

クイックスタートガイド

vShield Zones 1.0

JA-000166-00



最新情報を反映したテクニカルドキュメントは、VMware の Web サイトにてご覧いただけます。

<http://www.vmware.com/jp/support/>

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

本書に関するコメントがございましたら、次のメールアドレスにご連絡ください。

docfeedback@vmware.com

© 2009 VMware, Inc. All rights reserved. 本製品は、米国および国際的な著作権法および知的財産法によって保護されています。VMware の製品は、<http://www.vmware.com/go/patents> のリストに表示されている 1 つまたは複数の特許の対象です。

VMware、VMware ボックスロゴとデザイン、Virtual SMP および VMotion は、VMware, Inc. の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

目次

本書について	5
vShield Zones のインストール	7
要件	7
vShield Zones のコンポーネント	8
vShield Zones のインストール前に行う ESX のネットワーク構成の評価	8
vShield Zones のインストール	8
vShield Zones 仮想アプライアンスを入手する	8
vSphere Client を使用して vShield Manager を仮想マシンとしてインストールする	9
vShield イメージをインストールしてテンプレートに変換する	10
vShield Manager ユーザー インターフェイスにログインしてシステムの構成を行う	10
vShield を追加する	11
継続的な検出を有効にしてゲストの仮想マシンのトラフィックを特定する	12
vShield のための追加の vCenter 構成	13
vShield Zones 仮想マシンのパワーオフ	14
vShield の自動インストールの概要	14
vShield のインストールにより作成されるポートグループについて	15

本書について

『クイック スタート ガイド』では、VMware® Virtual Infrastructure 環境への vShield Zones のインストールについて説明します。

対象読者

本書は、vShield Zones をインストールまたは使用する方を対象にしています。本書の情報は、仮想マシンテクノロジーおよびデータ センターの運用に精通した、経験の豊富な Windows または Linux システムの管理者向けに記載されています。また本書は、vCenter Server 4.0、VMware ESX 4.0、vSphere Client を含む VMware Virtual Infrastructure に精通していることも前提にしています。

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。

VMware Infrastructure のドキュメント

vShield Zones のドキュメント セットは、次のドキュメントで構成されています。

- vShield Zones 管理ガイド
- vShield Zones クイック スタート ガイド
- vShield Zones の概要

また、vCenter Server および ESX のドキュメント を組み合わせたドキュメント セットもご利用いただけます。

テクニカル サポートおよび教育リソース

次のセクションでは、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によるサポート

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/jp/support/phone_support 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 教育サービスの有償トレーニングでは、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 プログラムおよび実装のベスト プラクティスについては、VMware コンサルティング サービスがご使用の仮想環境の評価、計画、構築、および管理に役立つサービスを提供しています。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 サービスについては、<http://www.vmware.com/jp/services> をご覧ください。

vShield Zones のインストール

vShield Zones は、ファイアウォールによる保護とトラフィックの分析を行うことにより、VMware vCenter Server 仮想インフラストラクチャを保護します。vShield Zones 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的に行われます。

この章には、次のトピックが含まれています。

- 「要件」 (P.7)
- 「vShield Zones のコンポーネント」 (P.8)
- 「vShield Zones のインストール前に行う ESX のネットワーク構成の評価」 (P.8)
- 「vShield Zones のインストール」 (P.8)
- 「vShield のための追加の vCenter 構成」 (P.13)
- 「vShield Zones 仮想マシンのパワーオフ」 (P.14)
- 「vShield の自動インストールの概要」 (P.14)
- 「vShield のインストールにより作成されるポートグループについて」 (P.15)

要件

vShield Zones をインストールするには、次のものがが必要です。

- vCenter Server 4.0 以降を実行しているシステム
- 1つ以上の ESX 4.0 が稼働している環境
- vSphere Client を備えた PC
- 仮想マシンを追加およびパワーオンするための権限
- 仮想マシンのファイルを格納するデータストアへのアクセスが可能であることと、そのデータストアにファイルをコピーするためのアカウント権限
- vShield Manager OVF ファイルおよび vShield OVF ファイル
- インストールする各 vShield インスタンスの管理インターフェイス用固定 IP アドレス
- vShield Manager 管理インターフェイス用の単一の固定 IP アドレス
- vShield Manager ユーザー インターフェイスへのアクセスに使用する Web ブラウザでのクッキーの有効化

