vShield Installation and Upgrade Guide

vShield Manager 5.5
vShield Edge 5.5
vShield Endpoint 5.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001281-00

vmware®

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

This manual, the *vShield Installation and Upgrade Guide*, describes how to install and configure the VMware® vShield™ system by using the vShield Manager user interface, the vSphere Client plug-in, and command line interface (CLI). The information includes step-by-step configuration instructions, and suggested best practices.

Intended Audience

This manual is intended for anyone who wants to install or use vShield in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware Infrastructure 5.x, including VMware ESX, vCenter Server, and the vSphere Client.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Document Feedback

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

Technical Support and Education Resources

The following technical support resources are 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.html.

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.

Introduction to vShield 1

This chapter introduces the VMware® vShield™ components you install.

This chapter includes the following topics:

vShield Components at a Glance

VMware vShield is a suite of security virtual appliances built for VMware vCenter Server integration. vShield is a critical security component for protecting virtualized datacenters from attacks and misuse, and helping you achieve your compliance-mandated goals.

vShield includes virtual appliances and services essential for protecting virtual machines. vShield can be configured through a web-based user interface, a vSphere Client plug-in, a command line interface (CLI), and REST API.

vCenter Server includes vShield Manager. The following vShield packages each require a license:

- vShield App
- vShield App with Data Security
- vShield Edge
- vShield Endpoint

One vShield Manager manages a single vCenter Server environment and multiple vShield App, vShield Edge, vShield Endpoint, and vShield Data Security instances.

vShield Manager

The vShield Manager is the centralized network management component of vShield, and is installed as a virtual appliance on any ESX™ host in your vCenter Server environment. A vShield Manager can run on a different ESX host from your vShield agents.

Using the vShield Manager user interface or vSphere Client plug-in, administrators install, configure, and maintain vShield components. The vShield Manager user interface leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel, and includes the Hosts & Clusters and Networks views.

vShield App

vShield App is a hypervisor-based firewall that protects applications in the virtual datacenter from network based attacks. Organizations gain visibility and control over network communications between virtual machines. You can create access control policies based on logical constructs such as VMware vCenter™ containers and vShield security groups—not just physical constructs such as IP addresses. In addition, flexible IP addressing offers the ability to use the same IP address in multiple tenant zones to simplify provisioning.

You should install vShield App on each ESX host within a cluster so that VMware vMotion operations work and virtual machines remain protected as they migrate between ESX hosts. By default, a vShield App virtual appliance cannot be moved by using vMotion.

The Flow Monitoring feature displays network activity between virtual machines at the application protocol level. You can use this information to audit network traffic, define and refine firewall policies, and identify threats to your network.

vShield Edge

vShield Edge provides network edge security and gateway services to isolate a virtualized network, or virtual machines in a port group, vDS port group, or Cisco Nexus 1000V port group. You install a vShield Edge at a datacenter level and can add up to ten internal or uplink interfaces. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

Standard vShield Edge Services (Including Cloud Director)

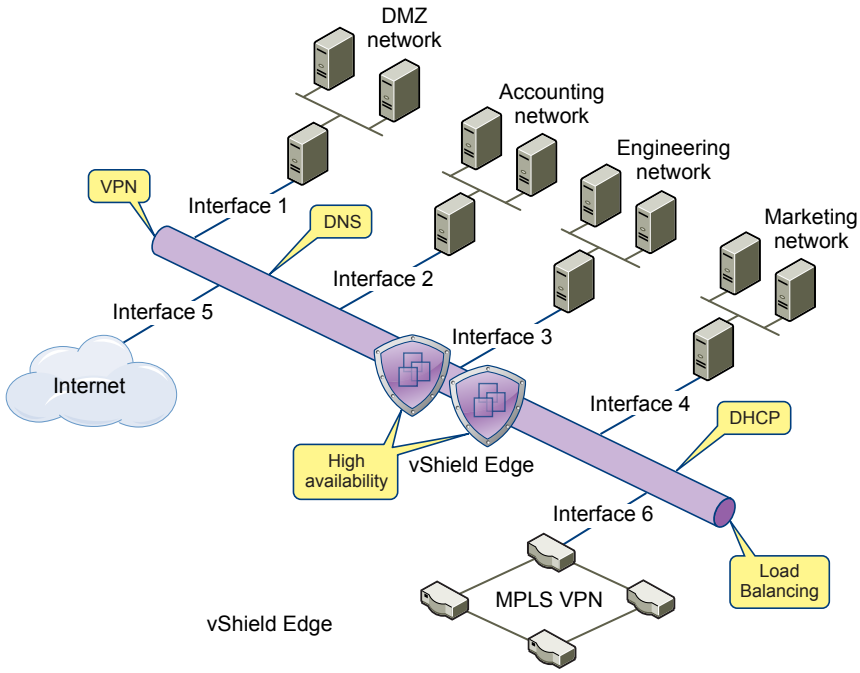
Firewall	Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for all protocols.
Network Address Translation	Separate controls for Source and Destination IP addresses, as well as port translation.
Dynamic Host Configuration Protocol (DHCP)	Configuration of IP pools, gateways, DNS servers, and search domains.

Advanced vShield Edge Services

Site-to-Site Virtual Private Network (VPN)	Uses standardized IPsec protocol settings to interoperate with all major VPN vendors.
SSL VPN-Plus	SSL VPN-Plus enables remote users to connect securely to private networks behind a vShield Edge gateway.
Load Balancing	Simple and dynamically configurable virtual IP addresses and server groups.
High Availability	High availability ensures an active vShield Edge on the network in case the primary vShield Edge virtual machine is unavailable.

vShield Edge supports syslog export for all services to remote servers.

Figure 1-1. Multi-Interface Edge

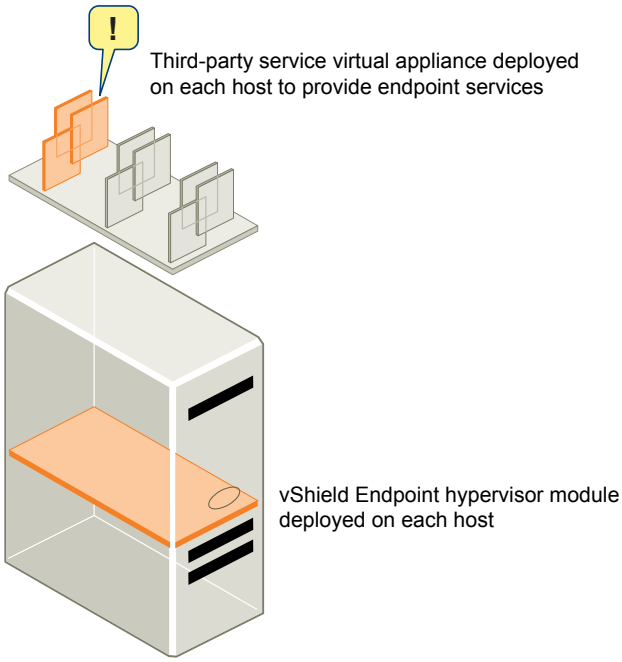


vShield Endpoint

vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. Since the secure virtual appliance (unlike a guest virtual machine) doesn't go offline, it can continuously update antivirus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

vShield Endpoint installs as a hypervisor module and security virtual appliance from a third-party antivirus vendor (VMware partners) on an ESX host. The hypervisor scans guest virtual machines from the outside, removing the need for agents in every virtual machine. This makes vShield Endpoint efficient in avoiding resource bottlenecks while optimizing memory use.

Figure 1-2. vShield Endpoint Installed on an ESX Host



vShield Data Security

vShield Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by vShield Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

Deployment Scenarios

Using vShield, you can build secure zones for a variety of virtual machine deployments. You can isolate virtual machines based on specific applications, network segmentation, or custom compliance factors. Once you determine your zoning policies, you can deploy vShield to enforce access rules to each of these zones.

Protecting the DMZ

The DMZ is a mixed trust zone. Clients enter from the Internet for Web and email services, while services within the DMZ might require access to services inside the internal network.

You can place DMZ virtual machines in a port group and secure that port group with a vShield Edge. vShield Edge provides access services such as firewall, NAT, and VPN, as well as load balancing to secure DMZ services.

