vShield インストールとアップグレードガイド

vShield Manager 5.5
vShield Edge 5.5
vShield Endpoint 5.5

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-001281-00

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）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 までお送りください。

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

ヴイ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

目次

本書について

このマニュアル、『vShield インストールおよびアップグレード 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 5.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 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。

1 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

VMware vShield は、VMware vCenter Server を統合するために構築されたセキュリティ仮想アプライアンスのスイートです。vShield は、攻撃や不正使用から仮想データセンターを保護し、コンプライアンスの遵守に関連した目標を達成するのに役立つ、重要なセキュリティ 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、1 つの vCenter Server 環境と、複数の vShield App、vShield Edge、vShield Endpoint、および vShield Data Security のインスタンスを管理します。

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、およびネットワークに対する脅威の識別を行うことができます。

vShield Edge

vShield Edge は、ネットワーク エッジ セキュリティとゲートウェイ サービスを提供して、仮想ネットワークを分離するか、ポート グループ、vDS ポート グループ、または Cisco Nexus 1000V ポート グループの仮想マシンを分離します。vShield Edge はデータセンター レベルでインストールし、内部またはアップリンクのインターフェイスを最大 10 個追加できます。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）

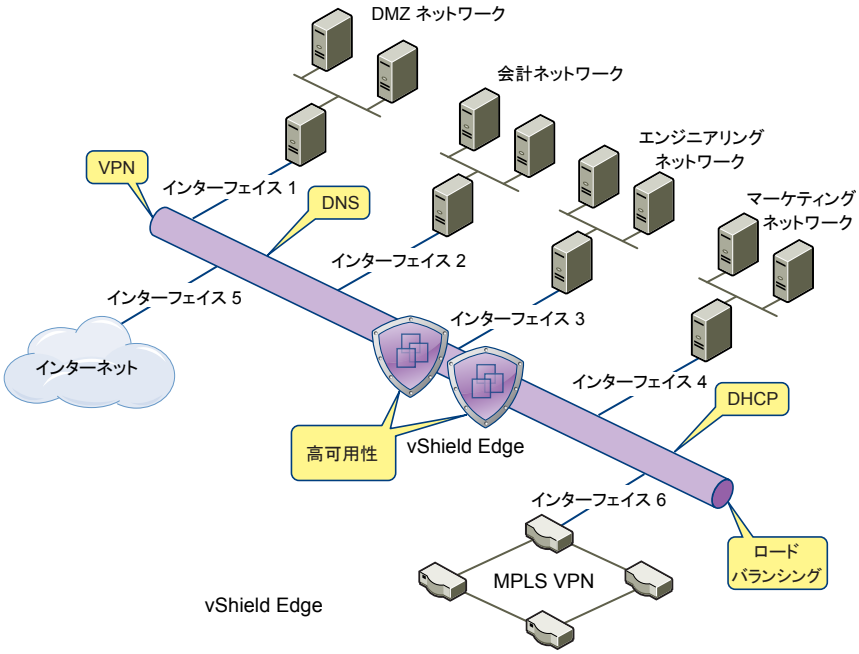
firewall	サポートされるルールには、すべてのプロトコルのステートフル インスペクションの対象となる IP レンジとポート レンジによる 5 個組みの IP 構成が含まれます。
ネットワーク アドレス変換	送信元と送信先の IP アドレス、およびポート変換の管理を分離します。
DHCP（Dynamic Host Configuration Protocol）	IP プール、ゲートウェイ、DNS サーバ、検索ドメインの構成します。

アドバンスト vShield Edge サービス

サイト間 VPN（Virtual Private Network）	標準化された IPsec プロトコル設定を使用して、すべての主要な VPN ベンダーと相互運用します。
SSL VPN-Plus	SSL VPN-Plus によりリモート ユーザーは、vShield Edge ゲートウェイの背後にあるプライベート ネットワークに安全に接続することができます。
ロード バランシング	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。
高可用性	高可用性により、プライマリ vShield Edge 仮想マシンが使用不可の場合でも、ネットワーク上にアクティブな vShield Edge が必ず存在するようにします。

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. マルチインターフェイス Edge

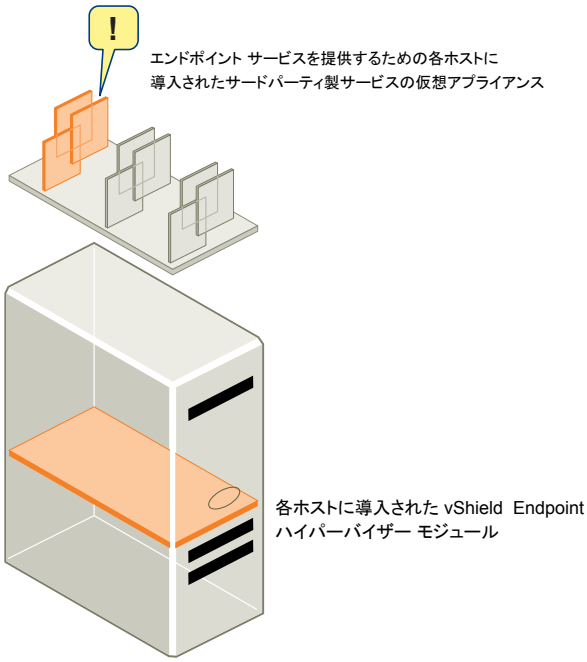


vShield Endpoint

vShield Endpoint は、アンチウィ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、アンチウィルス 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ィルス 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 アンチウィルス 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

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 サービスの良くある例が 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。

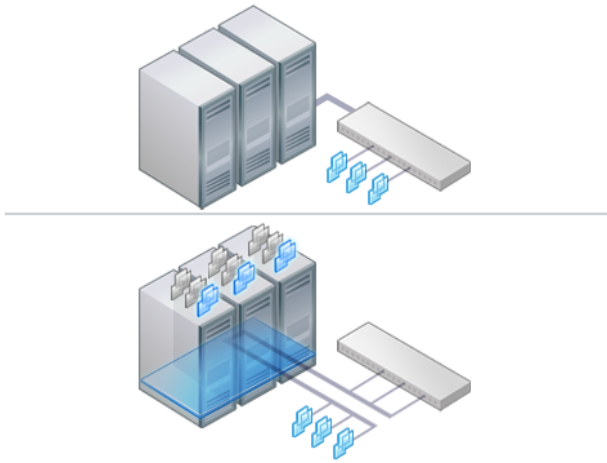
例えば、VLAN を論理的、組織的、またはネットワーク境界をベースとして仮想マシン ゾーンを分割し、使うことができます。Virtual Infrastructure SDK を活用することで、vShield Manager インベントリ パネルが Networks ビューの下に現在の VLAN ネットワークを表示します。各 VLAN ネットワークの仮想マシンへのアクセス ルールを設定し、タグのないトラフィックをこれらの仮想マシンへ選り分けておくことができます。

