

Administration Guide

vShield Zones 1.0

EN-000167-00



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

© 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware, the VMware “boxes” logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

| | |
|---|-----------|
| About This Book | 7 |
| 1 Overview of vShield Zones | 9 |
| vShield Zones Components | 9 |
| vShield Manager | 9 |
| vShield | 10 |
| 2 vShield Manager User Interface Basics | 11 |
| Logging in to the vShield Manager | 11 |
| Accessing the Online Help | 11 |
| vShield Manager User Interface | 12 |
| vShield Manager Inventory Panel | 12 |
| Refreshing the Inventory Panel | 12 |
| Searching the Inventory Panel | 12 |
| vShield Manager Configuration Panel | 12 |
| 3 Management System Settings | 13 |
| Identifying Your vCenter Server | 13 |
| Identifying DNS Services | 14 |
| Setting the vShield Manager Date and Time | 14 |
| Identifying a Proxy Server | 14 |
| Downloading a Technical Support Log from a Component | 15 |
| Backing Up vShield Manager Data | 15 |
| Viewing vShield Manager System Status | 15 |
| Installing a vShield Manually | 15 |
| Registering the vShield Manager as a vSphere Client Plug-in | 16 |
| 4 Backing Up vShield Manager Data | 17 |
| Backing Up Your vShield Manager Data on Demand | 17 |
| Scheduling a Backup of vShield Manager Data | 18 |
| Restoring a Backup | 18 |
| 5 Updating the System Software | 19 |
| Viewing Current System Software | 19 |
| Uploading an Update | 19 |
| Reviewing the Update History | 20 |
| 6 User Management | 21 |
| Managing User Rights | 21 |
| Managing the Default User Account | 22 |
| Adding a User | 22 |
| Assigning a Role and Rights to a User | 22 |
| Editing a User Account | 22 |
| Deleting a User Account | 23 |

| | | |
|-----------|--|-----------|
| 7 | System Events | 25 |
| | Viewing the System Event Report | 25 |
| | System Event Notifications | 26 |
| | vShield Manager Virtual Appliance Events | 26 |
| | vShield Virtual Appliance Events | 26 |
| | Syslog Format | 27 |
| 8 | Viewing the Audit Log | 29 |
| 9 | vShield Management | 31 |
| | Installing a vShield | 31 |
| | Installing a vShield Using the vShield Template | 31 |
| | Installing a vShield Manually on a vNetwork Distributed Switch | 32 |
| | Create a Second vNetwork Distributed Switch | 33 |
| | Create the Protected dvPort Group | 33 |
| | Create the Unprotected dvPort Group | 34 |
| | Install the vShield | 34 |
| | Assign the vShield Interfaces to Port Groups | 35 |
| | Move the Virtual Machines from vNDS-1 to vNDS-2 | 36 |
| | Uninstalling a vShield | 36 |
| | Uninstalling a Template-Based vShield | 36 |
| | Uninstalling a Manually Installed vShield | 37 |
| | Sending vShield System Events to a Syslog Server | 37 |
| | Backing Up the Running CLI Configuration of a vShield | 37 |
| | Viewing the Current System Status of a vShield | 38 |
| | Forcing a vShield to Synchronize with the vShield Manager | 38 |
| | Restarting a vShield | 38 |
| | Viewing Traffic Statistics by vShield Port | 38 |
| | Downloading the Firewall Logs of a vShield | 39 |
| | Powering off vShield Zones Virtual Machines | 39 |
| 10 | Firewall Management | 41 |
| | Configuring Firewall Settings Using VM Wall | 41 |
| | Default Rules | 41 |
| | Layer 4 Rules and Layer 2/Layer 3 Rules | 41 |
| | Hierarchy of VM Wall Rules | 42 |
| | Planning VM Wall Rule Enforcement | 42 |
| | Creating a Layer 4 Firewall Rule | 42 |
| | Creating a Layer 2/Layer 3 Firewall Rule | 43 |
| | Reverting to a Previous VM Wall Configuration | 44 |
| | Deleting a VM Wall Rule | 44 |
| 11 | Traffic Analysis | 45 |
| | Reading the VM Flow Charts | 45 |
| | Viewing a Specific Application in the VM Flow Charts | 46 |
| | Changing the Date Range of the VM Flow Charts | 46 |
| | Viewing the VM Flow Report | 46 |
| | Adding VM Wall Rules from the VM Flow Report | 47 |
| | Deleting All Recorded Flows | 47 |
| | Editing Port Mappings | 48 |
| | Adding an Application-Port Pair Mapping | 48 |
| | Deleting an Application-Port Pair Mapping | 49 |
| | Hiding the Port Mappings Table | 49 |