A common example of a DMZ service requiring an internal service is Microsoft Exchange. Microsoft Outlook Web Access (OWA) commonly resides in the DMZ cluster, while the Microsoft Exchange back end is in the internal cluster. On the internal cluster, you can create firewall rules to allow only Exchanged-related requests from the DMZ, identifying specific source-to-destination parameters. From the DMZ cluster, you can create rules to allow outside access to the DMZ only to specific destinations using HTTP, FTP, or SMTP.

Isolating and Protecting Internal Networks

You can use a vShield Edge to isolate an internal network from the external network. A vShield Edge provides perimeter firewall protection and edge services to secure virtual machines in a port group, enabling communication to the external network through DHCP, NAT, and VPN.

Within the secured port group, you can install a vShield App instance on each ESX host that the vDS spans to secure communication between virtual machines in the internal network.

If you utilize VLAN tags to segment traffic, you can use App Firewall to create smarter access policies. Using App Firewall instead of a physical firewall allows you to collapse or mix trust zones in shared ESX clusters. By doing so, you gain optimal utilization and consolidation from features such as DRS and HA, instead of having separate, fragmented clusters. Management of the overall ESX deployment as a single pool is less complex than having separately managed pools.

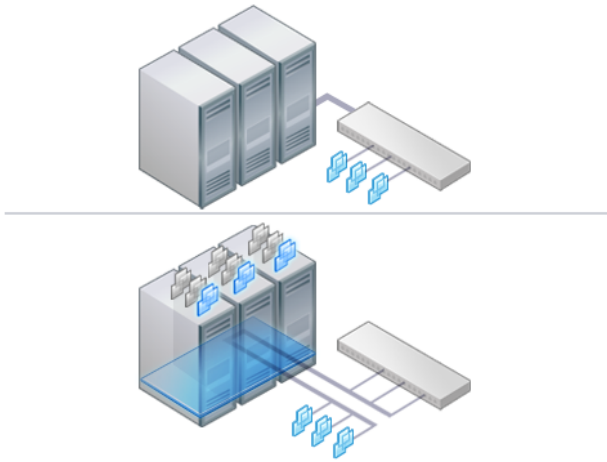
For example, you use VLANs to segment virtual machine zones based on logical, organizational, or network boundaries. Leveraging the Virtual Infrastructure SDK, the vShield Manager inventory panel displays a view of your VLAN networks under the Networks view. You can build access rules for each VLAN network to isolate virtual machines and drop untagged traffic to these machines.

Protecting Virtual Machines in a Cluster

You can use vShield App to protect virtual machines in a cluster.

In Figure 1-3, vShield App instances are installed on each ESX host in a cluster. Virtual machines are protected when moved via vMotion or DRS between ESX hosts in the cluster. Each vApp shares and maintains state of all transmissions.

Figure 1-3. vShield App Instances Installed on Each ESX Host in a Cluster



Common Deployments of vShield Edge

You can use a vShield Edge to isolate a stub network, using NAT to allow traffic in and out of the network. If you deploy internal stub networks, you can use vShield Edge to secure communication between networks by using LAN-to-LAN encryption via VPN tunnels.

vShield Edge can be deployed as a self-service application within VMware Cloud Director.

Common Deployments of vShield App

You can use vShield App to create security zones within a vDC. You can impose firewall policies on vCenter containers or Security Groups, which are custom containers you can create by using the vShield Manager user interface. Container-based policies enable you to create mixed trust zones clusters without requiring an external physical firewall.

In a deployment that does not use vDCs, use a vShield App with the Security Groups feature to create trust zones and enforce access policies.

Service Provider Admins can use vShield App to impose broad firewall policies across all guest virtual machines in an internal network. For example, you can impose a firewall policy on the second vNIC of all guest virtual machines that allows the virtual machines to connect to a storage server, but blocks the virtual machines from addressing any other virtual machines.

Preparing for Installation 2

This chapter provides an overview of the prerequisites for successful vShield installation.

This chapter includes the following topics:

System Requirements

Before you install vShield in your vCenter Server environment, consider your network configuration and resources. You can install one vShield Manager per vCenter Server, one vShield App or one vShield Endpoint per ESX™ host, and multiple vShield Edge instances per datacenter.

Hardware

Table 2-1. Hardware Requirements

Component	Minimum
Memory	■ vShield Manager: 8GB allocated, 3GB reserved ■ vShield App: 1GB allocated, 1 GB reserved ■ vShield Edge compact: 256 MB, large: 1 GB, x-large: 8 GB ■ vShield Data Security: 512 MB
Disk Space	■ vShield Manager: 60 GB ■ vShield App: 5 GB per vShield App per ESX host ■ vShield Edge compact and large: 320 MB, lx-Large: 4.4 GB (with 4 GB swap file) ■ vShield Data Security: 6GB per ESX host
vCPU	■ vShield Manager: 2 ■ vShield App: 2 ■ vShield Edge compact: 1, large and x-Large: 2 ■ vShield Data Security: 1

Software

For the latest interoperability information, see the Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

These are the minimum required versions of VMware products.

- VMware vCenter Server 5.0 or later

  For VXLAN virtual wires, you need vCenter Server 5.1 or later.

- VMware ESX 4.1 or later for each server

  For vShield Endpoint, you need VMware ESX 4.1 Patch 3 or later.

  For VXLAN virtual wires, you need VMware ESX 5.1 or later.

- VMware Tools

  For vShield Endpoint and vShield Data Security, you must upgrade your virtual machines to hardware version 7 or 8 and install VMware Tools 8.6.0 released with ESXi 5.0 Patch 3. For more information, see "Install VMware Tools on the Guest Virtual Machines," on page 34.

  You must install VMware Tools on virtual machines that are to be protected by vShield App.

- VMware vCloud Director 1.5 or later
- VMware View 4.5 or later

Client and User Access

- PC with the VMware vSphere Client
- If you added ESX hosts by name to the vSphere inventory, ensure that DNS servers have been configured on the vShield Manager and name resolution is working. Otherwise, vShield Manager cannot resolve the IP addresses.
- 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
- Enable cookies on your Web browser to access the vShield Manager user interface
- From vShield Manager, port 443 accessible from the ESX host, the vCenter Server, and the vShield appliances to be deployed. This port is required to download the OVF file on the ESX host for deployment.
- Connect to the vShield Manager using one of the following supported Web browsers:
  - Internet Explorer 6.x and later
  - Mozilla Firefox 1.x and later
  - Safari 1.x or 2.x

Deployment Considerations

Consider the following recommendations and restrictions before you deploy vShield components.

Deployment Considerations for vShield

This topic describes deployment considerations for vShield components.

Preparing Virtual Machines for vShield Protection

You must determine how to protect your virtual machines with vShield. As a best practice, you should prepare all ESX hosts within a DRS cluster for vShield App, vShield Endpoint, and vShield Data Security depending on the vShield components you are using. You must also upgrade your virtual machines to hardware version 7 or 8.

Consider the following questions:

How Are My Virtual Machines Grouped?

You might consider moving virtual machines to port groups on a vDS or a different ESX host to group virtual machines by function, department, or other organizational need to improve security and ease configuration of access rules. You can install vShield Edge at the perimeter of any port group to isolate virtual machines from the external network. You can install a vShield App on an ESX host and configure firewall policies per container resource to enforce rules based on the hierarchy of resources.

Are My Virtual Machines Still Protected if I vMotion Them to Another ESX Host?

Yes, if the hosts in a DRS cluster are prepared, you can migrate machines between hosts without weakening the security posture. For information on preparing your ESX hosts, see "Install vShield App," on page 26.

vShield Manager Uptime

The vShield Manager should be run on an ESX host that is not affected by downtime, such as frequent reboots or maintenance mode operations. You can use HA or DRS to increase the resilience of the vShield Manager. If the ESX host on which the vShield Manager resides is expected to require downtime, vMotion the vShield Manager virtual appliance to another ESX host. Thus, more than one ESX host is recommended.