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こともできます。

インストールの準備 2

この章では、vShield のインストールに成功するための必要条件についての概要を示します。

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

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。vCenter Server あたり 1 つの vShield Manager、ESX™ ホストあたり 1 つの vShield App か 1 つの vShield Endpoint、およびデータセンターあたり複数の vShield Edge インスタンス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 Manager: 8 GB 割り当て、3 GB 予約 ■ vShield App: 1 GB 割り当て、1 GB 予約 ■ vShield Edge コンパクト: 256 MB、ラージおよび超特大: 1 GB、X ラージ: 8 GB ■ vShield Data Security： 512 MB
ディスク スペース	■ vShield Manager: 60 GB ■ vShield App: ESX ホスト 1 台の vShield App につき 5 GB ■ vShield Edge コンパクト: 300 MB、ラージ、超特大、X ラージ: 448 MB ■ vShield Data Security： ESX ホストあたり 6 GB
vCPU	■ vShield Manager: 2 ■ vShield App: 2 ■ vShield Edge コンパクト: 1、ラージ: 2、超特大および X ラージ: 4 ■ vShield Data Security: 1

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 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 5.0 以降

  VXLAN 仮想ワイヤの場合は、vCenter Server 5.1 以降が必要です。

- サーバごとに VMware ESX 5.1 以降

  VXLAN 仮想ワイヤの場合は、VMware ESX 5.1 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 3 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. 34)」を参照してください。

  vShield App によって保護する仮想マシンには、VMware Tools をインストールする必要があります。

- VMware vCloud Director 5.1 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
- ESX ホストを名前別に vSphere インベントリに追加した場合は、vShield Manager で DNS サーバが構成されており、名前解決が機能していることを確認してください。DNS 名が提供されていなければ、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
- vShield Manager から、ESX ホスト、vCenter Server、およびデプロイされる vShield アプライアンスからアクセス可能なポート 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。
- 次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 の導入にあたって考慮すべき事柄

このトピックでは、vShield コンポーネントを導入する場合の考慮事項について説明します。

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、使用する vShield コンポーネントに応じて、vShield App、vShield Endpoint、および vShield Data Security の DRS クラスタ内のすべての ESX ホストを準備してください。また、仮想マシンをハードウェア バージョン 7 または 8 にアップグレードする必要があります。

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、DRS クラスタのホストの準備ができている場合は、セキュリティを弱体化させることなく、ホスト間でマシンを移行することができます。ESX ホストの準備の詳細については、「vShield App のインストール (P. 26)」 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 には、vCenter Server、ESXi ホスト、vShield App と vShield Edge インスタンス、vShield Endpoint モジュール、および vShield Data Security 仮想マシンとの間の接続が必要です。vShield コンポーネントはルート設定された接続だけでなく、異なる LAN 経由でも通信できます。

VMware では、vShield Manager が管理するクラスタから分離されている専用の管理クラスタに vShield Manager をインストールするようお勧めします。それぞれの vShield Manager が 1 つの vCenter Server 環境を管理します。

vCenter Server または vCenter Server データベースの仮想マシンが ESX ホストにあり、その ESX ホストに vShield App をインストールする場合は、vShield App をインストールする前にそれらの仮想マシンを別のホストに移行してください。

次のポートが開いていることを確認します。

- ESX ホスト、vCenter Server、および vShield Data Security から、それらへの、それらの間での通信で使用するポート 443/TCP
- vShield Manager と vShield App の間の時間同期で使用する UDP123
- REST API 呼び出しで使用する REST クライアントから vShield Manager への 443/TCP
- vShield Manager ユーザー インターフェイスを使用し、vSphere SDK への接続を開始する場合の 80/TCP および 443/TCP
- vShield Manager と vShield App の間の通信と、CLI のトラブルシューティングで使用する 22/TCP

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

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. 22)」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、アンチウィルス 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的アクセス権で 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 App の導入にあたって考慮すべき事柄

VMware では、ご使用の vCenter Server 環境を分析し、環境全体を保護するか、特定のクラスタのみを保護するかを決定するようお勧めします。

特定のクラスタを保護する場合は、クラスタ全体を準備し、それらのクラスタのすべての ESX ホストに vShield App をインストールする必要があります。クラスタのいくつかのホストに vShield App のみをインストールすると、保護されたホストから保護されていないホストに vMotion が仮想マシンを移動する可能性があり、そのためネットワークのセキュリティが侵害されることがあります。

必ず、メンテナンス用時間枠の期間に、ご使用の環境に vShield App をインストールしてください。インストールの合計時間は、ご使用の環境と各クラスタのホスト数に応じて異なりますが、平常運用を再開する前に必要なすべてのクラスタへの vShield App のインストールを完了する必要があります。

インストール後は、vSphere HA を有効にし、vShield App をインストールしたクラスタでのクラスタ機能を [VM and Application Monitoring] に設定することをお勧めします。この機能は、vShield App を監視し、失敗した場合には再起動を開始して、vShield App の停止時間を最小限に抑えます。この機能の詳細については、『vSphere 可用性』を参照してください。

VMware では、vShield App が通常運用中に実行されるようにし、vShield App Flow Monitoring ツールを使用して、仮想ネットワークを発着信するトラフィックに関するベースライン情報を収集するようお勧めします。その後、ネットワークの必要に応じてルールを追加できます。

vShield App の SpoofGuard 機能を有効にすることにより、VMware Tools によって報告される IP アドレスを認証し、必要に応じて変更してなりすましを防止することができます。選択する SpoofGuard モードに応じて、vShield App は、最初の使用時に IP 割り当てを自動的に信頼するか、使用前に IP 割り当てを手動で承認するよう要求します。ただし、仮想マシンの IP アドレスは、DHCP サーバがリリースを更新するか、サーバが再起動されるときに変更される可能性があることに注意してください。これは、SpoofGuard 機能が有効な場合には、新規または更新された IP アドレスを承認する必要があることを意味します。

vShield App をインストールする前に Flow Monitoring と SpoofGurard 機能に精通しておくことにより、最大限にセキュアな方法で vShield App を構成することができます。これらの機能の詳細については、『vShield 管理ガイド』を参照してください。

vShield Edge を導入する場合の考慮事項

vShield Edge をインストールする前に、ネットワーク トポロジについて理解しておく必要があります。vShield Edge では複数のインターフェイスを使用できますが、vShield Edge を導入できるようにするには、少なくとも 1 つの内部インターフェイスをポートグループまたは VXLAN 仮想ワイヤに接続する必要があります。

