Quick Start Guide

vShield Zones 1.0 Update 1

EN-000166-00

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

About This Book

The *Quick Start Guide* provides information about installing vShield Zones into your VMware® Virtual Infrastructure environment.

Intended Audience

This book is intended for anyone who wants to install or use vShield Zones. The information in this book is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations. This book also assumes familiarity with VMware Virtual Infrastructure, including vCenter Server 4.0, VMware ESX 4.0, and the vSphere Client.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware Infrastructure Documentation

The following documents comprise the vShield Zones documentation set:

- *vShield Zones Administration Guide*
- *vShield Zones Quick Start Guide*
- *Introduction to vShield Zones*

You should also have access to the combined vCenter Server and ESX documentation set.

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Installing vShield Zones

vShield Zones provides firewall protection and traffic analysis to protect your VMware vCenter Server virtual infrastructure. vShield Zones virtual appliance installation has been automated for most virtual datacenters.

This chapter includes the following topics:

Requirements

Before installing vShield Zones, you must have:

- A system running vCenter Server 4.0 or later
- At least one running ESX 4.0 installation
- A PC with the vSphere Client
- Permissions to add and power on virtual machines
- Access to the datastore where you store virtual machine files, and the account permissions to copy files to that datastore
- vShield Manager and vShield agent OVF files
- A static IP address for the management interface of each vShield agent you install
- A single static IP address for the vShield Manager management interface
- Enable cookies on your Web browser to access the vShield Manager user interface

vShield Zones Components

The following components comprise the vShield Zones solution:

- vShield Manager: The vShield Zones management center that manages all of the distributed vShield agents. Provides for monitoring, configuration, and software updating of your vShield agents.
- vShield agent : The active security component of vShield Zones that inspects traffic flow and provides firewall protection. You install a vShield agent on each ESX host you want to protect. A vShield agent installs within the traffic path to monitor all traffic into and out of an ESX host, as well as between virtual machines on the host.

Evaluating ESX Network Configuration Before Installing vShield Zones

Prior to installing vShield Zones in your vCenter Server environment, consider the network configuration of your ESX hosts. At a minimum, each host has at least one associated physical NIC and one vSwitch, which hosts the VMKernel, service console, and virtual machines. In more robust environments, an ESX host might have multiple dedicated physical NICs and multiple vSwitches to separate the VMKernel and service console from the virtual machines.

The vShield Zones appliances install as virtual machines on an ESX host. However, installation of a vShield agent requires some planning. You can install a vShield agent on any vSwitch with a dedicated NIC. vShield agent installation moves virtual machines from their original vSwitch to a cloned vSwitch. The vShield agent then installs between the original vSwitch and the cloned vSwitch to capture all traffic to and from the virtual machines. The original vSwitch keeps the NIC, while the new vSwitch does not associate with a NIC. Thus, if you have an ESX host with multiple vSwitches hosting a variety of virtual machines, you need one vShield agent per vSwitch. Any virtual machines connected to a vSwitch where a vShield agent is not installed is not protected by vShield Zones.

The installation of multiple vShield agents is simplified by installing the vShield agent OVF and then deploying the original vShield agent virtual machine as a template. This template is referenced by the vShield Manager, allowing you to install multiple vShield agents into your vCenter Server environment from the vShield Manager user interface. For more information on the vShield agent installation process, see "vShield Agent Automated Installation At-a-Glance" on page 14.

NOTE The vShield Zones system was built to protect virtual machines, and not the VMKernel or service console.

Installing vShield Zones

vShield Zones installation is a multi-step process. Perform the following tasks in sequence to complete vShield Zones installation successfully.

Obtain vShield Zones Virtual Appliances

vShield Zones virtual appliances are packaged using the Open Virtualization Format (OVF). This packaging simplifies the installation by allowing you to use the vSphere Client to import the virtual appliance into the datastore and virtual machine inventory.

Contact your VMware account team to obtain a vShield Zones software package, which consists of one vShield Manager and one vShield agent. One vShield agent virtual appliance can be used for multiple vShield agent installations.

Once you have obtained the package, download it to a PC where the vSphere Client is installed.

Install the vShield Manager as a Virtual Machine Using the vSphere Client

vShield Manager virtual machine installation requires creating a port group for the vShield Manager.

To add the vShield Manager to your vCenter Server inventory as a virtual machine

1. Log in to the vSphere Client.
2. Select an ESX host from the inventory panel.
3. Go to **File > Deploy OVF Template**.

   The Deploy OVF Template wizard opens.
4. Click **Deploy from file** and click **Browse** to locate the folder on your PC containing the vShield Manager OVF file.
5. Complete the wizard.

