを選択します。  
[IP address]、[Netmask]、および [Default Gateway] の詳細を入力します。

**注意** [Configure static IP for management interface] を選択しなかった場合には、DHCP (Dynamic Host Configuration Protocol) によって IP アドレスが割り当てられます。

- 8 [Install] をクリックします。  
vShield Data Security 仮想マシンが、選択したホスト上にインストールされます。



## vShield コンポーネントのアンインストール

---

この章では、vCenter インベントリから vShield コンポーネントをアンインストールする際に必要なステップについて説明します。

この章では次のトピックについて説明します。

- [vShield App 仮想アプライアンスのアンインストール \(P. 29\)](#)
- [ポート グループからの vShield Edge のアンインストール \(P. 30\)](#)
- [vShield Data Security 仮想マシンのアンインストール \(P. 30\)](#)
- [vShield Endpoint モジュールのアンインストール \(P. 30\)](#)

### vShield App 仮想アプライアンスのアンインストール

vShield App をアンインストールすると、この仮想アプライアンスがネットワークおよび vCenter Server から削除されます。



**注意** vShield App をアンインストールすると、ESX ホストはメンテナンス モードになります。アンインストールの完了後、ESX ホストは再起動されます。ターゲットの ESX ホスト上で稼働している仮想マシンのいずれか一つでも別の ESX ホストに移動できなかった場合、アンインストールを続ける前にこれらの仮想マシンをシャットダウンするか、手動で移動させる必要があります。vShield Manager が同じ ESX ホスト上にある場合は、vShield App をアンインストールする前に vShield Manager を移動する必要があります。

#### 手順

- 1 vSphere Client にログインします。
- 2 インベントリ ツリーから ESX ホストを選びます。
- 3 [vShield] タブをクリックします。
- 4 [vShield App] サービスについて、[Uninstall] をクリックします。  
ステートレス ESX ホスト上の vShield App をアンインストールする場合は、VIB のアンインストール エラーを無視してください。
- 5 vShield App のアンインストールを開始する前に ESX ホストがメンテナンス モードになっていた場合は、自動アンインストールが完了した後に vShield App 仮想マシンを手動で削除します。

インスタンスがアンインストールされました。

## ポート グループからの vShield Edge のアンインストール

vSphere Client を使用して、保護されたポート グループから vShield Edge をアンインストールできます。

### 手順

- 1 vSphere Client にログインします。
- 2 [表示] - [インベントリ] - [ネットワーク] に進みます。
- 3 [Edge] タブをクリックします。
- 4 [Uninstall] をクリックします。

## vShield Data Security 仮想マシンのアンインストール

vShield Data Security 仮想マシンをアンインストールしたら、VMware パートナーの手順説明に従って、仮想アプライアンスをアンインストールする必要があります。

### 手順

- 1 vSphere Client にログインします。
- 2 インベントリ ツリーから ESX ホストを選びます。
- 3 [vShield] タブをクリックします。
- 4 vShield Data Security サービスについて、[Uninstall] をクリックします。

## vShield Endpoint モジュールのアンインストール

vShield Endpoint モジュールをアンインストールすると、vShield Endpoint モジュールが ESX ホストから削除されます。これらの手順は、次の順番で実行しなければなりません。



**注意** vShield Data Security が ESX ホスト上にインストールされている場合は、vShield Endpoint をアンインストールする前に vShield Data Security をアンインストールする必要があります。

## vShield Endpoint を使用する製品のアンインストール

vShield Endpoint モジュールをホストからアンインストールする前に、vShield Endpoint を使用しているすべての製品をホストからアンインストールする必要があります。ソリューション プロバイダーの指示に従ってください。

## vSphere Client からの vShield Endpoint モジュールのアンインストール

vShield Endpoint モジュールをアンインストールすると、ESX ホストから vShield Endpoint モジュールが削除されます。

### 手順

- 1 vSphere Client にログインします。
- 2 インベントリ ツリーから ESX ホストを選びます。
- 3 [vShield] タブをクリックします。
- 4 [vShield Endpoint] サービスについて、[Uninstall] をクリックします。