アップリンク インターフェイスを使用すると、外部のネットワークに接続できます。外部への接続が可能なポート グループまたは VXLAN 仮想ワイヤを作成して構成しておく必要があります。また、内部インターフェイスを接続することができる仮想マシンを含んだポート グループも必要です。これらのインターフェイスのために用意する IP アドレスとサブネットを決定してください。また、vShield Edge のインストール後に有効にして構成するサービスについても考慮してください。vShield Edge サービスの詳細については、『vShield 管理ガイド』を参照してください。

vShield Edge をインストールしてから vShield Edge サービスを構成するまでの間に、そのポート グループの仮想マシンがネットワーク接続を失うことがあります。この問題を回避するため、新しいポート グループを作成し、そこに vShield Edge をインストールおよび構成して、仮想マシンをそのポート グループに移動することができます。

デフォルトの vShield Edge ファイアウォール ポリシーは着信トラフィックをすべてブロックするため、必要に応じて許可ルールを追加する必要があります。

vShield Manager のインストール 3

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。

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

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。

開始する前に

Enterprise Administrator または vShield Administrator ロールが割り当てられている必要がある。

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、ｖ Center Server、および ESXi のホストには、将来的な vShield Edge、vShield App、vShield Endpoint のインスタンスすべてからアクセス可能である必要があります。

3 [File] - [Deploy OVF Template] を選択します。

4 [参照] をクリックして、vShield Manager OVA ファイルが格納されている PC 上のフォルダに移動します。

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。

次に進む前に

vShield Manager 5.1 のデフォルト CPU は 2 vCPU です。vShield Manager を vSphere Fault Tolerance と併用する場合は、CPU を [1 vCPU] に設定する必要があります。

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. 22)」を参照してください。

4 [Log In] をクリックします。

vShield Manager のセットアップ

vCenter Server、DNS と NTP サーバ、および Lookup サーバの詳細を指定します。

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。

開始する前に

- vShield Manager と vCenter Server を同期するには、管理アクセス権限の付与された vCenter Server 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。

- vShield Manager で SSO を使用するには、vCenter Server 5.1 以上と Single Sign On サービスが vCenter Server にインストールされている必要があります。

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 [構成] タブをクリックします。

4 [DNS Servers] 領域に、vShield Manager のネットワーク設定を構成したときに指定した DNS サーバの IP アドレスが表示されます。

必要に応じてサーバを編集できます。

5 [NTP Server] で、 [Edit] をクリックし、NTP サーバの IP アドレスを入力します。

NTP サーバは共通ネットワーク時間を確立します。SSO サーバが使用する NTP サーバを使用することにより、vShield Manager サーバの時刻が NTP サーバと同期されるようにすることをお勧めします。

重要 NTP サーバの詳細を編集した後に、vShield Manager を再起動する必要があります。

6 [Lookup Service] で、 [Edit] をクリックし、検索サービスがあるホストのホスト名または IP アドレスを入力します。

7 必要に応じてポート番号を変更します。

Lookup Service の URL は、指定されたホストおよびポートに基づいて表示されます。

8 SSO ユーザー名とパスワードを入力します。

これにより vShield Manager は、それ自体を Security Token Service サーバで登録できます。

9 [vCenter Server] に、vCenter Server の IP アドレスまたはホスト名を入力します。

10 vSphere Client のログイン ユーザー名を入力します。

11 そのユーザー名に関連付けられたパスワードを入力します。

12 ログインしたユーザーに Enterprise Administrator ロールを割り当てるには、[このユーザーに vShield の Enterprise Administrator ロールを割り当てる] を選択します。

このロールにより、vShield の操作とセキュリティ権限がそのユーザーに付与されます。

13 プラグイン スクリプトのダウンロード先を変更するには、 [プラグイン スクリプトのダウンロード先を変更する] を選択し、vShield Manager の IP アドレスとポート番号を入力します。

これは、NAT 環境で必要になることがあります。デフォルトで使用される vShield Manager のアドレスは、`vShield_Manager_IP:443` です。

14 [保存] をクリックします。

15 (オプション) Windows サーバ コンピュータで、次の手順を実行して vShield Manager インベントリ パネルをロードします。

a Internet Explorer を開きます。

b [ツール] - [インターネット オプション] を選択します。

c [インターネット オプション] ウィンドウで、 [セキュリティ] タブを選択します。

d [信頼済みサイト] をクリックします。

e [サイト] ボタンをクリックします。

f vShield Manager の IP アドレスを入力して、 [追加] をクリックします。

g [閉じる] をクリックします。

h [OK] をクリックします。

i Internet Explorer を閉じます。

vShield Manager は、vCenter Server に接続してログオンし、VMware Infrastructure SDK を利用して vShield Manager インベントリ パネルを配置します。インベントリ パネルは画面の左側に表示されます。このリソース ツリーは、VMware Infrastructure インベントリ パネルと一致する必要があります。vShield Manager は、vShield Manager インベントリ パネルには表示されません。

次に進む前に

vSphere Client にログインし、ESX ホストを選択して、vShield がタブとして表示されることを確認します。その後、vShield Client から vShield のコンポーネントをインストールおよび構成します。

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 ウィンドウの右上にある [パスワードの変更] をクリックします。

3 [古いパスワード] に **`default`** （現在のパスワード） と入力します。

4 新しいパスワードを入力します。

5 [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。

6 [OK] をクリックして、変更内容を保存します。

vShield Manager データ バックアップのスケジュール設定

一度にスケジュール設定できるのは、1 種類のバックアップに対するパラメータだけです。構成のみのバックアップをスケジュールすることはできません。完全なデータ バックアップの同時実行をスケジュールすることもできません。

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 [Backups] をクリックします。

4 [[Scheduled Backups]] ドロップダウン メニューで、 [On] を選択します。

5 [[Backup Frequency]] ドロップダウン メニューで、 [[Hourly]] 、 [[Daily]] 、または [Weekly] を選択します。

[[Day of Week]] 、 [[Hour of Day]] 、および [[Minute]] ドロップダウン メニューは、選択された頻度に基づいて無効になります。たとえば、 [[Daily]] を選択すると、 [Day of Week] 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。

6 (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、 [Exclude System Events] チェック ボックスをオンにします。

7 (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、 [Exclude Audit Log] チェック ボックスをオンにします。

8 バックアップの保存先であるシステムの [Host IP Address] を入力します。

9 (オプション) バックアップ システムの [Host Name] を入力します。

10 バックアップ システムにログインするために必要な [User Name] を入力します。

11 [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。

12 [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。

13 [Filename Prefix] にテキスト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。

14 送信先でサポートされるプロトコルに応じて、 [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。

15 [Save Settings] をクリックします。

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。

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。

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

vShield Edge、vShield App、vShield Endpoint を購入および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て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 コンポーネント ライセンスのインストール

vShield App と vShield Edge をインストールする前に、CIS または vCloud Networking and Security (vCNS) ライセンスをインストールする必要があります。vSphere ライセンスには、vShield Endpoint のライセンスが含まれます。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。