vShield Zones のコンポーネント

vShield Zones ソリューションは、次のコンポーネントで構成されます。

- **vShield Manager:** 分散したすべての vShield インスタンスを管理する vShield Zones 管理センターです。vShield の監視、構成、およびソフトウェアのアップデートを行うことができます。
- **vShield :** トラフィック フローを調査し、ファイアウォールによる保護を提供する、vShield Zones のアクティブなセキュリティ コンポーネントです。vShield は、保護する ESX ホストにそれぞれインストールします。vShield はトラフィックの経路内にインストールされ、ESX ホストのすべての送受信トラフィックと、ホスト上の仮想マシン間のすべてのトラフィックを監視します。

vShield Zones のインストール前に行う ESX のネットワーク構成の評価

vShield Zones を vCenter Server 環境にインストールする前に、ESX ホストのネットワーク構成について検討します。少なくとも、各ホストに 1 つ以上の関連付けられた物理 NIC と 1 つの vSwitch があり、VMKernel、サービス コンソール、および仮想マシンをホストしている必要があります。より堅牢な環境にするためには、ESX ホストに複数の専用の物理 NIC と複数の vSwitch を用意して、VMKernel とサービス コンソールを仮想マシンから切り離します。

vShield Zones アプライアンスは仮想マシンとして ESX ホストにインストールされます。ただし、vShield のインストールでは多少計画を立てる必要があります。vShield は、専用の NIC を備えた任意の vSwitch にインストールできます。vShield のインストールでは、仮想マシンが元の vSwitch からクローンの vSwitch に移動されます。その後、vShield は元の vSwitch とクローンの vSwitch の間にインストールされ、仮想マシンの送受信トラフィックをすべてキャプチャできるようになります。元の vSwitch が NIC を保持し、新しい vSwitch は NIC には関連付けられません。このため、さまざまな仮想マシンをホストする複数の vSwitch を備えた ESX ホストの場合は、vSwitch ごとに vShield が必要です。vShield がインストールされていない vSwitch に接続された仮想マシンは、vShield Zones によって保護されません。

複数の vShield のインストールを簡素化するには、vShield OVF をインストールしてから、基にする vShield 仮想マシンをテンプレートとしてデプロイします。このテンプレートが vShield Manager によって参照され、vShield Manager ユーザー インターフェイスから複数の vShield を vCenter Server 環境にインストールすることが可能になります。vShield のインストール プロセスの詳細については、「[vShield の自動インストールの概要](#)」(P. 14) を参照してください。

注 vShield Zones システムは仮想マシンの保護を目的として設計されているため、VMKernel やサービス コンソールは保護しません。

vShield Zones のインストール

vShield Zones のインストールでは複数の手順を実行します。vShield Zones のインストールを滞りなく行うには、次のタスクを順番に実行してください。

vShield Zones 仮想アプライアンスを入手する

vShield Zones 仮想アプライアンスは、OVF (Open Virtualization Format) を使用してパッケージにまとめられています。このパッケージによって、vSphere Client を使用して仮想アプライアンスをデータストアや仮想マシンのインベントリにインポートできるようになり、インストールが簡素化されます。

1 つの vShield Manager と 1 つの vShield で構成される vShield Zones ソフトウェア パッケージを入手するには、VMware の顧客担当チームにご連絡ください。1 つの vShield 仮想アプライアンスを使用して、複数の vShield をインストールできます。