| | | |
|-----------|---|-----------|
| 12 | Virtual Machine Discovery and Inventory | 51 |
| | Reading the Discovery Results Table | 51 |
| | Enabling Continuous Discovery | 52 |
| | Running an On-Demand Discovery of Virtual Machines | 52 |
| | Scheduling Periodic Discovery of Virtual Machines | 53 |
| | Terminating an In-Progress Discovery | 53 |
| | Stopping a Scheduled Discovery Scan | 54 |
| | Using VM Inventory to View Virtual Machine Details | 54 |
| 13 | Command Line Interface | 55 |
| | Logging In and Out of the CLI | 55 |
| | CLI Command Modes | 55 |
| | CLI Syntax | 56 |
| | Moving Around in the CLI | 56 |
| | Getting Help within the CLI | 56 |
| | CLI Command Reference | 57 |
| | Appendix: Using VMotion with vShield Zones | 63 |
| | Preventing VMotion from Moving vShield Zones Virtual Appliances | 63 |
| | Permitting VMotion to Move Protected Virtual Machines | 64 |
| | Index | 65 |

About This Book

This manual, the *vShield Zones Administration Guide*, describes how to install, configure, monitor, and maintain the VMware vShield Zones system by using the vShield Manager user interface 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 Zones 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, including VMware ESX 4.0, vCenter Server, 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.

vShield Zones Documentation

The following documents comprise the vShield Zones documentation set:

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

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>.

Overview of vShield Zones

vShield Zones is an application-aware firewall built for VMware® vCenter Server integration. vShield Zones inspects client-server communications and inter-virtual-machine communication to provide detailed traffic analytics and application-aware firewall protection. vShield Zones is a critical security component for protecting virtualized datacenters from attacks and misuse helping you achieve your compliance-mandated goals.

This guide assumes you have administrator access to the entire vShield Zones system. The viewable resources in the vShield Manager user interface can differ based on the assigned role and rights of a user. If you are unable to access a screen or perform a particular task, consult your vShield Zones administrator.

vShield Zones Components

vShield Zones includes components and services essential for protecting virtual machines. vShield Zones can be configured through a web-based user interface and a command line interface (CLI).

To run vShield Zones, you need one vShield Manager virtual machine and at least one vShield virtual machine.

vShield Manager

The vShield Manager is the centralized network management component of vShield Zones and is installed as a virtual machine by using the vSphere Client. Using the vShield Manager user interface, administrators install, configure, and maintain vShield instances. A vShield Manager can run on a different ESX host from your vShield instances and still control many vShield instances across other ESX hosts. The vShield Manager leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel.

You can connect to the vShield Manager using one of the following supported Web browsers:

- Internet Explorer 5.x and later
- Mozilla Firefox 1.x and later
- Safari 1.x or 2.x

For more on the using the vShield Manager user interface, see [Chapter 2, “vShield Manager User Interface Basics,”](#) on page 11.

vShield

The vShield is the active security component, inspecting traffic and providing firewall protection. You can install a vShield instance on a vSwitch that homes a physical NIC. As an ESX host can have multiple vSwitches and physical NICs, you can install multiple vShield instances on a single ESX host. Each installed vShield instance monitors all incoming and outgoing traffic on the host vSwitch. As traffic passes through a vShield, a process called discovery inspects session headers to catalog the data. Discovery creates a profile for each virtual machine detailing the operating system, applications, ports, and protocols used in network communication. Based on this information, the vShield allows ephemeral port usage by permitting dynamic protocols such as FTP and RPC to pass through while maintaining lockdown on ports 1024 and higher.