Communication Between vShield Components

The management interfaces of vShield components should be placed in a common network, such as the vSphere management network. The vShield Manager requires connectivity to the vCenter Server, ESXi host, vShield App and vShield Edge instances, vShield Endpoint module, and vShield Data Security virtual machine. vShield components can communicate over routed connections as well as different LANs.

VMware recommends that you install vShield Manager on a dedicated management cluster separate from the cluster(s) that vShield Manager manages. Each vShield Manager manages a single vCenter Server environment.

If the vCenter Server or vCenter Server database virtual machines are on the ESX host on which you are installing vShield App, migrate them to another host before installing vShield App.

Ensure that the following ports are open:

- Port 443/TCP from, to, and among the ESX host, the vCenter Server, and vShield Data Security
- UDP123 between vShield Manager and vShield App for time synchronization
- 443/TCP from the REST client to vShield Manager for using REST API calls
- 80/TCP and 443/TCP for using the vShield Manager user interface and initiating connection to the vSphere SDK
- 22/TCP for communication between vShield Manager and vShield App and troubleshooting the CLI

Hardening Your vShield Virtual Machines

You can access the vShield Manager and other vShield components by using a web-based user interface, command line interface, and REST API. vShield includes default login credentials for each of these access options. After installation of each vShield virtual machine, you should harden access by changing the default login credentials. Note that vShield Data Security does not include default login credentials.

vShield Manager User Interface

You access the vShield Manager user interface by opening a web browser window and navigating to the IP address of the vShield Manager's management port.

The default user account, admin, has global access to the vShield Manager. After initial login, you should change the default password of the admin user account. See "Change the Password of the vShield Manager User Interface Default Account," on page 22.

Command Line Interface

You can access the vShield Manager, vShield App, and vShield Edge virtual appliances by using a command line interface via vSphere Client console session. To access the vShield Endpoint virtual appliance, refer to the instructions from the anti-virus solution provider. You cannot access the vShield Data Security virtual machine by using the command line interface.

Each virtual appliance uses the same default username (**`admin`**) and password (**`default`**) combination as the vShield Manager user interface. Entering Enabled mode also uses the password **`default`**.

For more on hardening the CLI, see the *vShield Command Line Interface Reference* .

REST Requests

All REST API requests require authentication with the vShield Manager.

Using Base 64 encoding, you identify a username-password combination in the following format: username:password. You must use a vShield Manager user interface account (username and password) with privileged access to perform requests. For more on authenticating REST API requests, see the *vShield API Programming Guide*.

Deployment Considerations for vShield App

VMware recommends that you analyze your vCenter Server environment and determine whether your want to protect the entire environment or certain clusters only.

If you decide to protect specific clusters, you must prepare the entire cluster and install vShield App on all ESX hosts in those clusters. If you install vShield App only on some hosts in a cluster, there is a chance that vMotion can move virtual machines from a protected to an unprotected host thus compromising the security of your network.

Ensure that you install vShield App in your environment during a maintenance window. The total install time may vary depending on your environment and the number of hosts in each cluster, but you must complete installing vShield App on all desired clusters before resuming normal operations.

After installation, VMware recommends that you enable vSphere HA and set the cluster feature to **VM and Application Monitoring** on the clusters where you installed vShield App. This feature monitors the vShield App and triggers a restart if it fails, which minimizes the vShield App outage. For more information on this feature, see *vSphere Availability*.

VMware recommends that you let vShield App run during normal operations and use the vShield App Flow Monitoring tool for baseline knowledge of the traffic flowing in and out of your virtual network. You can then add rules according to the needs of your network.

Enabling the SpoofGuard feature of vShield App allows you to authorize the IP addresses reported by VMware Tools, and alter them if necessary to prevent spoofing. Depending on the SpoofGuard mode you choose, vShield App either automatically trusts IP assignments on their first use or requires you to manually approve IP assignments before use. However, be aware that the IP address of a virtual machine may change when the DHCP server renews a lease or is rebooted. This means that you must approve the new or renewed IP address if the SpoofGuard feature is enabled.

Becoming familiar with the flow monitoring and SpoofGuard features before installing vShield App will enable you to configure vShield App in the most secure way possible. For more information on these features, see the *vShield Administration Guide*.

Deployment Considerations for vShield Edge

Before installing vShield Edge, you must become familiar with your network topology. vShield Edge can have multiple interfaces, but you must connect at least one internal interface to a portgroup or VXLAN virtual wire before you can deploy the vShield Edge.

The uplink interface provides connectivity to the outside world. You must have created and configured a port group or VXLAN virtual wire that has external connectivity. You must also have a port group with virtual machines to which you can connect the internal interface. Determine the IP addresses and subnets to be provided for these interfaces. Also think about the services that you should enable and configure after installing vShield Edge. For more information on vShield Edge services, see the *vShield Administration Guide*.

After you install vShield Edge and before you configure vShield Edge services, virtual machines in that port groups(s) may lose network connectivity. To avoid this issue, you may create a new port group, install and configure vShield Edge on it, and then move virtual machines to the port group.

Be aware that the default vShield Edge firewall policy blocks all incoming traffic, so you must add allow rules as required.

Installing the vShield Manager 3

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

The vShield Manager is the centralized management component of vShield. You use the vShield Manager to monitor and push configurations to vShield App, vShield Endpoint, and vShield Edge instances. The vShield Manager runs as a virtual appliance on an ESX host.

Installing the vShield Manager is a multistep process. You must perform all of the tasks that follow in sequence to complete vShield Manager installation successfully.

To enhance your network security posture, you can obtain licenses for vShield App, vShield Endpoint, and vShield Edge.

This chapter includes the following topics:

Obtain the vShield Manager OVA File

The vShield Manager virtual machine is packaged as an Open Virtualization Appliance (OVA) file, which allows you to use the vSphere Client to import the vShield Manager into the datastore and virtual machine inventory.

Install the vShield Manager Virtual Appliance

You can install the vShield Manager virtual machine on an ESX host in a cluster configured with DRS.

With vShield 5.0 and later, you can install the vShield Manager in a different vCenter than the one that the vShield Manager will be interoperating with. A single vShield Manager serves a single vCenter Server environment.

The vShield Manager virtual machine installation includes VMware Tools. Do not attempt to upgrade or install VMware Tools on the vShield Manager.

Prerequisites

You must have been assigned the Enterprise Administrator or vShield Administrator role .

Procedure

1 Log in to the vSphere Client.

2 Create a port group to home the management interface of the vShield Manager.

The vShield Manager management interface, vCenter Server, and ESXi hosts must be reachable by all future vShield Edge, vShield App, and vShield Endpoint instances.

3 Select **File > Deploy OVF Template**.

4 Click **Browse** to locate the folder on your PC that contains the vShield Manager OVA file.

5 Complete the installation.

The vShield Manager is installed as a virtual machine in your inventory.

6 Power on the vShield Manager virtual machine.

What to do next

The default CPU for vShield Manager 5.1 is 2 vCPU. For vShield Manager to work with vSphere Fault Tolerance, you must set the CPU to 1 vCPU.

Log In to the vShield Manager User Interface

After you have installed and configured the vShield Manager virtual machine, log in to the vShield Manager user interface.

Procedure

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

The vShield Manager user interface opens in a web browser window using SSL.

2 Accept the security certificate.

NOTE You can use an SSL certificate for authentication. Refer to the *vShield Administration Guide*.

The vShield Manager login screen appears.

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

You should change the default password as one of your first tasks to prevent unauthorized use. See "Change the Password of the vShield Manager User Interface Default Account," on page 22.

4 Click **Log In**.

Set up vShield Manager

Specify vCenter Server, DNS and NTP server, and Lookup server details.

NOTE The vShield Manager virtual machine does not appear as a resource in the inventory panel of the vShield Manager user interface. The **Settings & Reports** object represents the vShield Manager virtual machine in the inventory panel.

Prerequisites

- You must have a vCenter Server user account with administrative access to synchronize vShield Manager with the vCenter Server . If your vCenter password has non-Ascii characters, you must change it before synchronizing the vShield Manager with the vCenter Server.
- To use SSO on vShield Manager, you must have vCenter Server 5.1 or above and single sign on service must be installed on the vCenter Server.