# vShield のアップグレード

---

vShield をアップグレードするには、最初に vShield Manager をアップグレードし、次に、ライセンスを所有しているその他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。

この章では次のトピックについて説明します。

- [vShield Manager のアップグレード \(P. 31\)](#)
- [vShield App のアップグレード \(P. 32\)](#)
- [vShield Edge のアップグレード \(P. 32\)](#)
- [vShield Endpoint のアップグレード \(P. 33\)](#)
- [vShield Data Security のアップグレード \(P. 34\)](#)

## vShield Manager のアップグレード

vShield Manager の新しいバージョンへのアップグレードは、vShield Manager ユーザー インタフェースからのみ実行できます。vShield App および vShield Edge の新しいバージョンへのアップグレードは、vShield Manager ユーザー インタフェースから実行するか、REST API を使用して実行することができます。

vShield Manager の新しいバージョンへのアップグレードは、vShield Manager ユーザー インタフェースからのみ実行できます。vShield App および vShield Edge の新しいバージョンへのアップグレードは、vShield Manager ユーザー インタフェースから実行するか、REST API を使用して実行することができます。

### 開始する前に

vShield Endpoint を使用している場合は、vShield Manager のアップグレード前に vShield Endpoint をアンインストールしてください。



**注意** vShield Manager アプライアンスの導入されたインスタンスはアンインストールしないでください。

---

### 手順

- 1 vShield Manager から参照できる場所に vShield 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の名前は、`VMware-vShield-Manager-upgrade_bundle-<buildNumber>.tar.gz` のようになります。
- 2 vShield Manager インベントリ パネルから [Settings & Reports] をクリックします。
- 3 [[Updates]] タブをクリックします。
- 4 [[Upload Settings]] をクリックします。

- 5 [Browse] をクリックして、`VMware-vShield-Manager-upgrade_bundle-<buildNumber>.tar.gz` ファイルを選択します。
- 6 [Open] をクリックします。
- 7 [Upload File] をクリックします。
- 8 [Install] をクリックして、アップグレード プロセスを開始します。
- 9 [Confirm Install] 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。
- 10 vShield Manager 仮想マシンを右クリックし、[Open Console] をクリックして vShield Manager のコマンドライン インターフェイス (CLI) を開きます。
- 11 メッセージ [e1000\_watchdog\_task: NIC Link is up] が表示されたら、vShield Manager ユーザー インターフェイスにログインします。
- 12 [[Updates]] タブをクリックします。  
Installed Release パネルに、インストールした vShield リリースのビルド番号が表示されます。

#### 次に進む前に

- 製品の以前のバージョンにアクセスしたことがあるすべてのクライアント上のブラウザ キャッシュをクリアします。これにより、キャッシュされた javascript あるいは現在のバージョンにおいて変更された可能性があるその他のファイルがクリアされます。
- vShield Manager ユーザー インターフェイスへログインし直します。

## vShield App のアップグレード

データセンター内の各ホスト上の vShield App をアップグレードします。

#### 手順

- 1 vSphere Client にログインします。
- 2 [Inventory] - [Hosts and Clusters] を選択します。
- 3 vShield App をアップグレードするホストを選択します。
- 4 [vShield] タブをクリックします。  
[General] タブに、選択したホスト上にインストールされている各 vShield コンポーネントと、使用可能なリリースが表示されます。
- 5 vShield App の隣の [Update] を選択します。
- 6 [vShield App] チェックボックスを選択します。
- 7 [Install] をクリックします。

## vShield Edge のアップグレード

データセンター内の各ポート グループ上の vShield Edge をアップグレードします。

#### 手順

- 1 vSphere Client にログインします。
- 2 [Views] - [Inventory] - [Networking] を選択します。
- 3 [vShield Edge] タブをクリックします。