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 [管理] タブで、 [資産] を選択します。

3 CIS または vCNS アセットを右クリックし、 [ライセンス キーの変更] 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。

vShield App のインストール

ESX ホストに vShield App をインストールできます。

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。保護が不要な vCenter Server、vCenter Server データベース、およびサード パーティまたは内部サービスの仮想マシンは、仮想マシン除外リストに含めることをお勧めします。vShield App の保護から仮想マシンを除外する方法の詳細については、『vShield 管理ガイド』を参照してください。

重要 vCenter Server または vCenter Server データベースの仮想マシンが ESX ホストにあり、その ESX ホストに vShield App をインストールする場合は、vShield App をインストールする前にそれらの仮想マシンを別のホストに移行してください。

開始する前に

- 各 vShield App 仮想アプライアンスの管理 (MGT) ポートに固有の IP アドレスが設定されてい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。不正確な IP アドレスを使用すると、ホストで vShield App をアンインストールし、もう一度インストールすることが必要になります。
- 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
[データストア]	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。
[IP アドレス]	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。 重要 入力した IP アドレスが正しいことを確認します。vShield App のインストール後に IP アドレスを変更するには、vShield App をアンインストールし、ESX ホストを再起動する必要があります。
[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 [Intstall] 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。

次に進む前に

vShield App が通常の稼働時に実行されるようにして、仮想ネットワークに出入りするトラフィックを調べます。この情報に基づいてファイアウォール 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. 27)」の手順に従ってください。

注意 vSphere クライアントを介し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。

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 [構成] 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] - [vmservice-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] - [vmservice-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-5.0.1-766127.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 バンドルを使用して、ステートレスな ESX 構成をアップデートします。

vShield Edge のインストール

データセンターには複数の vShield Edge 仮想アプライアンスをインストールできます。各 vShield Edge 仮想アプライアンスには、アップリンクと内部のネットワーク インターフェイスを合計で 10 個指定できます。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、そのポート グループ内の保護された仮想マシンすべて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。ファイアウォール ルールと他の vShield Edge サービスは、インターフェイス間のトラフィックに適用されます。

vShield Edge のアップリンク 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対するアクセス権を持つアップリンク ポート グループに接続します。

ロードバランサー、サイト間 VPN、NAT サービス用に複数の外部 IP アドレスを構成できます。重複する IP アドレスは内部インターフェイスで許容されず、重複するサブネットは内部とアップリンクのインターフェイスで許容されません。

開始する前に

Enterprise Administrator または vShield Administrator ロールが割り当てられている必要がある。

手順

1 エッジの追加ウィザードを開く (P. 29)

エッジの追加ウィザードを開いて、vShield Edge インスタンスをインストールおよび構成します。

2 vShield Edge の名前付け (P. 29)

vShield Edge には、1 つのテナントのすべての vShield Edge 仮想マシンの中で一意の分かりやすい名前が必要です。この名前は vCenter インベントリに表示されます。

3 CLI 資格情報の指定 (P. 29)

コマンド ライン インターフェイス （CLI） へのログインで使用する認証情報を編集します。

4 アプライアンスの追加 (P. 30)

vShield Edge をデプロイできるようにするには、まずアプライアンスを追加する必要があります。vShield Edge のインストール時にアプライアンスを追加しないと、vShield Edge はアプライアンスが追加されるまでオフライン モードのままになります。

5 内部およびアップリンク インターフェイスの追加 (P. 31)

内部およびアップリンクのインターフェイスは、最大で 10 個まで vShield Edge 仮想マシンに追加できます。

6 デフォルト ゲートウェイの構成 (P. 32)

vShield Edge デフォルト ゲートウェイの IP アドレスを指定します。

7 ファイアウォール ポリシーと高可用性の構成 (P. 32)

デフォルトのファイアウォール ポリシーでは、すべての受信トラフィックをブロックするように定義されており、この設定は変更することができます。

8 設定の確認と vShield Edge のインストール (P. 33)

vShield Edge をインストールする前に、入力した設定値を確認してください。

エッジの追加ウィザードを開く

エッジの追加ウィザードを開いて、vShield Edge インスタンスをインストールおよび構成します。

手順

1 vSphere Client にログインします。

2 インベントリ ツリーからデータセンター リソースを選択します。

3 [ネットワーク仮想化] タブをクリックします。.

4 [エッジ] をクリックします。

5 [追加] （  ） アイコンをクリックします。

エッジの追加ウィザードが表示されます。

vShield Edge の名前付け

vShield Edge には、1 つのテナントのすべての vShield Edge 仮想マシンの中で一意の分かりやすい名前が必要です。この名前は vCenter インベントリに表示されます。

手順

1 vShield Edge 仮想マシンの名前を入力します。

この名前は vCenter インベントリに表示されます。1 つのテナントのすべての Edge の中で一意の名前を付けてください。

名前を指定しないと、vShield Manager が vShield Edge ごとに一意の名前を作成します。

2 (オプション) vShield Edge 仮想マシンのホスト名を入力します。

この名前は CLI に表示されます。ホスト名を指定しない場合は、手順 1 で指定した名前が CLI にも表示されます。

3 (オプション) この vShield Edge の説明を入力します。

4 (オプション) この vShield Edge のテナントを入力します。

5 (オプション) [HA の有効化] を選択して高可用性（HA）を有効にします。

6 [Next] をクリックします。

CLI 資格情報の指定

コマンド ライン インターフェイス （CLI） へのログインで使用する認証情報を編集します。

手順

1 [CLI 資格情報] ページで、vShield Edge 仮想マシンの CLI 認証情報を指定します。

オプション	操作
CLI ユーザー名	必要に応じて編集します。
CLI パスワード	必要に応じて編集します。

2 (オプション) 必要に応じて、 [SSH アクセスの有効化] をクリックします。

3 [Next] をクリックします。

[エッジ アプライアンス] ページが表示されます。

アプライアンスの追加

vShield Edge をデプロイできるようにするには、まずアプライアンスを追加する必要があります。vShield Edge のインストール時にアプライアンスを追加しないと、vShield Edge はアプライアンスが追加されるまでオフライン モードのままになります。

開始する前に

高可用性の場合は、両方の HA 仮想マシンをデプロイするのに十分な容量がリソース プールにあることを確認してください。コンパクト vShield Edge 仮想マシンの場合は 256 MB のメモリ、ラージ vShield Edge 仮想マシンの場合は 1 GB のメモリ、X ラージ vShield Edge 仮想マシンの場合は 8 GB のメモリが必要です。データストアには少なくとも 512 MB のディスク領域が必要です。