   The vShield Manager is installed into your inventory.
6. Create a port group named **`vsmgmt`** for the vShield Manager on the ESX host where the vShield Manager installed.

   Each installed vShield agent recognizes this port group name, which prevents the vShield agent from moving the vShield Manager virtual machine during vShield agent installation.
7. Edit the settings of the vShield Manager virtual machine to connect at power on and set the network label to the vsmgmt port group.

   a. Right-click the vShield Manager virtual machine and click **Edit Settings**.

      The vShield Manager - Virtual Machine Properties dialog box opens.

   b. Under the **Hardware** tab, click **Network Adapter 1**.

   c. Select **Connect at power on** under Device Status.

   d. In the **Network label** drop-down list and select **vsmgmt**.

   e. Click **OK** to close the window.
8. Power on the vShield Manager virtual machine.
9. Click the **Console** tab from the right-hand pane to open the vShield Manager CLI.

   The booting process might take a couple of minutes.
10. After the `manager login` prompt appears, log in to the CLI by using the username **`admin`** and the password **`default`**.
11. Run the `setup` command to launch the CLI setup wizard.

    The CLI setup wizard guides you through IP address assignment for the vShield Manager's management interface and identification of the default network gateway. The IP address of the management interface must be reachable by all installed vShield agents, as well as by a Web browser for system management.

```
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.
```

You do not need to log out at this time. vShield Manager installation is complete.

12 Ping the default gateway to verify network connectivity.

```
manager> ping 10.115.219.253
```

13 From your PC, ping the vShield Manager IP address to validate that the IP address is reachable.

14 Install VMware Tools on the vShield Manager virtual machine.

Install the vShield Agent and Convert it into a Template

Install the vShield agent as a virtual machine and convert it into a template. After the vShield agent virtual machine is converted to template format, the template can be referenced by the vShield Manager for vShield agent installation on multiple ESX instances.

To add the vShield agent to vCenter Server and convert it to a template

1 Log in to the vSphere Client.

2 Select an ESX host from the inventory panel.

3 Go to **File > Deploy OVF Template**.

The Deploy OVF Template wizard opens.

4 Click **Deploy from file** and click **Browse** to locate the folder on your client machine containing the vShield agent OVF file.

5 Complete the wizard.

The vShield agent is installed into your inventory.

CAUTION Do not power on or edit the vShield agent virtual machine at this time. Powering on or editing the virtual machine at this point can cause network issues, such as an endless loop.

6 After the wizard completes installation, convert the vShield agent into a virtual machine template.

The template enables automated installation of multiple vShield agents from the vShield Manager user interface.

Log In to the vShield Manager User Interface to Configure the System

After the vShield Manager virtual appliance has been installed and the vShield agent has been converted to a template, log in to the vShield Manager user interface and configure the vShield Manager to authenticate with the vCenter Server. This authentication allows the vShield Manager to display your vCenter Server inventory, install vShield agents, and configure the firewall to protect your resources.

To log in to the vShield Manager user interface

1 Open a Web browser window and type the IP address assigned to the vShield Manager.

You must prepend the IP address with **`https`**.

2 Accept the security certificate.

The vShield Manager login screen appears.

3 Log in to the vShield Manager user interface by using the username **`admin`** and the password **`default`**.

The vShield Manager user interface opens to the **Configuration > vCenter** tab content in the right-side frame. Upon initial login, no information is displayed in the vShield Manager as you have not yet synchronized communication with the vCenter Server.

4 Complete the **vCenter** tab form as follows:

Field	Action
IP address/Name	Type the IP address of your vCenter Server.
User Name	Type your vSphere Client user name.
Password	Type the password associated with your vSphere Client user name.

5 Click **Commit**.

The vShield Manager connects to the vCenter Server, logs in, and accesses the VMware Virtual Infrastructure SDK. The inventory tree on the left side of the vShield Manager screen should match your vSphere Client Hosts & Clusters inventory tree view.

NOTE The vShield Manager does not appear in the vShield Zones inventory panel. The **Settings & Reports** object represents the vShield Manager in the inventory panel.

Add a vShield Agent

You can add vShield agents to the vCenter Server and vShield Zones inventories by creating clones from the vShield agent template.

You should install one vShield agent per vSwitch with an attached NIC. Any virtual machines connected to a vSwitch where a vShield agent is not installed are not protected by vShield Zones.

NOTE To install a vShield agent on a vNetwork Distributed Switch (vNDS), refer to the *vShield Zones Administration Guide*.