Procedure

1 Log in to the vShield Manager.

2 Click **Settings & Reports** from the vShield Manager inventory panel.

3 Click the **Configuration** tab.

4 The **DNS Servers** area displays the IP addresses of the DNS servers you specified when you configured the network settings of the vShield Manager.

You can edit the servers if required.

5 In **NTP Server**, click **Edit** and type the IP address of your NTP server.

The NTP server establishes a common network time. It is recommended that you use the NTP server used by the SSO server so that the time on the vShield Manager server is in synch with the NTP server.

IMPORTANT You must reboot the vShield Manager after editing the NTP server details.

---

6 In **Lookup Service**, click **Edit** and type the host name or IP address of the host that has the lookup service.

7 Change the port number if required.

The Lookup Service URL is displayed based on the specified host and port.

8 Type the SSO user name and password.

This enables vShield Manager to register itself on the Security Token Service server.

9 In **vCenter Server**, type the IP address or hostname of your vCenter Server.

10 Type your vSphere Client login user name.

11 Type the password associated with the user name.

12 To assign the Enterprise Administrator role to the user you have logged in as, select **Assign vShield Enterprise Administrator role to this user**.

This role gives vShield operations and security permissions to the user.

13 To modify the plug-in script download location, select **Modify plug-in script download location** and type the vShield Manager IP address and port number.

This may be required for NAT environments. By default, the vShield Manager address used is `vShield_Manager_IP:443`.

14 Click **Save**.

15 (Optional) On a Windows server computer, perform the following steps to load the vShield Manager inventory panel:

a Open Internet Explorer.

b Select **Tools > Internet Options**.

c In the Internet Option window, select the **Security** tab.

d Click **Trusted sites**.

e Click the **Sites** button.

f Type the IP address of the vShield Manager and click **Add**.

g Click **Close**.

h Click **OK**.

i Close Internet Explorer.

The vShield Manager connects to the vCenter Server, logs on, and utilizes the VMware Infrastructure SDK to populate the vShield Manager inventory panel. The inventory panel is presented on the left side of the screen. This resource tree should match your VMware Infrastructure inventory panel. The vShield Manager does not appear in the vShield Manager inventory panel.

What to do next

Login to the vSphere Client, select an ESX host, and verify that vShield appears as a tab. You can then install and configure vShield components from the vSphere Client.

Change the Password of the vShield Manager User Interface Default Account

You can change the password of the admin account to harden access to your vShield Manager.

Procedure

1 Log in to the vShield Manager user interface.

2 Click **Change Password** on the top right corner of the window.

3 In **Old password**, type `default` (the current password).

4 Type a new password.

5 Confirm the password by typing it a second time in the **Retype Password** field.

6 Click **OK** to save your changes.

Schedule a Backup of vShield Manager Data

You can only schedule the parameters for one type of backup at any given time. You cannot schedule a configuration-only backup and a complete data backup to run simultaneously.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **Backups**.

4 From the **Scheduled Backups** drop-down menu, select **On**.

5 From the **Backup Frequency** drop-down menu, select **Hourly**, **Daily**, or **Weekly**.

The **Day of Week**, **Hour of Day**, and **Minute** drop-down menus are disabled based on the selected frequency. For example, if you select **Daily**, the **Day of Week** drop-down menu is disabled as this field is not applicable to a daily frequency.

6 (Optional) Select the **Exclude System Events** check box if you do not want to back up system event tables.

7 (Optional) Select the **Exclude Audit Log** check box if you do not want to back up audit log tables.

8 Type the **Host IP Address** of the system where the backup will be saved.

9 (Optional) Type the **Host Name** of the backup system.

10 Type the **User Name** required to login to the backup system.

11 Type the **Password** associated with the user name for the backup system.

12 In the **Backup Directory** field, type the absolute path where backups will be stored.

13 Type a text string in **Filename Prefix**.

This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as `ppdbHH_MM_SS_DayDDMonYYYY`.

14 From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**, based on what the destination supports.

15 Click **Save Settings**.

Installing vShield Edge, vShield App, vShield Endpoint, and vShield Data Security

4

After the vShield Manager is installed, you can obtain licenses to activate the vShield App, vShield Endpoint, vShield Edge, and vShield Data Security components. The vShield Manager OVA package includes the drivers and files required to install these add-on components. A vShield App license allows you to use the vShield Endpoint component as well.

vShield virtual appliances include VMware Tools. Do not attempt to alter or upgrade the VMware Tools software on a vShield virtual appliance.

This chapter includes the following topics:

Running vShield Licensed Components in Evaluation Mode

Before purchasing and activating licenses for vShield Edge, vShield App, and vShield Endpoint, you can install and run evaluation modes of the software. When run in evaluation mode, intended for demonstration and evaluation purposes, your vShield Edge, vShield App, and vShield Endpoint are completely operational immediately after installation, do not require any licensing configuration, and provide full functionality for 60 days from the time you first activate them.

When run in evaluation mode, vShield components can support a maximum allowed number of instances.

After the 60-day trial period expires, unless you obtain licenses for your software, you cannot use vShield. For example, you cannot power on vShield App or vShield Edge virtual appliances or protect your virtual machines.

To continue using the vShield App and vShield Edge functionality without interruptions or to restore the features that become unavailable after the 60-day trial, you need to obtain and install license files that activate the features appropriate for the vShield component you purchased.

Install vShield Component Licenses

You must install a CIS or vCloud Networking and Security (vCNS) license before installing vShield App and vShield Edge. The vSphere license includes a license for vShield Endpoint. You can install these licenses after vShield Manager installation is complete by using the vSphere Client.

Procedure

1 From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.

2 From the Management tab, select **Asset**.

3 Right-click a CIS or vCNS asset and select **Change license key**.

4 Select **Assign a new license key** and click **Enter Key**.

5 Enter the license key, enter an optional label for the key, and click **OK**.

6 Click **OK**.

7 Repeat these steps for each vShield component for which you have a license.

Install vShield App

You can install vShield App on an ESX host.

NOTE The network connection of a virtual machine is interrupted when you protect it with vShield App. If vCenter Server is running on a virtual machine and it becomes disconnected from the network, the vShield App installation process might halt without completing. VMware recommends that you place the vCenter Server, vCenter Server database, and third party or internal service virtual machines that you do not want protected in the Virtual Machines Exclusion List. For information on excluding virtual machines from vShield App protection, see the *vShield Administration Guide*.

IMPORTANT If the vCenter Server or vCenter Server database virtual machines are on the ESX host on which you are installing vShield App, migrate them to another host before installing vShield App.

Prerequisites

- Verify that you have a unique IP address for the management (MGT) port of each vShield App virtual appliance. Each IP address should be reachable from vShield Manager and sit on the Management network used for vCenter and ESX host management interfaces. Using an incorrect IP address will require you to uninstall and re-install vShield App on this host.
- Local or network storage in which to place the vShield App.

Procedure

1 Log in to the vSphere Client.

2 Select an ESX host from the inventory tree.

3 Click the **vShield** tab.

4 Accept the security certificate.

5 Click **Install** for the **vShield App** service.

6 Under vShield App, provide the following information.

Option	Description
Datastore	Select the datastore on which to store the vShield App virtual machine files.
Management Port Group	Select the port group to host the vShield App management interface. This port group must be able to reach the vShield Manager's port group.
IP Address	Type the IP address to assign to the vShield App management interface. IMPORTANT Ensure that you type the correct IP address. To change the IP address after installing vShield App, you would need to uninstall vShield App and reboot the ESX host.
Netmask	Type the IP subnet mask associated with the assigned IP address.
Default Gateway	Type the IP address of the default network gateway.

7 Click **Install**.

You can follow the progress of the vShield App installation on the Recent Tasks pane of the vSphere Client screen.

What to do next

Allow vShield App to run during normal operation and then examine the traffic going in and out of your virtual network. Based on this information, configure firewall rules. Each vShield App inherits global firewall rules set in the vShield Manager. The default firewall rule set allows all traffic to pass. You must configure blocking rules to explicitly block traffic. To configure App Firewall rules, see the *vShield Administration Guide*.