手順

1 [エッジ アプライアンス] ページで、使用するシステム リソースに基づいて vShield Edge インスタンスを選択します。

[Large] vShield Edge には、 [Compact] vShield Edge よりも多くの CPU、メモリ、およびディスク領域があり、大量数の同時 SSL VPN-Plus ユーザーをサポートします。 [X ラージ] の vShield Edge は、百万単位の同時セッションを処理するロード バランサーが実装されている環境に適しています。X ラージ vShield Edge は SSL VPN をサポートしません。

2 ファイアウォール、NAT、およびルーティングのルートを追加してこれらのサービスで送信される制御トラフィックを有効にするには、 [Enable auto rule generation] をクリックします。

[Enable auto rule generation] を選択しない場合は、ファイアウォール ルールを手動で作成し、ファイアウォール、NAT、およびルーティングのルートを追加することにより、ロード バランシングや VPN などの vShield Edge サービスの制御チャンネル トラフィックを許可する必要があります。

注意　自動ルール生成では、データ チャンネル トラフィックのルールを作成しません。

---

3 [AESNI の有効化] をクリックして、Intel® Advanced Encryption Standard New Instructions（Intel® AES-NI）を有効にします。

4 [エッジ アプライアンス] で、 [追加] （  ）アイコンをクリックしてアプライアンスを追加します。

[Name and Description] ページで [Enable HA] を選択した場合は、2 つのアプライアンスを追加できます。アプライアンスを 1 つ追加すると、vShield Edge はその構成をスタンバイ アプライアンス用に複製します。これにより、DRS と vMotion を使用した後でも (それらの仮想マシンを手動で同じホストに vMotion しない限り)、2 つの HV vShield Edge 仮想マシンが同じ ESX ホストに存在することがないようにします。

5 [エッジ アプライアンスの追加] ダイアログ ボックスで、アプライアンスのクラスタまたはリソース プール、およびデータストアを選択します。

6 (オプション) アプライアンスを追加するホストを選択します。

7 (オプション) アプライアンスを追加する vCenter フォルダを選択します。

8 [Add] をクリックします。

9 [Next] をクリックします。

[インターフェイス] ページが表示されます。

内部およびアップリンク インターフェイスの追加

内部およびアップリンクのインターフェイスは、最大で 10 個まで vShield Edge 仮想マシンに追加できます。

手順

1 [インターフェイス] ページで、[追加] （  ）アイコンをクリックし、インターフェイスの名前を入力します。

2 [内部] または [アップリンク] を選択して、内部と外部のどちらのインターフェイスなのかを指定します。

HA を有効にするには、内部インターフェイスを少なくとも 1 つ追加する必要があります。

3 このインターフェイスを接続するポート グループ VXLAN 仮想ワイヤを選択します。

a [接続先] フィールドの横の [選択] をクリックします。

b インターフェイスに接続する対象に応じて、[Virtual Wire]、[Standard Portgroup]、または [Distributed Portgroup] タブをクリックします。

c 該当する仮想ワイヤまたはポート グループを選択します。

d [選択] をクリックします。

4 インターフェイスの接続ステータスを選択します。

5 [サブネットの構成] で、[追加] （  ） アイコンをクリックし、インターフェイスのサブネットを追加します。

1 つのインターフェイスには、重複しない複数のサブネットを設定できます。

6 [サブネットの追加] で、[追加] （  ） アイコンをクリックし、IP アドレスを追加します。

複数の IP アドレスを入力した場合は、プライマリ IP アドレスを選択できます。インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。vShield Edge は、ローカルで生成されたトラフィックの場合、プライマリ IP アドレスを送信元アドレスとみなします。

何からの機能構成で使用する前に、インターフェイスに IP アドレスを追加する必要があります。

7 インターフェイスのサブネット マスクを入力し、[保存] をクリックします。

8 (オプション) インターフェイスの MAC アドレスを入力します。HA が有効な場合は、2 つの管理 IP アドレスを CIDR 形式で入力します。

2 つの vShield Edge HA 仮想マシンのハートビートは、これらの管理 IP アドレスを介して通信されます。管理 IP アドレスは、同じ L2/サブネットに存在し、相互に通信可能になっている必要があります。

9 必要に応じてデフォルトの MTU を変更します。

10 [オプション] で、必要なオプションを選択します。

オプション	説明
プロキシ ARP の有効化	異なるインターフェイス管での重複ネットワーク転送をサポートします。
ICMP リダイレクトの送信	ルーティング情報を各ホストに伝達します。

11 fence パラメータを入力し、[追加] をクリックします。

12 手順 手順 1 から 手順 11 を繰り返してインターフェイスを追加します。

13 [次へ] をクリックします。

[デフォルト ゲートウェイ] ページが表示されます。

デフォルト ゲートウェイの構成

vShield Edge デフォルト ゲートウェイの IP アドレスを指定します。

手順

1 [デフォルト ゲートウェイ] ページで、 [デフォルト ゲートウェイの構成] を選択します。

2 次ホップまたはゲートウェイ IP アドレスと通信できるインターフェイスを選択します。

3 デフォルト ゲートウェイの IP アドレスを入力します。

4 [MTU] に、手順 2 で選択したインターフェイスのデフォルト MTU が表示されます。この値は編集することができますが、インターフェイスに設定されている MTU より大きくすることはできません。

5 [Next] をクリックします。

[ファイアウォールと HA] ページが表示されます。

ファイアウォール ポリシーと高可用性の構成

デフォルトのファイアウォール ポリシーでは、すべての受信トラフィックをブロックするように定義されており、この設定は変更することができます。

vShield Edge でのネットワーク構成で高可用性を有効にするには、HA パラメータを構成する必要があります。vShield Edge は高可用性で 2 つの仮想マシンをサポートし、どちらの仮想マシンもユーザー構成で最新の状態に維持されます。プライマリ仮想マシンでハートビート障害が発生すると、セカンダリ仮想マシンの状態がアクティブに変化します。このようにして、ネットワーク上では常に 1 つの vShield Edge 仮想マシンがアクティブの状態になります。

手順

1 [ファイアウォールと HA] ページで、 [ファイアウォールのデフォルト ポリシーの構成] を選択します。

2 受信トラフィックをデフォルトで受け入れるか拒否するかを指定します。

作成するファイアウォール ルールはデフォルト ポリシーをオーバーライドします。

3 受信トラフィックをログに記録するかどうかを選択します。

デフォルト ポリシーをオーバーライドするファイアウォール ルールを作成する場合、ログに記録するかどうかは作成するルールによって決まります。デフォルトのログ記録を有効にすると、生成されるログが過度に多くなり、vShield Edge のパフォーマンスに影響する可能性があります。したがって、デフォルトのログはトラブルシューティングかデバッグを実行する間のみ有効にすることをお勧めします。