4 [Upgrade] をクリックします。

#### 次に進む前に

vShield Edge を前回のリリースからアップグレードする際、vShield Edge は互換モードとなります。これを通常モードに切り替えることができます。

互換モードでは、デフォルトのファイアウォールポリシーが内部インターフェイスにのみ適用されます。外部およびVPNインターフェイス上の送受信両方向のすべてのトラフィックが許可されます。通常モードへの切り替え時に、デフォルトのファイアウォールポリシーのルールが変更されることはありません。ファイアウォールの構成を変更すると、vShield Edge 5.0.1 のデフォルトのファイアウォールのルールが適用され、受信トラフィックがブロックされて発信トラフィックが許可されるようになります。詳細については、『vShield 管理ガイド』を参照してください。

vShield Edge のアップグレード後、vShield Edge アプライアンス上のコマンドライン インターフェイス (CLI) 証明書はリセットされます。CLI へログインするには、デフォルトのユーザー名とパスワードを使用し、その後パスワードをリセットしてください。

## vShield Endpoint のアップグレード

アップグレードの手順は、使用している製品のバージョンにより異なります。

### vShield Endpoint のアップグレード

vShield Endpoint を 4.1 から後続のリリースにアップグレードするには、まずデータセンターの各ホストの vShield Endpoint をアンインストールして vShield Manager をアップグレードしてから、新しいリリースをインストールする必要があります。

- 1 保護された仮想マシンがクラスタ内で動作している場合は、DRS を非アクティブ化します。
- 2 すべての Trend DSVa を非アクティブ化します。これは、仮想マシンから vShield 関連の VFILE フィルタ エントリを削除するために必要です。
- 3 手順 1 で DRS を非アクティブ化している場合は、それを再度アクティブ化します。
- 4 データセンター内の各ホスト上の vShield Endpoint をアンインストールします。詳細については、[\[vSphere Client からの vShield Endpoint モジュールのアンインストール \(P. 30\)\]](#) を参照してください。
- 5 VMware vCenter を希望のバージョンへアップグレードします。詳細については、[第 2 章「インストールの準備 \(P. 13\)」](#) を参照してください。
- 6 各ホストを希望の VMware ESX のバージョンへアップグレードします。詳細については、[第 2 章「インストールの準備 \(P. 13\)」](#) を参照してください。
- 7 vShield Manager をアップグレードします。詳細については、[\[vShield Manager のアップグレード \(P. 31\)\]](#) を参照してください。
- 8 vShield Endpoint をインストールします。詳細については、[\[vShield Endpoint のインストール \(P. 25\)\]](#) を参照してください。

### vShield Endpoint 5.0 からそれ以降のバージョンへのアップグレード

vShield Endpoint を 5.0 から後続のバージョンにアップグレードするには、まず vShield Manager をアップグレードしてから、データセンター内の各ホスト上の vShield Endpoint をアップデートしてください。

#### 手順

- 1 vSphere Client にログインします。
- 2 [Inventory] - [Hosts and Clusters] を選択します。
- 3 vShield Endpoint をアップグレードするホストを選択します。

- 4 [vShield] タブをクリックします。  
[General] タブに、選択したホスト上にインストールされている各 vShield コンポーネントと、使用可能なバージョンが表示されます。
- 5 vShield Endpoint の横にある [Update] を選択します。
- 6 [vShield Endpoint] チェックボックスを選択します。
- 7 [Install] をクリックします。

## vShield Data Security のアップグレード

データセンター内の各ホスト上の vShield Data Security をアップグレードします。vShield Data Security のアップグレードの前に、vShield Endpoint をアップグレードすることをお勧めします。