NOTE If you have installed vShield App on a stateless ESX, you must follow the steps in "Install vShield App on a Stateless ESX Host," on page 27 before rebooting the host.

CAUTION Do not modify service virtual machines through the vSphere client. This may break communication between vShield Manager and vShield App and compromise the security of your network.

Install vShield App on a Stateless ESX Host

If you installed vShield App on a stateless ESX host, you must perform the steps below before rebooting any of the ESX hosts on which vShield App is installed.

Prerequisites

- Install vShield App on the stateless ESX host.
- Ensure that the firewall configuration changes done on the host by the VIB are complete.
  a In the vCenter client, select the stateless ESX host from the inventory panel.
  b Click the **Configuration** tab.
  c Check that a DVFilter entry appears in the Incoming Connections under the Firewall panel. If no DVFilter entry appears, click **Refresh.**
- Create a host profile. For more information, see the *vSphere Installation and Setup Guide*.

Procedure

1 Edit the host profile.
  a In the vCenter client, select **Home > Management > Host Profiles.**
  b Select the profile to edit.

c Click **Edit Host Profile**.

d Select **Networking Configuration > Host Port Group > vmservice-vmknic-pg > IP address settings > How is IPv4 address determined**.

e Type the IP address as **`169.254.1.1`** and Subnet mask as **`255.255.255.0`**.

f Select **Networking Configuration > Host Port Group > vmservice-vmknic-pg > Determine how MAC address for vmknic should be decided**.

g Select **User must explicitly choose the policy option**.

2 Save the host profile.

3 In a web browser, type https://vsm-ip/bin/offline-bundles/VMware-vShield-fastpath-esx5x-5.0.1-766127.zip and download the zip file.

4 Use the host profile you created in Step 1 and the offline bundle you downloaded in Step 3 to update the stateless ESX configuration.

Installing vShield Edge

You can install multiple vShield Edge virtual appliances in a datacenter. Each vShield Edge virtual appliance can have a total of ten uplink and internal network interfaces. The internal interfaces connect to secured port groups and act as the gateway for all protected virtual machines in the port group. The subnet assigned to the internal interface can be RFC 1918 private space. Firewall rules and other vShield Edge services are enforced on traffic between interfaces.

uplink interfaces of vShield Edge connect to uplink port groups that have access to a shared corporate network or a service that provides access layer networking.

Multiple external IP addresses can be configured for load balancer, site-to-site VPN, and NAT services. Overlapping IP addresses are not allowed for internal interfaces, and overlapping subnets are not allowed for internal and uplink interfaces.

Prerequisites

You must have been assigned the Enterprise Administrator or vShield Administrator role .

Procedure

1 Open the Add Edge Wizard on page 29

Open the Add Edge wizard to install and configure a vShield Edge instance.

2 Name vShield Edge on page 29

vShield Edge requires a descriptive name that is unique across all vShield Edge virtual machines in a single tenant. This name appears in your vCenter inventory.

3 Specify the CLI Credentials on page 29

Edit the credentials to be used for logging in to the Command Line Interface (CLI).

4 Add Appliances on page 30

You must add an appliance before you can deploy a vShield Edge. If you do not add an appliance when you install vShield Edge, vShield Edge remains in an offline mode until you add an appliance.

5 Add Internal and Uplink Interfaces on page 31

You can add up to ten internal and uplink interfaces to a vShield Edge virtual machine.

6 Configure the Default Gateway on page 32

Provide the IP address for the vShield Edge default gateway.

7 Configure Firewall Policy and High Availability on page 32

You can change the default firewall policy, which blocks all incoming traffic.

8 Confirm Settings and Install the vShield Edge on page 33

Before you install the vShield Edge, review the settings you entered.

Open the Add Edge Wizard

Open the Add Edge wizard to install and configure a vShield Edge instance.

Procedure

1 Log in to the vSphere Client.

2 Select a datacenter resource from the inventory tree.

3 Click the **Network Virtualization** tab.

4 Click **Edges**.

5 Click the **Add** ( ) icon.

The Add Edge wizard appears.

Name vShield Edge

vShield Edge requires a descriptive name that is unique across all vShield Edge virtual machines in a single tenant. This name appears in your vCenter inventory.

Procedure

1 Type a name for the vShield Edge virtual machine.

This name appears in your vCenter inventory. The name should be unique across all Edges within a single tenant.

If you do not specify a name, vShield Manager creates a unique name for each vShield Edge.

2 (Optional) Type a host name for the vShield Edge virtual machine.

This name appears in CLI. If you do not specify the hostame, the name you specified in Step 1 shows up in CLI as well.

3 (Optional) Type a description for this vShield Edge.

4 (Optional) Type the tenant for this vShield Edge.

5 (Optional) Select **Enable HA** to enable high availability (HA).

6 Click **Next.**

Specify the CLI Credentials

Edit the credentials to be used for logging in to the Command Line Interface (CLI).

Procedure

1 On the CLI Credentials page, specify the CLI credentials for your vShield Edge virtual machine.

Option	Action
CLI user name	Edit if required.
CLI password	Edit tif required.

2 (Optional) Click **Enable SSH access** if required.

3 Click **Next**.

The Edge Appliances page appears.

Add Appliances

You must add an appliance before you can deploy a vShield Edge. If you do not add an appliance when you install vShield Edge, vShield Edge remains in an offline mode until you add an appliance.

Prerequisites

For high availability, verify that the resource pool has enough capacity for both HA virtual machines to be deployed. A compact vShield Edge virtual machine requires 256 MB of memory, a large vShield Edge virtual machine requires 1 GB of memory, and an X-Large vShield Edge virtual machine requires 8 GB of memory. The datastore must have at least 512 MB disk space.

Procedure

1 On the Edge Appliances page, select the size of the vShield Edge instance based on your system resources.

The **Large** vShield Edge has more CPU, memory, and disk space than the **Compact** vShield Edge, and supports a bigger number of concurrent SSL VPN-Plus users. The **X-Large** vShield Edge is suited for environments which have Load Balancer with millions of concurrent sessions. The X-Large vShield Edge does not support SSL VPN.

2 Click **Enable auto rule generation** to add firewall, NAT, and routing routes to enable control traffic to flow for these services..

If you do not select **Enable auto rule generation**, you must manually create firewall rules to add firewall, NAT, and routing routes to allow control channel traffic for vShield Edge services such as Load Balancing, VPN, etc.

NOTE Auto rule generation does not create rules for data-channel traffic.

---

3 Click **Enable AESNI** to enable Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI).

4 In **Edge Appliances**, click the **Add** ( ) icon to add an appliance.

If you had selected **Enable HA** on the Name and Description page, you can add two appliances. If you add a single appliance, vShield Edge replicates its configuration for the standby appliance ensures that the two HA vShield Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMontion them to the same host).

5 In the Add Edge Appliance dialog box, select the cluster or resource pool and datastore for the appliance.

6 (Optional) Select the host on which the appliance is to be added.

7 (Optional) Select the vCenter folder within which the appliance is to be added.

8 Click **Add**.

9 Click **Next.**

The Interfaces page appears.

Add Internal and Uplink Interfaces

You can add up to ten internal and uplink interfaces to a vShield Edge virtual machine.

Procedure

1 On the Interfaces page, click the **Add** ( ) icon and type a name for the interface.

2 Select **Internal** or **Uplink** to indicate whether this is an internal or external interface.

You must add at least one internal interface for HA to work.

3 Select the port group or VXLAN virtual wire to which this interface should be connected.

a Click **Select** next to the **Connected To** field.

b Dpending on what you want to connect to the interface, click the **Virtual Wire**, **Standard Portgroup**, or **Distributed Portgroup** tab.

c Select the appropriate virtual wire or portgroup.

d Click **Select**.

4 Select the connectivity status for the interface.

5 In **Configure Subnets**, click the **Add** ( ) icon to add a subnet for the interface.

An interface can have multiple non-overlapping subnets.

6 In **Add Subnet**, click the **Add** ( ) icon to an IP address.

If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. vShield Edge considers the Primary IP address as the source address for locally generated traffic.

You must add an IP address to an interface before using it on any feature configuration.