パッケージを入手したら、それを vSphere Client がインストールされている PC にダウンロードします。

vSphere Client を使用して vShield Manager を仮想マシンとしてインストールする

vShield Manager 仮想マシンをインストールするには、vShield Manager 用のポート グループを作成する必要があります。

vCenter Server インベントリに仮想マシンとして vShield Manager を追加するには

- 1 vSphere Client にログインします。
- 2 インベントリ パネルから ESX ホストを選択します。
- 3 **[File] - [Deploy OVF Template]** の順に選択します。
OVF テンプレートのデプロイ ウィザードが表示されます。
- 4 **[Deploy from file]** をクリックし、次に **[Browse]** をクリックして、vShield Manager OVF ファイルが含まれているフォルダを PC から探します。
- 5 ウィザードを完了します。
vShield Manager がインベントリにインストールされます。
- 6 vShield Manager をインストールした ESX ホスト上に、vShield Manager 用の **vsmgmt** という名前のポートグループを作成します。
インストールされる各 vShield はこのポート グループ名を認識するため、vShield のインストール中に vShield が vShield Manager 仮想マシンを移動することがなくなります。
- 7 vShield Manager がパワーオン時に接続してネットワーク ラベルを vsmgmt ポート グループに設定するように、vShield Manager 仮想マシンの設定を編集します。
 - a vShield Manager 仮想マシンを右クリックして、**[Edit Settings]** をクリックします。
[vShield Manager - Virtual Machine Properties] ダイアログ ボックスが開きます。
 - b **[Hardware]** タブで **[Network Adapter 1]** をクリックします。
 - c [Device Status] の下にある **[Connect at power on]** を選択します。
 - d **[Network label]** ドロップダウン リストで **[vsmgmt]** を選択します。
 - e **[OK]** をクリックしてウィンドウを閉じます。
- 8 vShield Manager 仮想マシンをパワーオンします。
- 9 右側のペインで **[Console]** タブをクリックし、vShield Manager CLI を開きます。
起動には数分かかる場合があります。
- 10 **manager login** プロンプトが表示されたら、ユーザー名 **admin** およびパスワード **default** を使用して CLI にログインします。
- 11 **setup** コマンドを実行して CLI セットアップ ウィザードを起動します。

CLI セットアップ ウィザードに従って、vShield Manager の管理インターフェイス用の IP アドレスの割り当てや、デフォルト ネットワーク ゲートウェイの識別を行います。管理インターフェイスの IP アドレスには、インストールされているすべての vShield インスタンスと、システム管理用の Web ブラウザからアクセスできる必要があります。

```
manager> setup
```

```
Use ctrl-d to abort configuration dialog at any prompt.
Default settings are in square brackets '['].
```

```
Hostname [manager]:
IP Address [10.115.216.66/255.255.255.0]:
Default gateway [10.115.219.253]:
Old configuration will be lost, and system needs to be rebooted
Do you want to save new configuration (y/[n]):y
Please log out and log back in again.
```

この時点でログアウトする必要はありません。vShield Manager のインストールが完了します。

- 12 デフォルト ゲートウェイに ping を実行してネットワーク接続を確認します。

```
manager> ping 10.115.219.253
```

- 13 使用する PC から vShield Manager の IP アドレス宛てに ping を実行し、その IP アドレスにアクセスできるかどうかを検証します。

vShield イメージをインストールしてテンプレートに変換する

vShield を仮想マシンとしてインストールし、テンプレートに変換します。vShield 仮想マシンがテンプレート形式に変換されると、vShield Manager が vShield を複数の ESX インスタンスにインストールするために、そのテンプレートを参照できるようになります。

vShield を vCenter Server に追加してテンプレートに変換するには

- 1 vSphere Client にログインします。
- 2 インベントリ パネルから ESX ホストを選択します。
- 3 **[File] - [Deploy OVF Template]** の順に選択します。
OVF テンプレートのデプロイ ウィザードが表示されます。
- 4 **[Deploy from file]** をクリックし、次に **[Browse]** をクリックして、vShield OVF ファイルが含まれているフォルダをクライアント マシンから探します。
- 5 ウィザードを完了します。
これで vShield がインベントリにインストールされます。



注意 この時点では、vShield 仮想マシンのパワーオンや編集は行わないでください。この時点で仮想マシンのパワーオンや編集を行うと、無限ループなどのネットワークの問題が発生する可能性があります。

- 6 ウィザードによるインストールが完了したら、vShield インスタンスを仮想マシン テンプレートに変換します。
このテンプレートにより、vShield Manager ユーザー インターフェイスから複数の vShield インスタンスを自動的にインストールできるようになります。

vShield Manager ユーザー インターフェイスにログインしてシステムの構成を行う

vShield Manager 仮想アプライアンスがインストールされ、vShield イメージがテンプレートに変換されたら、vShield Manager ユーザー インターフェイスにログインし、vCenter Server で認証されるように vShield Manager を構成します。この認証により、vShield Manager が vCenter Server インベントリを表示したり、vShield インスタンスをインストールしたり、リソースを保護するためにファイアウォールを構成したりすることが可能になります。

vShield Manager ユーザー インターフェイスにログインするには

- 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。
IP アドレスの先頭に、**https** を付加する必要があります。
- 2 セキュリティ証明書を受け入れます。
vShield Manager のログイン画面が表示されます。
- 3 ユーザー名 **admin** とパスワード **default** を使用して、vShield Manager ユーザー インターフェイスにログインします。