4 [名前と説明] ページで [HA の有効化] を選択した場合は、 [HA パラメータの構成] セクションで必要な設定を完了します。

vShield Edge はスタンバイ アプライアンス用にプライマリ アプライアンスの構成を複製し、DRS や vMotion の使用後であっても、2 つの HA vShield Edge 仮想マシンが同じ ESX ホストに存在することのないようにします。2 つの仮想マシンは、構成したアプライアンスと同じリソース プールおよびデータストアにある vCenter にデプロイされます。vShield Edge HA の HA 仮想マシンにはローカル リンク IP が割り当てられるため、それらの仮想マシンは相互に通信できます。管理 IP アドレスを指定してローカル リンクをオーバーライドすることができます。

a HA パラメータを構成する内部インターフェイスを選択します。

b (オプション) バックアップ アプライアンスがプライマリ アプライアンスからハートビート信号を受信しない場合に、プライマリ アプライアンスを非アクティブと見なし、バックアップ アプライアンスで引き継ぐまでの最大期間を秒単位で入力します。

デフォルトの間隔は 6 秒です。

c (オプション) 2 つの管理 IP アドレスを CIDR 形式で入力して、HA 仮想マシンに割り当てられたローカル リンク IP をオーバーライドします。

管理 IP アドレスがインターフェイスのサブネットのどれとも重複することのないようにしてください。

5 [次へ] をクリックします。

[サマリ] ページが表示されます。

設定の確認と vShieldEdge のインストール

vShield Edge をインストールする前に、入力した設定値を確認してください。

手順

1 [サマリ] ページで、vShield Edge の設定を確認します。

2 設定を修正するには、 [前へ] をクリックします。

3 設定に同意して vShield Edge をインストールするには、 [完了] をクリックします。

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 5.1 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 のイベントール 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 アンチウィルス 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 保護対象のすべての仮想マシンにインストールしている VMware Tools の最新バージョン (ESX のバージョン用) を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のある vShield シン エージェントが含まれます。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、次の 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 SP3 以降（32 ビット）
- Windows 2003 SP2 以降（32 ビットまたは 64 ビット）
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (64 bit)

手順

1 VMware Tools のインストールのタイプを選択します。

ホストの ESX バージョン	操作
ESX 5.0 Patch 1 以降	[タイプのセットアップ] ウィザードが表示されるまで、VMware Tools のインストールと構成のインストール手順に従います。
ESX 4.1 Patch 3 以降	[タイプのセットアップ] ウィザードが表示されるまで、ナレッジ ベースの記事 http://kb.vmware.com/kb/2008084 のインストール手順に従います。

2 [タイプのセットアップ] ウィザードで、次のいずれかのオプションを選択します。

- 完了
- カスタム
  - VMware デバイス ドライバ リストで VMCI ドライバを選択してから、vShield ドライバを選択します。

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 5

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

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。ESX ホストはアンインストール時に再起動します。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 モードであった場合は、自動アンインストールの完了後に vShield App 仮想マシンを手動で削除してください。

インスタンスがアンインストールされました。

vShield Edge のアンインストール

vShield Edge は vSphere Client を使用してアインストールできます。

開始する前に

Enterprise Administrator または vShield Administrator ロールが割り当てられている必要がある。

手順

1 vSphere Client にログインします。

2 インベントリ ツリーからデータセンター リソースを選択します。

3 [ネットワーク仮想化] タブをクリックします。.

4 [エッジ] をクリックします。

5 [削除] （  ）アイコンをクリックします。

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 6

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デ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

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 インタフェイ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 インターフェイスから実行するか、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 Manager のスナップショットを作成し、アップグレードに失敗した場合に元に戻すことができるようにします。

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。

vShield Manager バージョン 5.0 から 5.1.2 へのアップグレード

vShield Manager バージョン 5.1 以降には、少なくとも 2.5 GB のディスク領域が必要です。メンテナンス バンドルを実行して、アップグレードした vShield Manager でディスク領域を使用できるようにする必要があります。

手順

1 メンテナンス バンドルのインストールによる空きディスク領域の増加 (P. 40)

アップグレード プロセスでは、`/common` パーティションに少なくとも 2.5 GB の空き容量が必要です。vShield メンテナンス バンドルを適用すると、vShield Manager のディスク領域が使用できるようになります。vShield Manager プロセスが停止され、ファイル システムのクリーンアップ アクティビティが完了すると、プロセスが再開されます。

2 vShield Manager のバージョン 5.1 以降へのアップグレード (P. 41)

3 アップグレード後のバックアップの作成 (P. 42)

バージョン 5.1 以降の vShield Manager では、その仮想ハードウェアへのアップグレードが必要です。vShield Manager 5.0.x 以前のバージョンでは、この仮想ハードウェアのアップグレードは、vShield アップグレード プロセスの一環として自動的には実行されません。スケーラビリティとパフォーマンスの向上、ログ記録とレポートの機能強化を目的としたアーキテクチャの変更を利用するには、vShield Manager の仮想ハードウェアのアップグレードが必要です。アーキテクチャの変更には、64 ビットのサポート、2 つの vCPU、8 GB RAM、より大きな仮想ディスク、その他の仮想ハードウェア プロパティなどが含まれます。

4 アップグレード後のバックアップのリストア (P. 42)

vShield Manager のバックアップをリストアします。

5 5.1.2a メンテナンス パッチのインストール (P. 43)

vShield バージョン 5.1.2 を使用している場合、5.1.2a パッチをインストールする必要があります。

メンテナンス バンドルのインストールによる空きディスク領域の増加

アップグレード プロセスでは、`/common` パーティションに少なくとも 2.5 GB の空き容量が必要です。vShield メンテナンス バンドルを適用すると、vShield Manager のディスク領域が使用できるようになります。vShield Manager プロセスが停止され、ファイル システムのクリーンアップ アクティビティが完了すると、プロセスが再開されます。

開始する前に

注意　vShield Manager アプライアンスの既存のログ、フロー監視データ、システム イベントおよび監査ログは、このプロシージャの一環として削除されます。システム イベントと監査ログは、メンテナンス バンドルを適用する前に適切な REST API 呼び出しを使用することで取得できます。テクニカル サポート ログ バンドルには、このプロシージャのログ メッセージが含まれています。

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。

2 有効モードに切り替えます。

3 ログインしたら、`show filesystems` コマンドを入力します。

メンテナンス バンドルをインストールするには、 `/common` パーティションに少なくとも 5% の空き領域が必要です。

4 `show manager log follow` コマンドを入力します。このコンソールを開いたままにして、残りの手順を実行してください。

5 vShield Manager から参照できる場所に vShield のメンテナンス バンドルをダウンロードします。メンテナンス バンドル ファイルの名前は、`VMware-vShield-Manager-upgrade-bundle-maintenance-`<bundlebuildNumber>`.tar.gz` のようになります。