7 Type the subnet mask for the interface and click **Save**.

8 (Optional) Type the MAC address for the interface. If HA is enabled, type two management IP addresses in CIDR format.

Heartbeats of the two vShield Edge HA virtual machines are communicated through these management IP addresses. The management IP addresses must be in the same L2/subnet and be able to communicate with each other.

9 Change the default MTU if required.

10 In **Options**, select the required options.

Option	Description
Enable Proxy ARP	Supports overlapping network forwarding between different interfaces.
Send ICMP Redirect	Conveys routing information to hosts.

11 Type the fence parameters and click **Add**.

12 Repeat steps Step 1 through Step 11 to add additional interfaces.

13 Click **Next**.

The Default Gateway page appears.

Configure the Default Gateway

Provide the IP address for the vShield Edge default gateway.

Procedure

1 On the Default Gateway page, select **Configure Default Gateway**.

2 Select the interface that can communicate with the next hop or gateway IP address.

3 Type the IP address for the default gateway.

4 In **MTU**, the default MTU for the interface you selected in Step 2 is displayed. You can edit this value, but it cannot be more than the configured MTU on the interface.

5 Click **Next.**

The Firewall & HA page appears.

Configure Firewall Policy and High Availability

You can change the default firewall policy, which blocks all incoming traffic.

You must configure HA parameters for high availability to work on network configurations on vShield Edge. vShield Edge supports two virtual machines for high availability, both of which are kept up to date with user configurations. If a heartbeat failure occurs on the primary virtual machine, the secondary virtual machine state is changed to active. Thus, one vShield Edge virtual machine is always active on the network.

Procedure

1 On the Firewall & HA page, select **Configure Firewall default policy**.

2 Specify whether to accept or deny incoming traffic by default.

Any firewall rules you create override the default policy.

3 Select whether to log incoming traffic.

If you create firewall rules that override the default policy, logging is determined by the rules you created. Enabling default logging may generate too many logs and affect the performance of your vShield Edge. Hence, it is recommended that you enable default logging only while troubleshooting or debugging.

4 If you selected **Enable HA** on the Name & Description page, complete the **Configure HA parameters** section.

vShield Edge replicates the configuration of the primary appliance for the standby appliance and ensures that the two HA vShield Edge virtual machines are not on the same ESX host even after you use DRS and vMotion. Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured. Local link IPs are assigned to HA virtual machines in the vShield Edge HA so that they can communicate with each other. You can specify management IP addresses to override the local links.

a Select the internal interface for which to configure HA parameters.

b (Optional) Type the period in seconds within which, if the backup appliance does not receive a heartbeat signal from the primary appliance, the primary appliance is considered inactive and the back up appliance takes over.

The default interval is 6 seconds.

c (Optional) Type two management IP addresses in CIDR format to override the local link IPs assigned to the HA virtual machines.

Ensure that the management IP addresses are not overlapping with any of the interface subnets.

5 Click **Next**.

The Summary page appears.

Confirm Settings and Install the vShieldEdge

Before you install the vShield Edge, review the settings you entered.

Procedure

1 On the Summary page, review the settings for the vShield Edge.

2 Click **Previous** to modify the settings

3 Click **Finish** to accept the settings and install the vShield Edge.

Installing vShield Endpoint

The installation instructions that follow assume that you have the following system:

- A datacenter with supported versions of vCenter Server and ESXi installed on each host in the cluster. For information on the required versions, see Chapter 2, "Preparing for Installation," on page 13.
- vShield Manager 5.1 installed and running.
- Anti-virus solution management server installed and running.

vShield Endpoint Installation Workflow

After you prepare the ESX host for vShield Endpoint installation, install vShield Endpoint in these stages:

1 Deploy and configure a security virtual machine (SVM) to each ESX host according to the instructions from the anti-virus solution provider.

2 Install the latest version of VMware Tools released for the version of ESX that you have on all virtual machines to be protected.

The vShield Endpoint host component adds two firewall rules to the ESX host:

- The vShield-Endpoint-Mux rule opens ports 48651 to port 48666 for communication between the host component and partner security VMs.

- The vShield-Endpoint-Mux-Partners rule may be used by partners to install a host component. It is disabled by default.

Install VMware Tools on the Guest Virtual Machines

VMware Tools include the vShield Thin Agent that must be installed on each guest virtual machine to be protected. Virtual machines with VMware Tools installed are automatically protected whenever they are started up on an ESX host that has the security solution installed. That is, protected virtual machines retain the security protection through shut downs and restarts, and even after a vMotion move to another ESX host with the security solution installed.

Prerequisites

Make sure that the guest virtual machine has a supported version of Windows installed. The following Windows operating systems are supported for vShield Endpoint 5.0:

- Windows Vista (32 bit)
- Windows 7 (32/64 bit)
- Windows XP SP3 and above (32 bit)
- Windows 2003 SP2 and above (32/64 bit)
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (64 bit)

Procedure

1 Select the type of installation for VMware Tools.

ESX Version of the Host	Action
ESX 5.0 Patch 1 or later	Follow the installation instructions in *Installing and Configuring VMware Tools* till the point you see the Setup Type wizard.
ESX 4.1 Patch 3 or later	Follow the installation instructions in the Knowledge Base article http://kb.vmware.com/kb/2008084 till the point you see the Setup Type wizard.

2 in the Setup Type wizard, select one of the following options:

- Complete.
- Custom.
  - From the VMware Device Drivers list, select VMCI Driver, then select vShield Driver.

Install vShield Data Security

You can install vShield Data Security only after installing vShield Endpoint.

Prerequisites

Verify that vShield Endpoint has been installed on the host and guest virtual machines..

Procedure

1 Log in to the vSphere Client.

2 Select an ESX host from the inventory tree.

3 Click the **vShield** tab.

4 Click **Install** next to vShield Data Security.

5 Select the **vShield Data Security** checkbox.

6 Under vShield Data Security, enter the following information.

Option	Description
Datastore	Select the datastore on which to add the vShield Data Security service virtual machine.
Management Port Group	Select the port group to host the vShield Data Security's management interface. This port group must be able to reach the vShield Manager's port group.

7 To configure a static IP, select the **Configure static IP for management interface** checkbox.

Enter the **IP address**, **Netmask**, and **Default Gateway** details.

NOTE If you do not select **Configure static IP for management interface**, an IP address is assigned using Dynamic Host Configuration Protocol (DHCP).

8 Click **Install.**

The vShield Data Security virtual machine is installed on the selected host.

Uninstalling vShield Components 5

This chapter details the steps required to uninstall vShield components from your vCenter inventory.

This chapter includes the following topics:

Uninstall a vShield App Virtual Appliance

Uninstalling a vShield App removes the virtual appliance from the network and vCenter Server.

CAUTION Uninstalling a vShield App places the ESX host in maintenance mode. The ESX host reboots during uninstallation. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling the vShield App.

Procedure

1 Log in to the vSphere Client.

2 Select the ESX host from the inventory tree.

3 Click the **vShield** tab.

4 Click **Uninstall** for the **vShield App** service.

If you are uninstalling vShield App on a stateless ESX host, ignore the VIB uninstallation errors.

5 If the ESX host was in maintenance mode before you started uninstalling vShield App, remove the vShield App virtual machines manually after the automatic uninstallation is complete.

The instance is uninstalled.

Uninstall a vShield Edge

You can uninstall a vShield Edge by using the vSphere Client.

Prerequisites

You must have been assigned the Enterprise Administrator or vShield Administrator role .

Procedure

1 Log in to the vSphere Client.

2 Select a datacenter resource from the inventory tree.

3 Click the **Network Virtualization** tab.

4 Click **Edges**.

5 Click the **Delete** ( ) icon.

Uninstall a vShield Data Security Virtual Machine

After you uninstall the vShield Data Security virtual machine, you must uninstall the virtual appliance according to the instructions from the VMware partner.

Procedure

1 Log in to the vSphere Client.

2 Select an ESX host from the inventory tree.

3 Click the **vShield** tab.

4 Click **Uninstall** for the vShield Data Security service.

Uninstall a vShield Endpoint Module

Uninstalling a vShield Endpoint module removes a vShield Endpoint module from an ESX host. You must perform these steps in the following order.