Each vShield provides rich traffic statistics, which you can use to create firewall allow and deny rules to regulate access in and out of your virtual network. Traffic statistics can also be used for network troubleshooting, such as detecting high or low traffic usage by an application, server, or client.

Using the vSphere Client, you install the vShield software as a template. The template allows you to install multiple vShield instances from the vShield Manager into your vCenter environment.

vShield Manager User Interface Basics

2

The vShield Manager user interface offers configuration and data viewing options specific to vShield Zones use. By utilizing the VMware Infrastructure SDK, the vShield Manager displays your vSphere Client inventory panel for a complete view of your vCenter environment.

The chapter includes the following topics:

- [“Logging in to the vShield Manager”](#) on page 11
- [“Accessing the Online Help”](#) on page 11
- [“vShield Manager User Interface”](#) on page 12

Logging in to the vShield Manager

You access the vShield Manager management interface by using a Web browser.

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**.
You should change the default password as one of your first tasks to prevent unauthorized use. See [“Editing a User Account”](#) on page 22.
- 4 Click **Log In**.

Accessing the Online Help

The Online Help can be accessed by clicking  in the upper right of the vShield Manager.

vShield Manager User Interface

The vShield Manager user interface is divided into two panels: the inventory panel and the configuration panel. You select a resource from the inventory panel to open the available details and configuration options in the configuration panel.

vShield Manager Inventory Panel






The vShield Manager inventory panel hierarchy mimics the vSphere Client inventory hierarchy. Resources include the root folder, datacenters, clusters, port groups, ESX hosts, and virtual machines, including your installed vShield instances. As a result, the vShield Manager maintains solidarity with your vCenter Server inventory to present a complete view of your virtual deployment. The vShield Manager is the only virtual machine that does not appear in the vShield Manager inventory panel. vShield Manager settings are configured from the **Settings & Reports** resource atop the inventory panel.

The inventory panel offers two views: Hosts & Clusters and Networks. The Hosts & Clusters view displays the clusters, resource pools, and ESX hosts in your inventory. The Networks view displays the VLAN networks and port groups in your inventory. These views are consistent with the same views in the vSphere Client.


When clicked, each inventory object has a specific set of tabs that appear in the configuration panel.

There are differences in the icons for virtual machines and vShield instances between the vShield Manager and the vSphere Client inventory panels. Custom icons are used to show the difference between vShield instances and virtual machines, and the difference between protected and unprotected virtual machines.


Table 2-1. vShield and Virtual Machine Icons in the Inventory Panel

| Icon | Description |
|---|--|
|  | A powered on vShield in active protection state. |
|  | A powered off vShield. |
|  | A powered on virtual machine that is protected by a vShield. |
|  | A powered on virtual machine that is not protected by a vShield. |
|  | A virtual machine that is powered off. |

Refreshing the Inventory Panel

To refresh the list of resources in the inventory panel, click . The refresh action requests the latest resource information from the vCenter Server. By default, the vShield Manager requests resource information from the vCenter Server every five minutes.

Searching the Inventory Panel

To search the inventory panel for a specific resource, type a string in the field atop the vShield Manager inventory panel and click .

vShield Manager Configuration Panel

The vShield Manager configuration panel presents the settings that can be configured based on the selected inventory resource and the output of vShield Zones operation. Each resource offers multiple tabs, each tab presenting information or configuration forms corresponding to the resource.

Because each resource has a different purpose, some tabs are specific to certain resources. Also, some tabs have a second level of options.

Management System Settings

The vShield Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

The chapter includes the following topics:

- [“Identifying Your vCenter Server”](#) on page 13
- [“Identifying DNS Services”](#) on page 14
- [“Setting the vShield Manager Date and Time”](#) on page 14
- [“Identifying a Proxy Server”](#) on page 14
- [“Downloading a Technical Support Log from a Component”](#) on page 15
- [“Viewing vShield Manager System Status”](#) on page 15
- [“Installing a vShield Manually”](#) on page 15
- [“Registering the vShield Manager as a vSphere Client Plug-in”](#) on page 16

Identifying Your vCenter Server

After installing the vShield Manager as a virtual machine, log in to the vShield Manager user interface to connect to your vCenter Server. This enables the vShield Manager to display your VMware Infrastructure inventory.