右側のフレームにある **[Configuration] - [vCenter]** タブに対応する vShield Manager ユーザー インターフェイスが開きます。初回ログイン時には、まだ vCenter Server と通信の同期をとっていないため、vShield Manager には何の情報も表示されません。

- 4 **[vCenter]** タブのフォームに次のように入力します。

フィールド	操作
IP address/Name	vCenter Server の IP アドレスを入力します。
User Name	vSphere Client ユーザー名を入力します。
Password	vSphere Client ユーザー名に関連付けられたパスワードを入力します。

- 5 **[Commit]** をクリックします。

vShield Manager が vCenter Server に接続し、ログインして、VMware Virtual Infrastructure SDK にアクセスします。vShield Manager 画面の左側にあるインベントリ ツリーが、vSphere Client の [Hosts and Clusters] インベントリ ツリービューと一致します。

注 vShield Zones インベントリ パネルには、vShield Manager は表示されません。**[Settings & Reports]** オブジェクトが、インベントリ パネル内の vShield Manager を表します。

vShield を追加する

vShield テンプレートからクローンを作成することにより、vShield を vCenter Server インベントリや vShield Zones インベントリに追加できます。

NIC を備えている vSwitch ごとに 1 つずつ vShield インスタンスをインストールする必要があります。vShield がインストールされていない vSwitch に接続された仮想マシンは、vShield Zones によって保護されません。

注 vShield を vNDS (vNetwork Distributed Switch) にインストールする場合は、『vShield Zones 管理ガイド』を参照してください。

vShield を追加するには

- 1 vShield Manager にログインします。
- 2 インベントリ ツリーで、保護する ESX ホストをクリックします。
- 3 右側のフレームの上に表示されている **[Install vShield]** タブをクリックします。
- 4 **[Configure install parameters]** をクリックします。
- 5 フォームに次のように入力します。

フィールド	操作
Select from available vShields	このフィールドは空白のままにします。このフィールドは、テンプレートを作成せずに vShield を追加する場合にのみ使用します。
Select template to clone	このドロップダウン メニューをクリックして、vShield テンプレートを選択します。
Select a datastore to place clone	このドロップダウン メニューをクリックして、vShield クローンを格納するデータストアを選択します。
Enter a name for the clone	vShield クローンの一意の名前を入力します。この名前は vSphere Client と vShield Manager の各インベントリに表示されます。
Specify IP Address of vShield VM	vShield の管理ポートに割り当てる IP アドレスを入力します。
Specify IP Mask for vShield	割り当てた IP アドレスに関連付ける IP サブネット マスクを入力します。
Specify IP Address of Default Gateway for vShield	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。

フィールド	操作
Specify Secure Key for vShield (leave blank for default)	(任意) 安全な通信のために vShield と vShield Manager の間で使用するキーを入力します。デフォルトでは、このフィールドの入力内容はマスクされます。このデフォルトシードは、vShield と vShield Manager の間の暗号化された通信に使用されます。キーはネットワーク上で共有されることはありません。
Select a vSwitch to shield	このドロップダウンメニューをクリックして、保護する vSwitch を選択します。保護することができる vSwitch は、付随する表中で緑色に強調表示されます。

- 6 フォームの上にある **[Continue]** をクリックします。

インストールの概要を示す画面が表示されます。この画面には、ESX に vShield をインストールする前後の例についての説明が表示されます。

注 この説明は固定のものであり、実際の仮想ネットワークを直接反映したものではありません。画面の右側にある番号付きのインストールスクリプトは、実際のインストール手順を示しています。

- 7 **インストール** をクリックします。

vSphere Client ウィンドウの下部にある **[Recent Tasks]** ステータス ペインから、vShield のインストール手順を実行できます。インストールプロセスの詳細については、「[vShield の自動インストールの概要](#)」(P. 14) を参照してください。

これで vShield のインストールが完了します。

- 8 インストールが完了したら、vSphere Client を開きます。

- 9 インベントリ内の vShield を探します。

vShield がパワーオンされている必要があります。

継続的な検出を有効にしてゲストの仮想マシンのトラフィックを特定する

vShield Manager と vShield がインストールされ、vShield が vShield Manager と通信するようになったら、vShield に対する継続的な検出処理を有効にして、仮想マシンを保護する必要があります。