CAUTION If vShield Data Security is installed on the ESX host, you must uninstall it before uninstalling vShield Endpoint.

Uninstall Products That Use vShield Endpoint

Before you uninstall a vShield Endpoint module from a host, you must uninstall all products that are using vShield Endpoint from that host. Use the instructions from the solution provider.

Uninstall the vShield Endpoint Module from the vSphere Client

Uninstalling an vShield Endpoint module removes the vShield Endpoint Module from an ESX host.

Procedure

1 Log in to the vSphere Client.

2 Select an ESX host from the inventory tree.

3 Click the **vShield** tab.

4 Click **Uninstall** for the **vShield Endpoint** service.

Upgrading vShield 6

To upgrade vShield, you must first upgrade the vShield Manager, then update the other components for which you have a license.

This chapter includes the following topics:

Upgrade vShield Manager

You can upgrade vShield Manager to a new version only from the vShield Manager user interface. You can upgrade vShield App and vShield Edge to a new version from the vShield Manager user interface or by using REST APIs.

Prerequisites

- Take a snapshot of vShield Manager so that you can revert to it in case the upgrade fails.
- If you are using vShield Endpoint 4.1, uninstall vShield Endpoint before upgrading vShield Manager.

CAUTION Do not uninstall a deployed instance of vShield Manager appliance.

Upgrade vShield Manager from Version 4.x to Version 5.1 or Later

To upgrade vShield Manager 4.x to version 5.1 or later, you must first upgrade to version 5.0 and then to version 5.1.

Upgrade vShield Manager to Version 5.0

This is the first step when upgrading vShield manager from version 4.x to version 5.1 or later.

Procedure

1. Download the vShield upgrade bundle to a location to which vShield Manager can browse. The name of the upgrade bundle file is something like `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.
2. From the vShield Manager inventory panel, click **Settings & Reports**.
3. Click the **Updates** tab.

4 Click **Upload Settings**.

5 Click **Browse** and select the `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz` file.

6 Click **Open**.

7 Click **Upload Upgrade Bundle**.

8 Click **Install** to begin the upgrade process.

9 Click **Confirm Install**. The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.

10 After the reboot, log back in to the vShield Manager and click the Updates tab. The Installed Release panel displays version 5.0 that you just installed.

What to do next

When upgrading from vShield Manager 4.1, you must register the vCenter Server again.

You can now upgrade to vShield Manager 5.1 or later. See "Upgrade vShield Manager from Version 5.1 to 5.1.x," on page 44.

Upgrade vShield Manager from Version 5.0 to Version 5.1.x

vShield Manager version 5.1 and later needs a minimum of 2.5 GB disk space. You must run the maintenance bundle to make disk space available for the upgraded vShield Manager.

Procedure

1 Free Disk Space by Installing Maintenance Bundle on page 41

A minimum of 2.5 GB free disk space in the `/common` partition is required for the upgrade process. The vShield maintenance bundle makes disk space available on the vShield Manager. It stops the vShield Manager process and starts it again after the completion of the file system cleanup activity.

2 Upgrade vShield Manager to Version 5.1 or Later on page 41

3 Create Post-Upgrade Backup on page 43

Starting from version 5.1, vShield Manager requires an upgrade to its virtual hardware. This virtual hardware upgrade is not automatically performed as part of the vShield upgrade process for vShield Manager versions 5.0.x or below. Architectural changes for improved scalability, performance and increased logging and reporting capabilities require an upgrade of vShield Manager's virtual hardware. Some of these changes include 64-bit support, 2 vCPUs, 8 GB RAM, a larger virtual disk along with other virtual hardware properties.

4 Restore Post-Upgrade Backup on page 43

Restore the vShield Manager backup.

5 Install 5.1.2a Maintenance Patch on page 43

If you are using vShield version 5.1.2, you must install the 5.1.2a patch.

Free Disk Space by Installing Maintenance Bundle

A minimum of 2.5 GB free disk space in the `/common` partition is required for the upgrade process. The vShield maintenance bundle makes disk space available on the vShield Manager. It stops the vShield Manager process and starts it again after the completion of the file system cleanup activity.

Prerequisites

NOTE Existing logs, flow monitoring data, and system event and audit logs on the vShield Manager appliance are deleted as part of this procedure. You can retrieve the system event and audit logs using the appropriate REST API call before applying the maintenance bundle. The tech support log bundle contains log messages of this procedure.

Procedure

1 Right-click the vShield Manager virtual machine and click **Open Console** to open the command line interface (CLI) of the vShield Manager.

2 Switch to enable mode.

3 After logging in, type the `show filesystems` command.

You need at least 5% free disk space in the `/common` partition to install the maintenance bundle.

4 Type the `show manager log follow` command. Keep this console open as you follow the rest of the steps.

5 Download the vShield maintenance bundle to a location to which vShield Manager can browse. The name of the maintenance bundle file is something like `VMware-vShield-Manager-upgrade-bundle-maintenance-`*`bundlebuildNumber`*`.tar.gz`.

6 In the vShield Manager Inventory panel, click **Settings & Reports**.

7 Click the **Updates** tab.

8 Click **Upload Settings**.

9 Click **Browse** and select the `VMware-vShield-Manager-upgrade-bundle-maintenance-`*`bundlebuildNumber`*`.tar.gz` file.

10 Click **Open**.

11 Click **Upload File**.

12 Click **Install** to begin the upgrade process.

13 Click **Confirm Install**.

14 In the CLI, follow the output of the `show manager log` command. After you see the `maintenance-fs-cleanup: Filesystem cleanup successful` message, log in to the vShield Manager user interface.

The upgrade process restarts the vShield Manager service, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are restarted.

15 Log in to the CLI of the vShield Manager, switch to enable mode, and run the `show filesystems` command to ensure there is at least 2.5 GB free space for the upgrade.

Upgrade vShield Manager to Version 5.1 or Later

Procedure

1 Download the vShield upgrade bundle to a location to which vShield Manager can browse. The name of the upgrade bundle file is something like `VMware-vShield-Manager-upgrade_bundle-`*`buildNumber`*`.tar.gz`.

2 From the vShield Manager inventory panel, click **Settings & Reports**.

3 Click the **Updates** tab.

4 Click **Upload Settings**.

5 Click **Browse** and select the `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz` file.

6 Click **Open**.

7 Click **Upload Upgrade Bundle**.

8 Click **Install** to begin the upgrade process.

9 Click **Confirm Install**. The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.

10 After the reboot, log back in to the vShield Manager and click the Updates tab. The Installed Release panel displays version 5.1.2 that you just installed.

vShield App rules from the previous release are upgraded as described below.

Firewall feature in prior version	Result of upgrade to version 5.1
Firewall rules allowed at datacenter, cluster, and port group levels	Firewall rules allowed at namespace level - datacenter, port group with independent name space, and virtual wire levels After upgrade, firewall rules from non-namespace contexts are moved to corresponding datacenter. Migrated rules are merged with datacenter rules in the following order: ■ datacenter high ■ cluster ■ Non-namespace port group or dvport group ■ datacenter low ■ datacenter default
Firewall rules supported raw IP and MAC addresses as well as port-protocol and protocol-subtype	Firewall rules support only IPsets, MACsets, and security groups After upgrade, IPset, MACset, or service is internally created as appropriate. The names of the created containers follow these naming conventions: ■ IPset/MACset: *ip/macValue-contextName* ■ Service: *protocolName-portNumber-contextName* or *protocolName-subtypeName-contextName*
Firewall rules included High and Low precedence rules. Non-namespace port group rules had None precedence.	High and Low precedence rules not supported. After upgrade, all non-default precedence rules are changed to None precedence.
A single Spoofguard global setting was applied across all datacenters in inventory	Spoofguard global settings are applied to each namespace. You can change spoofguard settings on per namespace basis after upgrade.

In addition, all firewall histories and flows recorded prior to upgrade are deleted.