6 vShield Manager インベントリ パネルで、 [設定とレポート] をクリックします。

7 [Updates] タブをクリックします。

8 [Upload Settings] をクリックします。

9 [Browse] をクリックして、`VMware-vShield-Manager-upgrade-bundle-maintenance-`<bundlebuildNumber>`.tar.gz` ファイルを選択します。

10 [Open] をクリックします。

11 [Upload File] をクリックします。

12 [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。

13 [Confirm Install] をクリックします。

14 CLI で、**show manager log** コマンドの出力に従います。メッセージ **maintenance-fs-cleanup: Filesystem cleanup successful** と表示されたら、vShield Manager ユーザー インターフェイスにログインします。

アップグレード プロセスによって vShield Manager サービスが再開されるため、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開されません。

15 vShield Manager の CLI にログインし、有効モードに切り替えて、**show filesystems** コマンドを実行してアップグレードのために少なくとも 2.5 GB の空き領域があることを確認します。

vShield Manager のバージョン 5.1 以降へのアップグレード

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 ファイルの名前は、**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 [設定とレポート] 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 Upgrade Bundle] 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 再起動した後で、vShield Manager にログインし直して [Updates] タブをクリックします。[インストールされたリリース] パネルに、インストールしたバージョン 5.1.2 が表示されます。

前のリリースからの vShield App ルールは、以下のようにアップグレードされます。

前バージョンの ファイアウォール機能	バージョン 5.1 へのアップグレードの結果
ファイアウォール ルールは、データセンター、クラスタ、およびポート グループの各レベルで許可されました	ファイアウォール ルールはネーム スペース レベル (データセンター、独立したネームスペースのポート グループ、および仮想ワイヤの各レベル) で許可されました アップグレード後、ネーム スペース以外のコンテキストからのファイアウォールは対応するデータセンターに移動されます。移行したルールは、次の順序でデータセンターのルールとマージされます。 ■ データセンター高 ■ クラスタ ■ ネームスペース以外のポート グループまたは dvport グループ ■ データセンター低 ■ データセンター デフォルト
ファイアウォール ルールは、未処理の IP アドレスと MAC アドレス、およびポート プロトコルとプロトコル サブタイプをサポートしました	ファイアウォール ルールは、IPset、MACset、およびセキュリティ グループのみをサポートします アップグレード後、IPset、MACset、またはサービスは、必要に応じて内部で作成されます。作成されるコンテナの名前は、次の命名規則に従います。 ■ IPset/MACset: <ip/macValue>-<contextName> ■ サービス： <protocolName-portNumber>-<contextName> または <protocolName>-<subtypeName>-<contextName>

前バージョンの ファイアウォール機能	バージョン 5.1 へのアップグレードの結果
ファイアウォール ルールには高および低の優先ルールが含まれていました。ネームスペース以外のポート グループ ルールには優先なしがありました。	高および低の優先ルールはサポートされません。 アップグレード後、デフォルト以外のすべての優先ルールは優先なしに変更されます。
単一の SpoofGuard グローバル設定がインベントリ内のすべてのデータセンターに適用されました	SpoofGuard グローバル設定は各ネームスペースに適用されます。アップグレード後、SpoofGuard の設定値はネームスペース単位で変更できます。

また、アップグレードが削除される前に、すべてのファイアウォールの履歴とフローが記録されます。

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。

アップグレード後のバックアップの作成

バージョン 5.1 以降の vShield Manager では、その仮想ハードウェアへのアップグレードが必要です。vShield Manager 5.0.x 以前のバージョンでは、この仮想ハードウェアのアップグレードは、vShield アップグレード プロセスの一環として自動的には実行されません。スケーラビリティとパフォーマンスの向上、ログ記録とレポートの機能強化を目的としたアーキテクチャの変更を利用するには、vShield Manager の仮想ハードウェアのアップグレードが必要です。アーキテクチャの変更には、64 ビットのサポート、2 つの vCPU、8 GB RAM、より大きな仮想ディスク、その他の仮想ハードウェア プロパティなどが含まれます。

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 [構成] タブをクリックします。

3 [Backups] をクリックします。

4 バックアップの保存先であるシステムのホスト IP アドレスまたは名前を入力します。

5 バックアップ システム （ftp/sftp サーバ） 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。

6 [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。

7 [Filename Prefix] にテキスト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 **ppdb**<HH_MM_SS_DayDDMonYYYY> となります。

8 送信先でサポートされるプロトコルに応じて、 [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。

9 [Save Settings] をクリックしてから [Backup] をクリックします。

10 [View Backups] をクリックして、バックアップが作成されていることを確認します。

アップグレード後のバックアップのリストア

vShield Manager のバックアップをリストアします。

手順

1 vShield Manager をパワーオフします。

2 5.1.2 vShield Manager .OVA インストール パッケージをダウンロードします。

3 新しい vShield Manager を vSphere インベントリにデプロイし、既存の vShield Manager を置き換えます。

4 新しい vShield Manager をパワーオンして初期セットアップを行い、現在パワーオフしている Shield Manager と同じ IP アドレスを指定します。

5 vShield Manager バックアップ ページを、現在 ftp/sftp サーバに格納されているバックアップを表示するように構成します。

6 前に作成された vShield Manager のバックアップを指定して、 [リストア] をクリックします。

5.1.2a メンテナンス パッチのインストール

vShield バージョン 5.1.2 を使用している場合、5.1.2a パッチをインストールする必要があります。

手順

1 vShield Manager から参照できる場所に vShield 5.1.2a メンテナンス パッチをダウンロードします。パッチのバンドル ファイルの名前は、 [VMware-vShield-Manager-upgrade-bundle-maintenance-] <bundlebuildNumber> [.tar.gz] のようになります。

2 vShield Manager 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 [Updates] タブをクリックします。

4 [Upload Settings] をクリックします。

5 [参照] をクリックして、手順 1 でダウンロードしたファイルを選択します。

6 [開く] 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。

vShield Manager バージョン 5.1 から 5.1.2 へのアップグレード

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 ファイルの名前は、**`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 [設定とレポート] をクリックします。

3 [アップデート] タブをクリックします。

4 [設定のアップロード] をクリックします。

5 [参照] 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 [開く] をクリックします。

7 [アップグレード バンドルのアップロード] をクリックします。

8 [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。

9 [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。

10 再起動した後で、vShield Manager にログインし直して [Updates] タブをクリックします。[インストールされたリリース] パネルに、インストールしたバージョン 5.1.2 が表示されます。