### 手順

- 1 vSphere Client にログインします。
- 2 [Inventory] - [Hosts and Clusters] に移動します。
- 3 vShield App をアップグレードするホストを選択します。  
[Summary] タブに、選択したホスト上にインストールされている各 vShield コンポーネントと、使用可能なリリースが表示されます。
- 4 vShield Data Security の隣の [Update] を選択します。
- 5 [vShield Data Security] チェックボックスを選択します。
- 6 [Install] をクリックします。

## vShield のインストールの失敗

---

vShield App のインストールがエラーとなりました。

### 問題

vShield App のインストールに失敗すると、製品をアンインストールするためのプロンプトが表示されます。

### 原因

vShield vApp をアンインストールする際、必要なすべてのコンポーネントが削除されるわけではありません。

### 解決方法

- 1 [Uninstall] をクリックし、すべての vShield コンポーネントをアンインストールします。詳細については、[第 5 章 \[vShield コンポーネントのアンインストール \(P. 29\)\]](#) を参照してください。
- 2 VIB のインストール中に問題があったことを示すエラーメッセージが表示された場合は、ESX ホストを再起動します。
- 3 vShield App を再インストールします。



# インデックス

## C

### CLI

- vShield Manager ネットワーク設定の構成 18
- 堅牢化 16

## D

- DMZ 11

## E

- Endpoint のアップグレード、5.0 から後続のバージョンへ 33
- ESX ホストの準備 22

## G

- GUI パスワードの変更 20
- GUI へのログイン 19

## R

- REST 16

## V

- vCenter Server の同期 19
- vMotion 15
- vShield
  - ESX ホストの準備 22
  - vShield App 8
  - vShield Edge 9
  - vShield Endpoint 10
  - vShield Manager 8
    - 堅牢化 15
    - コンポーネント通信 15
    - コンポーネントの評価 21
    - 導入シナリオ 10
  - vShield Protection のための仮想マシンの用意 15
- vShield App
  - アンインストール 29
  - インストール 22
  - 説明 8
  - よくある導入 12
  - ライセンス 22
- vShield Data Security 10
- vShield Edge
  - アンインストール 30
  - インストール 24
  - 説明 9
  - ネットワークの分離 11

- よくある導入 12

- ライセンス 22

### vShield Endpoint

- SVM の登録解除 30
- アンインストール 30
- インストール 22, 25
- インストール手順 26
- 説明 10
- シン エージェントのインストール 26
- ライセンス 22

### vShield Endpoint SVM の登録解除 30

### vShield Manager

- GUI パスワードの変更 20
- GUI へのログイン 19
- vCenter Server の同期 19
- 稼働時間 15
- インストール 17
- 説明 8
- ネットワーク設定 18
- プラグインの登録 20

### vShield Manager GUI 16

### vShield Manager と vCenter Server の同期 19

### vShield Manager ネットワーク設定の構成 18

### vShield Zones、vShield Manager 8

### vShield コンポーネントの評価 21

### vSphere Client プラグイン 20

## あ

### アップグレード

- vShield App 32
  - vShield Edge 32
  - vShield Endpoint 33
  - vShield Manager 31
- ### アンインストール
- vShield App 29
  - vShield Data Security 30
  - vShield Edge 30
  - vShield Endpoint モジュール 30

## い

### インストール

- vShield App 22
- vShield Edge 24, 25
- vShield Endpoint 22
- vShield Endpoint シン エージェント 26

vShield Manager 17

ライセンス 22

## か

仮想マシンの保護 15

## く

クライアント要件 13

クラスタの保護 12

## け

堅牢化

CLI 16

REST 16

vShield Manager GUI 16

## こ

コンポーネント間の通信 15

## し

システム要件 13

シンエージェントのインストール 26

## と

導入

DMZ 11

クラスタ 12

導入シナリオ 10

導入にあたって考慮すべき事柄 14

## ね

ネットワークの分離 11

## は

パスワードの変更 20

## ふ

プラグイン 20

## ら

ライセンス

インストール 22

評価モード 21