仮想マシンのトラフィックの継続的な検出を有効にするには

- 1 vShield Manager にログインします。
- 2 インベントリ ツリーで vShield インスタンスをクリックします。
- 3 **[VM Discovery]** タブをクリックします。
- 4 **[Automated]** という小見出しをクリックします。
- 5 **[Scheduled Discovery Status]** ドロップダウンメニューで、**[Continuous]** を選択します。

このフォーム内のその他のフィールドには入力しないでください。

- 6 **[OK]** をクリックします。

検出処理が開始します。検出が継続的に行われ、アプリケーションおよびプロトコルの仕様を基準にしてトラフィックフローが特定されます。

- 7 検出の結果を表示するには、**[VM Discovery] - [Results]** の順に選択します。

検出されたトラフィックは仮想マシンの IP アドレスごとに分けられます。検出された各仮想マシンは **[VM Inventory]** タブに保存され、vShield Manager 内のデータセンターレベルやクラスタ コンテナレベルのほかに、仮想マシンレベルでも表示できます。

vShield のための追加の vCenter 構成

VMware HA 機能または VMware DRS 機能を有効にした場合は、vShield Zones 仮想アプライアンスの移動を無効にする必要があります。これは、各 vShield Zones コンポーネントをインストールしたあとに実行する必要があります。

vShield Manager 仮想アプライアンスの移行は、VMotion を使用して問題なく行うことができます。

VMware HA または VMware DRS による vShield Zones 仮想アプライアンスの移動を無効にするには

- 1 vSphere Client にログインします。
- 2 vShield Zones 仮想アプライアンスを含むクラスタを右クリックし、**[Edit Properties]** をクリックします。
[Admin Settings] ダイアログ ボックスが開きます。
- 3 VMware HA の下にある **[Virtual Machine Options]** をクリックします。
リストで vShield Manager と vShield を探します。
- 4 個々の vShield Zones 仮想アプライアンスについて、次の値を選択します。
 - **[VM Restart Priority]: Disabled**
 - **[Host Isolation Response]: Leave VM powered on**
- 5 DRS を有効にした場合は、VMware DRS の下にある **[Virtual Machine Options]** をクリックします。
リストで vShield Manager と vShield を探します。
- 6 個々の vShield Zones 仮想アプライアンスの **[Automation Level]** で **[Disabled]** を選択します。
- 7 すべての vShield Zones 仮想アプライアンスが構成されたあとで、**[OK]** をクリックします。

vShield のデフォルトの動作では、オペレータまたは VMotion が仮想マシンの移行を試行しているときにエラーが発生します。このエラーは、サーバが仮想イントラネットに接続していることを示します。この仮想イントラネットは、vShield が保護する側の vSwitch 上で仮想マシンが接続しているネットワークです。この vSwitch は物理 NIC に接続していません。vShield は、物理 NIC に接続しているネットワークの保護しない側に、トラフィックをブリッジ接続します。

VMotion を有効にして仮想イントラネットをチェックしないようにするには

- 1 vCenter Server を実行しているマシン上で vpxd.cfg ファイルを探します。デフォルトでは、このファイルは C:\Documents and Settings\All Users\Application Data\VMware\VMware vCenter Server にインストールされます。
- 2 vpxd.cfg ファイルをテキスト エディタで編集します。
config セクションのサブレベルとして、vpxd セクションと同じレベルに次の行を追加します。


```
<migrate>
  <test>
    <CompatibleNetworks>
      <VMOnVirtualIntranet>false</VMOnVirtualIntranet>
    </CompatibleNetworks>
  </test>
</migrate>
```
- 3 vpxd.cfg ファイルを保存します。
- 4 VMware vCenter Server サービスを再起動します。サービス メニューにアクセスするには、**[コントロールパネル]-[管理ツール]-[サービス]** を開きます。

vShield Zones の詳細な構成については、『vShield Zones 管理ガイド』を参照してください。

vShield Zones 仮想マシンのパワーオフ

vShield Zones 仮想マシンはいつでもパワーオフできます。vShield Zones 仮想マシンをパワーオフすると、仮想マシンがパワーオンされるときに、最後に保存された構成が使用されます。