To add a vShield agent

1 Log in to the vShield Manager.

2 From the inventory tree, click the ESX host that you want to protect.

3 Click the **Install vShield** tab that appears above the right frame.

4 Click **Configure install parameters**.

5 Complete the form as follows:

Field	Action
Select from available vShields	Leave this field blank. Use this field only when you are adding a vShield agent without an established template.
Select template to clone	Click this drop-down menu and select the vShield agent template.
Select a datastore to place clone	Click this drop-down menu and select the datastore on which to store the vShield agent clone.
Enter a name for the clone	Type a unique name for the vShield agent clone. This name appears in your vSphere Client and vShield Manager inventories.
Specify IP Address of vShield VM	Type the IP address to be assigned to the vShield agent's management port.
Specify IP Mask for vShield	Type the IP subnet mask associated with the assigned IP address.
Specify IP Address of Default Gateway for vShield	Type the IP address of the default network gateway
Specify Secure Key for vShield (leave blank for default)	(Optional) Type a key to be used between the vShield agent and the vShield Manager for secure communication. By default, this entry in this field is masked. This default seed is used for encrypted communication between the vShield agent and the vShield Manager. Keys are not shared across the network.
Select a vSwitch to shield	Click this drop-down menu and select the vSwitch to protect. The vSwitches eligible for protection are highlighted in green in the accompanying table.

6 Click **Continue**.

The installation summary screen appears. This screen displays before and after example illustrations of installing a vShield agent on the ESX.

NOTE The example illustrations are static and do not directly reflect your virtual network. The numbered installation script on the right-hand side of the screen details the actual installation steps.

---

7 Click **Install**.

You can follow the vShield agent installation steps from the Recent Tasks status pane located at the bottom of the vSphere Client window. For more details on the installation process, see "vShield Agent Automated Installation At-a-Glance" on page 14.

vShield agent installation is complete.

8 After installation has completed, open your vSphere Client.

9 Locate the vShield agent in your inventory.

Note that it is powered on.

10 Install VMware Tools on the vShield Manager virtual machine.

Enable Continuous Discovery to Identify Your Guest Virtual Machine Traffic

After your vShield Manager and vShield agent are installed, and your vShield agent communicates with your vShield Manager, you must enable the continuous discovery operation for the vShield agent to protect your virtual machines.

To enable continuous discovery of virtual machine traffic

1 Log in to the vShield Manager.

2 Click the vShield agent from the inventory tree.

3 Click the **VM Discovery** tab.

4 Click the **Automated** subhead.

5 In the **Scheduled Discovery Status** drop-down menu, select **Continuous**.

Do not complete any other fields in the form.

6 Click **OK**.

The discovery operation begins. Discovery runs continuously, identifying traffic flows by application and protocol specifications.

7 Go to **VM Discovery** > **Results** to view the discovery output.

Discovered traffic is separated by virtual machine IP address. Each discovered virtual machine is saved under the **VM Inventory** tab, which is available at the datacenter and cluster container levels, as well as at the virtual machine level within the vShield Manager.

Additional vCenter Configuration for vShield Agents

If you have enabled the VMware HA or VMware DRS features, you must disable movement of vShield agent virtual machines. This must be performed after installation of each vShield agent virtual machine.

You can migrate the vShield Manager virtual appliance by using VMotion without consequence.

To disable VMware HA or VMware DRS from moving the vShield agent virtual machines

1 Log in to the vSphere Client.

2 Right-click the cluster containing your vShield agent virtual machines and click **Edit Properties**.

The Admin Settings dialog box opens.

3 Under VMware HA, click **Virtual Machine Options**.

Locate the vShield agents in the list.

4 For each vShield agent virtual machine, select the following values:

- **VM Restart Priority**: **Disabled**
- **Host Isolation Response**: **Leave VM powered on**

5 If you have enabled DRS, click **Virtual Machine Options** under VMware DRS.

Locate the vShield agents in the list.

6 For each vShield agent virtual machine, select **Disabled** for **Automation Level**.

7 Click **OK** after all vShield agent virtual machines have been configured.

In default operation, a vShield agent raises an error during attempted virtual machine migration by the operator or VMotion. The error states that the server is connected to a virtual intranet. This virtual intranet is the vSwitch that a virtual machine connects to on the protected side of the vShield agent. This vSwitch does not home a physical NIC. The vShield agent bridges traffic to the unprotected side of the network that is connected to a physical NIC.

To enable VMotion to disable the virtual intranet check

1 Locate the `vpxd.cfg` file on the machine running vCenter Server. By default, this file is installed at `C:\Documents and Settings\All Users\Application Data\VMware\VMware vCenter Server`.