What to do next

Clear the browser cache on all clients that have accessed the previous version of the product. This action clears the cached javascript or other files from that version that might have changed in the current version

Create Post-Upgrade Backup

Starting from version 5.1, vShield Manager requires an upgrade to its virtual hardware. This virtual hardware upgrade is not automatically performed as part of the vShield upgrade process for vShield Manager versions 5.0.x or below. Architectural changes for improved scalability, performance and increased logging and reporting capabilities require an upgrade of vShield Manager's virtual hardware. Some of these changes include 64-bit support, 2 vCPUs, 8 GB RAM, a larger virtual disk along with other virtual hardware properties.

Procedure

1 From the vShield Manager Inventory panel, click **Settings & Reports**.

2 Click the **Configuration** tab.

3 Click **Backups.**

4 Type the host IP address or name of the system where the backup is to be saved.

5 Type the user name and password required to login to the backup system (ftp/sftp server).

6 In the **Backup Directory** field, type the absolute path where backups will be stored.

7 Type a text string in **Filename Prefix**. This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type `ppdb`, the resulting backup is named as `ppdb`*HH_MM_SS_DayDDMonYYYY*.

8 From the **Transfer Protocol** drop-down menu, select SFTP or FTP, based on what the destination supports.

9 Click **Save Settings** and then click **Backup**.

10 Click **View Backups** to ensure the backup was created.

Restore Post-Upgrade Backup

Restore the vShield Manager backup.

Procedure

1 Power off the vShield Manager.

2 Download the 5.1.2 vShield Manager .OVA installation package.

3 Deploy a new vShield Manager into your vSphere inventory to replace the existing vShield Manager.

4 Power on the new vShield Manager and go through the initial setup, giving it the same IP address as the one that is currently powered off.

5 Configure the vShield Manager Backups page to view the backups currently stored on the ftp/sftp server.

6 Identify the vShield Manager backup created earlier and click **Restore**.

Install 5.1.2a Maintenance Patch

If you are using vShield version 5.1.2, you must install the 5.1.2a patch.

Procedure

1 Download the vShield 5.1.2a maintenance patch to a location to which vShield Manager can browse. The name of the patch bundle file is something like **VMware-vShield-Manager-upgrade-bundle-maintenance-***bundlebuildNumber***.tar.gz**.

2 From the vShield Manager Inventory panel, click **Settings & Reports**.

3 Click the **Updates** tab.

4 Click **Upload Settings**.

5 Click **Browse** and select the file you had downloaded in Step 1.

6 Click **Open**.

7 Click **Upload File**.

8 Click **Install** to begin the upgrade process.

9 Click **Confirm Install**.

The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.

Upgrade vShield Manager from Version 5.1 to 5.1.x

Procedure

1 Download the vShield upgrade bundle to a location to which vShield Manager can browse. The name of the upgrade bundle file is something like `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

2 From the vShield Manager inventory panel, click **Settings & Reports**.

3 Click the **Updates** tab.

4 Click **Upload Settings**.

5 Click **Browse** and select the `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz` file.

6 Click **Open**.

7 Click **Upload Upgrade Bundle**.

8 Click **Install** to begin the upgrade process.

9 Click **Confirm Install**. The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.

10 After the reboot, log back in to the vShield Manager and click the Updates tab. The Installed Release panel displays version 5.1.2 that you just installed.

11 Download the vShield 5.1.2a maintenance patch to a location to which vShield Manager can browse. The name of the patch bundle file is something like **VMware-vShield-Manager-upgrade-bundle-maintenance-***bundlebuildNumber***.tar.gz.**

12 Follow Step 2 till Step 4.

13 Click **Browse** and select the file you had downloaded in Step 11

14 Follow Step 6 till Step 9.

Upgrade vShield Edge

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 is not backward compatible and you cannot use 2.0 REST calls after the upgrade.

Prerequisites

You must have been assigned the Enterprise Administrator or vShield Administrator role .

Procedure

1 Log in to the vSphere Client.

2 Select **Views > Inventory > Networking**.

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.

Upgrade vShield Endpoint

The upgrade procedure to follow depends on the product version that you are using.

Upgrade vShield Endpoint from Version 4.1 to 5.0

To upgrade vShield Endpoint from version 4.1 to 5.0, you must first uninstall vShield Endpoint on each host in your datacenter, upgrade vShield Manager, and then install the new release.

1 If the protected virtual machines are running in a cluster, deactivate DRS.

2 Deactivate all Trend DSVAs. This is required to remove vShield related VFILE filter entries from the virtual machines.

3 If you had deactivated DRS in step 1, re-activate it.

4 Uninstall vShield Endpoint on each host in your datacenter. For more information, see "Uninstall the vShield Endpoint Module from the vSphere Client," on page 38.

5 Upgrade VMware vCenter to the required version. For more information, see Chapter 2, "Preparing for Installation," on page 13.

6 Upgrade each host to the required VMware ESX version. For more information, see Chapter 2, "Preparing for Installation," on page 13.

7 Upgrade vShield Manager. For more information, see "Upgrade vShield Manager," on page 39.

8 Install vShield Endpoint. For more information, see "Installing vShield Endpoint," on page 33.

Upgrade vShield Endpoint from 5.0 to a Later Version

To upgrade vShield Endpoint from 5.0 to a later version, you must first upgrade vShield Manager, then update vShield Endpoint on each host in your datacenter.

Procedure

1 Log in to the vSphere Client.

2 Select **Inventory > Hosts and Clusters**.

3 Select the host on which you want to upgrade vShield Endpoint.

4 Click the **vShield** tab.

The **General** tab displays each vShield component that is installed on the selected host and the available version.

5 Select **Update** next to vShield Endpoint.

6 Select the **vShield Endpoint** check box.

7 Click **Install**.

Upgrade vShield Data Security

Upgrade vShield Data Security on each host in your datacenter. It is recommended that you upgrade vShield Endpoint before upgrading vShield Data Security.

Procedure

1 Log in to the vSphere Client.

2 Go to **Inventory > Hosts and Clusters**.

3 Select the host on which you want to upgrade vShield App.

The **Summary** tab displays each vShield component that is installed on the selected host and the available release.

4 Select **Update** next to vShield Data Security.

5 Select the **vShield Data Security** checkbox.

6 Click **Install.**

Troubleshooting Installation Issues 7

This section describes installation issues.

This chapter includes the following topics:

vShield App Installation Fails

Installing vShield App results in an error.

Problem

vShield App installation may fail due to a previous incomplete installation or problems during uninstallation of a previous version.

Solution

1 Start with an automated uninstall of vShield App. See Chapter 5, "Uninstalling vShield Components," on page 37.

2 Verify that the required modules are loaded in the ESX host by logging in to an SSH client and typing the following command:

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

dvfilter 2 72

vmkapiv1_0_0_0_dvfilter_shim0 8
```

3 If the required modules are not loaded, type the following commands to load them.

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

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

4 Log in to vShield Manager CLI as an admin and reset the web interface by typing the following command:

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

5 After the **`no web-manager`** command is completed, restart the web services by typing the following command:

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

If you were logged in to the vShield Manager user interface, log back in after the web services restart.

6 (Optional) Reboot the ESX host if you had seen the following error when installing vShield App:

```
vShield App installation encountered error while installing vib
```

7 Delete the vmservice-vswitch that was created during the install by following the steps below.

a Log in to the vSphere Client.

b Select the ESX host from the inventory tree.

c Click the **Configuration** tab.

d In the Software panel, click **Networking**.

e In the **Standard Switch:vmservice-vswitch** area, click **Remove**.

8 Delete the **Net.DVFilterBindIpAddress** property for the host by following the steps below:

a In the vSphere client, select the ESX host from the inventory tree.

b Click the **Configuration** tab.

c In the Software panel, click **Advanced Settings**

d In the Advanced Settings dialog box, click **Net**.

e Ensure that the Net.**DVFilterBindIpAddress** field is blank.

9 Install vShield App again. See "Install vShield App," on page 26.

vShield Data Security Installation Fails

Problem

During vShield Data Security installation, I get an error while installing the service virtual machine and an error message on vSphere client.

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

.

Cause

The DNS setup for vShield Manager may not be consistent with the DNS setup for the host in vCenter Server.

Solution

Change the vShield Manager DNS setup so that it matches the host setup.

Index