11 vShield Manager から参照できる場所に vShield 5.1.2a メンテナンス パッチをダウンロードします。パッチのバンドル ファイルの名前は、 [VMware-vShield-Manager-upgrade-bundle-maintenance-] <bundlebuildNumber> [.tar.gz] のようになります。

12 手順 2 から手順 4 まで行います。

13 [参照] をクリックして、手順 11 でダウンロードしたファイルを選択します。

14 手順 6 から手順 9 まで行います。

vShield Manager バージョン 5.5 へのアップグレード

開始する前に

vShield Manager 5.5 にはバージョン 5.1.2 からのみアップグレードできます。環境内に以前のバージョンの vShield Manager がインストールされている場合は、vShield Manager をバージョン 5.5 にアップグレードする前にバージョン 5.1.2 にアップグレードする必要があります。

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 ファイルの名前は、**`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 パネルで [設定 & レポート] をクリックします。

3 [アップデート] タブをクリックします。

4 [設定のアップロード] をクリックします。

5 [参照] 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 [開く] をクリックします。

7 [アップグレード バンドルのアップロード] をクリックします。

8 [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。

9 [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。

10 再起動した後で、vShield Manager にログインし直して [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バージョン 5.5 が表示されます。

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。

開始する前に

vShield App バージョン 4.1 を使用している場合は、バージョン 5.1 以降にアップグレードする前にバージョン 5.0 または 5.0.1 にアップグレードする必要があります。

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クリックします。

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 [Intstall] をクリックします。

注意 vShield App のアップグレード中は ESXi ホストはメンテナンス モードになり、再起動されます。ESXi ホストの仮想マシンが移行されているか (DRS または vMotion を使用)、またはホストをメンテナンス モードにできるように仮想マシンがパワーオフされていることを確認します。

次に進む前に

アップグレードした各ルールを検査して、意図どおり機能することを確認します。新しいファイアウォール ルールの追加の詳細については、『 [vShield 管理ガイド] 』を参照してください。

Upgrade vShield Edge from 5.0.x to 5.5

You must upgrade vShield Edge on each port group in your datacenter. You cannot upgrade vShield Edge if the same backend IP address has been configured under different listeners with different ports.

vShield Edge 5.1 and later is not backward compatible and you cannot use 2.0 REST calls after the upgrade.

During the vShield Edge upgrade, there will be a brief network disruption for the networks that are being served by the given vShield Edge instance.

Prerequisites

You must have been assigned the Enterprise Administrator or vShield Administrator role. If you have vShield Edge 5.0.x, each 5.0.x vShield Edge instance on each portgroup in your datacenter must be upgraded to 5.5.

Procedure

1 Log in to the vSphere Client.

2 Click the portgroup on which the vShield Edge is deployed.

3 Click the [vShield Edge] tab.

4 Click [Upgrade] .

5 View the upgraded vShield Edge.

a Select the datacenter corresponding to the port group on which you upgraded the vShield Edge.

b Click the [Network Virtualization] tab.

c Click [Edges] .

vShield Edge is upgraded to the compact size. A system event is generated to indicate the ID for each upgraded vShield Edge instance.

What to do next

IMPORTANT Firewall rules from the previous release are upgraded with some modifications. Inspect each upgraded rule to ensure it works as intended. For information on adding new firewall rules, see the vShield Administration Guide.

If a user's scope in a previous release was limited to a port group which had a vShield Edge installation, the user is automatically granted access to that vShield Edge after the upgrade.

vShield Endpoint 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 [インベントリ] - [ホストおよびクラスタ] 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。

[全般] 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 [更新] を選択します。

6 [vShield Endpoint] チェックボックスを選択します。

7 [インストール] 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 をアップグレードする前に 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 Data Security 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。

インストール問題のトラブルシューティング 7

このセクションでは、インストール問題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 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 のインストールは、以前の不完全なインストールや、前のバージョンのアンインストール時の問題のために失敗することがあります。

解決方法

1 vShield App の自動アンインストールから開始します。第 5 章「vShield コンポーネントのアンインストール (P. 37)」を参照してください。

2 SSH クライアントにログインして次のコマンドを入力することにより、ESX ホストに必要なモジュールがロードされていることを確認します。

```
esx01# esxcfg-module -l | grep -i dvf

dvfilter 2 72

vmkapiv1_0_0_0_dvfilter_shim0 8
```

3 必要なモジュールがロードされていない場合は、次のコマンドを入力してそれらのモジュールをロードします。

```
#esxcfg-module -e /usr/lib/vmware/vmkmod/dvfilter

#esxcfg-module -v -e /usr/lib/vmware/vmkmod/vmkapiv1_0_0_0_dvfilter_shim
```

4 vShield Manager の CLI に admin としてログインし、次のコマンドを入力して Web インターフェイスをリセットします。

enable > config t > **no web-manager**

5 **no web-manager** コマンドが完了したら、次のコマンドを入力して Web サービスを再開します。

enable > config t > **web-manager**

vShield Manager ユーザー インターフェイスにログインしていた場合は、Web サービスが再開した後にもう一度ログインします。

6 (オプション) vShield App のインストール時に次のエラーが表示された場合は、ESX ホストを再起動します。

vShield App installation encountered error while installing vib

7 次の手順に従って、インストール時に作成された vmservice-vswitch を削除します。

a vSphere Client にログインします。

b インベントリ ツリーから ESX ホストを選びます。

c [構成] タブをクリックします。

d [ソフトウェア] パネルで、 [ネットワーク] をクリックします。

e [Standard Switch:vmservice-vswitch] 領域で、 [削除] をクリックします。

8 次の手順に従って、ホストの [Net.DVFilterBindIpAddress] プロパティを削除します。

a vSphere Client で、インベントリ ツリーから ESX ホストを選択します。

b [構成] タブをクリックします。

c [ソフトウェア] パネルで、 [詳細設定] をクリックします。

d [詳細設定] ダイアログ ボックスで、 [Net] をクリックします。

e Net. [DVFilterBindIpAddress] フィールドが空白になっていることを確認します。

9 もう一度 vShield App をインストールします。「vShield App のインストール (P. 26)」を参照してください。

vShield Data Security のインストールの失敗

問題

vShield Data Security のインストール中、サービス仮想マシンをインストールするときにエラーが表示され、vSphere Client について次のようなエラー メッセージが表示されました。

```
NAME=deploy OVF template Target=VMWARE-Data Security-<xxxx> Status=operation timed out
```

.

原因

vShield Manager の DNS セットアップと vCenter Server のホストの DNS セットアップの間に一貫性がない可能性があります。

解決方法

ホストのセットアップと一致するように vShield Manager の DNS のセットアップを変更してください。

インデックス