vShield Zones 仮想マシンをパワーオフするには

- 1 vSphere Client で、インベントリ パネルから vShield Zones 仮想マシンを選択します。
- 2 **[Console]** タブをクリックして vShield Zones CLI を開きます。
- 3 CLI にログインします。
- 4 ログインのあと、**enable** と入力して特権モードにします。
- 5 **shutdown** と入力します。
- 6 CLI のシャットダウンが完了したあと、インベントリ パネルから仮想マシンを右クリックし、**[Power]-[Power Off]** の順に選択します。

vShield の自動インストールの概要

vShield を参照テンプレートからインストールする際は、次の手順でインストールプロセスが実行されます。

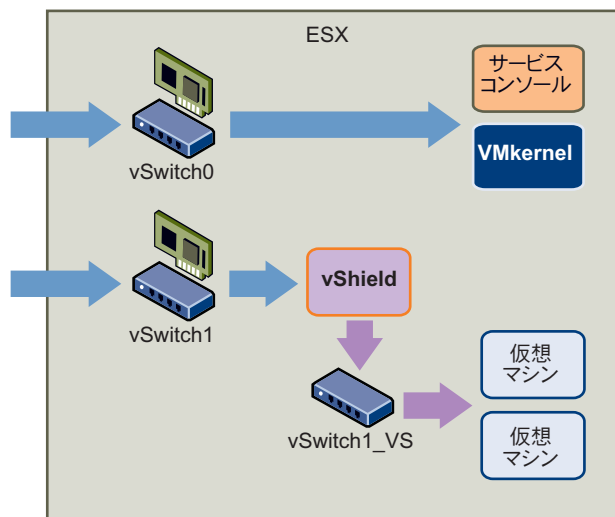
- 1 vSwitch ホストのクローンを作成します。
この vSwitch クローンに NIC は含まれません。vSwitch クローンの名前は、vSwitch ホスト名に **_VS** を付加した名前になります (例: vSwitch1_VS)。
- 2 保護ゾーンのポート グループ **VSprot_<vShield 名>** を作成し、このポート グループを vSwitch ホストに追加します。
- 3 vShield インスタンスの管理インターフェイス用の vSwitch ホスト上に、管理ポート グループ **VSgmt_<vShield 名>** を作成します。
- 4 保護ゾーンのポート グループ **VSunprot_<vShield 名>** を作成し、このポート グループを vSwitch クローンに追加します。

重要 仮想マシンを、保護ポート グループまたは非保護ポート グループに追加しないでください。これらのポート グループは無差別モードがオンの状態で構成されているため、通過するすべてのトラフィックが vShield から見えるようになっています。

- 5 vShield インスタンスに接続し、インスタンスをパワーオンします。
- 6 vShield 上の仮想インターフェイスを、保護ポート グループと非保護ポート グループに追加します。
- 7 仮想マシンを vSwitch ホストから vSwitch クローンに移動します。

同じ vSwitch 上に vShield Manager の仮想マシンがある場合、その仮想マシンは移動されません。vShield Manager のインストール中に、vShield Manager を配置するための **vsmgmt** というポート グループを作成しました。vShield のインストールプロセスではこのポート グループ名が識別され、このポート グループ内のすべての仮想マシンが無視されます。

図 1. vSwitch への vShield のインストール



vShield のインストールにより作成されるポート グループについて

vShield をインストールするには、2つのポート グループを作成する必要があります。これらのポート グループは、「非保護」および「保護」の信頼ゾーンを表します。非保護ゾーンは受信トラフィックを監視し、保護ゾーンは送信トラフィックを監視します。各ポート グループは vShield インターフェイス（非保護ゾーン用は「U0」、保護ゾーン用は「P0」）に接続します。これらのインターフェイスを作成済みのポート グループに接続することにより、vShield で受信トラフィックと送信トラフィックをすべて監視できます。

非保護ポート グループと保護ポート グループは、無差別モードが有効な状態で構成されます。無差別モードでは、ゲスト アダプタはすべての通過パケットを待機できます。無差別モード以外では、ゲスト アダプタは自身の MAC アドレスに関するトラフィックのみ待機します。デフォルトでは、ゲスト アダプタは無差別モード以外に設定されます。保護するためには、vShield からすべての通過トラフィックが見えるようにする必要があります。その他の仮想マシンをこれらのポート グループに追加しないでください。