2 Edit the `vpxd.cfg` file in a text editor.

Add the following lines as a sub-level to the `config` section, and at the same level as the `vpxd` section.

```
<migrate>
    <test>
        <CompatibleNetworks>
            <VMOnVirtualIntranet>false</VMOnVirtualIntranet>
        </CompatibleNetworks>
    </test>
</migrate>
```

3 Save the `vpxd.cfg` file.

4 Restart the VMware vCenter Server service. You can access the service menu by going to **Control Panel > Administrative Tools > Services**.

To further configure vShield Zones, refer to the *vShield Zones Administration Guide*.

Powering off vShield Zones Virtual Machines

You can power off vShield Zones virtual machines at any time. When you power off a vShield Zones virtual machine, the last saved configuration is used when the virtual machine is powered on.

To power off vShield Zones virtual machines

1 In the vSphere Client, select the vShield Zones virtual machines from the inventory panel.

2 Click the **Console** tab to open the vShield Zones CLI.

3 Log in to the CLI.

4 After logging in, type `enable` to enter Privileged mode.

5 Type `shutdown`.

6 After CLI shutdown is completed, right-click the virtual machine from the inventory panel and select **Power > Power Off**.

vShield Agent Automated Installation At-a-Glance

When installed from a referenced template, the vShield agent installation process performs the following steps:

1 Creates a clone of the vSwitch host.

This vSwitch clone does not include a NIC. The name of the vSwitch clone includes the name of the vSwitch host with _VS appended: vSwitch1_VS.

2 Creates a protected zone port group, VSprot_*vShieldagent-name*, and attaches this port group to the vSwitch host.

3 Creates a management port group, VSmgmt_*vShieldagent-name*, on the vSwitch host for the vShield agent's management interface.

4 Creates an unprotected zone port group, VSunprot_*vShieldagent-name*, and attaches this port group to the vSwitch clone.

IMPORTANT Do not add virtual machines to the protected or unprotected port groups. These port groups are configured with promiscuous mode turned on, which allows the vShield agent to see all passing traffic.

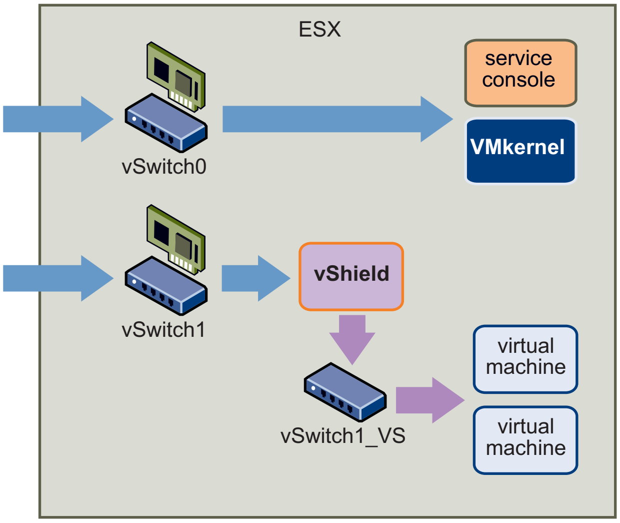
5 Connects and powers on the vShield agent.

6 Attaches the virtual interfaces on the vShield agent to the protected and unprotected port groups.

7 Moves the virtual machines from the vSwitch host to the vSwitch clone.

If the vShield Manager virtual machine resides on the same vSwitch, it is not moved. During vShield Manager installation, you created a port group called **`vsmgmt`** in which to place the vShield Manager. vShield agent installation recognizes this port group name and ignores any virtual machines in this port group.

Figure 1. Installation of a vShield agent on a vSwitch



Understanding the Port Groups Created from vShield Agent Installation

vShield agent installation requires the creation of two port groups. These port groups delineate zones of trust: unprotected and protected. The unprotected zone monitors incoming traffic, while the protected zone monitors outgoing traffic. Each port group homes a vShield agent interface: U0 for the unprotected zone and P0 for the protected zone. Connecting these interfaces to the created port groups enables the vShield agent to monitor all incoming and outgoing traffic.

The unprotected and protected port groups are configured with promiscuous mode enabled. In promiscuous mode, a guest adapter can listen to all passing packets. In non-promiscuous mode, a guest adapter listens to traffic only on its own MAC address. By default, guest adapters are set to non-promiscuous mode. For protection purposes, the vShield agent must be able to see all passing traffic. Do not add any other virtual machines to these port groups.