To identify your vCenter Server from the vShield Manager

- 1 Log in to the vShield Manager.

Upon initial login, the vShield Manager opens to the **Configuration > vCenter** tab. If you have previously configured the **vCenter** tab form, perform the following steps:

- a Click the **Settings & Reports** from the vShield Manager inventory panel.
- b Click the **Configuration** tab.

The **vCenter** screen appears.

- 2 Type the IP address of your vCenter Server in the **IP address/Name** field.
- 3 Type your vSphere Client login user name in the **User Name** field.
This user account must have administrator access.
- 4 Type the password associated with the user name in the **Password** field.
- 5 Click **Commit**.

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.

Identifying DNS Services

You can specify up to three DNS servers that the vShield Manager can use for IP address and host name resolution. As all of the IP addresses and hostnames are generally not available on one DNS server, identifying a second or third DNS server provides the best coverage.

To identify a DNS server

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **DNS**.
- 4 Type an IP address in **Primary DNS IP Address** to identify the primary DNS server.
This server is checked first for all resolution requests.
- 5 (Optional) Type an IP address in the **Secondary DNS IP Address** field.
- 6 (Optional) Type an IP address in the **Tertiary DNS IP Address** field.
- 7 Click **Save**.

Setting the vShield Manager Date and Time

You can set the date, time, and time zone of the vShield Manager. You can also specify a connection to an NTP server to establish a common network time. Date and time values are used in the system to stamp events as they occur.

To set the date and time configuration of the vShield Manager

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Date/Time**.
- 4 In the **Date and Clock** field, type the date and time in the format YYYY-MM-DD HH:MM:SS.
- 5 In the **NTP Server** field, type the IP address of your NTP server.
- 6 From the **Time Zone** drop-down menu, select the appropriate time zone.
- 7 Click **Save**.

Identifying a Proxy Server

If you use a proxy server for network connectivity, you can configure the vShield Manager to use the proxy server. The vShield Manager supports application-level HTTP/HTTPS proxies such as CacheFlow and Microsoft ISA Server.

To identify a proxy server

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **HTTP Proxy**.
- 4 From the **Use Proxy** drop-down menu, select **Yes**.
- 5 (Optional) Type the host name of the proxy server in the **Proxy Host Name** field.

- 6 Type the IP address of the proxy server in the **Proxy IP Address** field.
- 7 Type the connecting port number on your proxy server in the **Proxy Port** field.
- 8 Type the **User Name** required to log in to the proxy server.
- 9 Type the **Password** associated with the user name for proxy server login.
- 10 Click **Save**.

Downloading a Technical Support Log from a Component

You can use the **Support** option to download the system log from a vShield Zones component to your PC. A system log can be used to troubleshoot operational issues.

To download a vShield Zones component system log

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Support**.
- 4 Under **Tech Support Log Download**, click **Initiate** next to the appropriate component.
Once initiated, the log is generated and uploaded to the vShield Manager. This might take several seconds.
- 5 After the log is ready, click the **Download** link to download the log to your PC.
The log is compressed and has the proprietary file extension **.blsl**. You can open the log using a decompression utility by browsing for **All Files** in the directory where you saved the file.

Backing Up vShield Manager Data

You can use the **Backups** option to back up vShield Manager data. See [“Backing Up vShield Manager Data”](#) on page 17.

Viewing vShield Manager System Status

The **Status** tab displays the status of vShield Manager system resource utilization, and includes the software version details, license status, and serial number. The serial number must be registered with technical support for update and support purposes.

To view the system status of the vShield Manager

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Status**.
- 4 (Optional) Click **Version Status** to review the current version of system software running on your vShield Zones components.

The **Update Status** tab appears. See [“Viewing Current System Software”](#) on page 19.

Installing a vShield Manually

You can use the **Manual Install** option to install a vShield in a vNetwork Distributed Switch environment. See [“Installing a vShield Manually on a vNetwork Distributed Switch”](#) on page 32.

Registering the vShield Manager as a vSphere Client Plug-in

The **vSphere Plug-in** option lets you register the vShield Manager as a vSphere Client plug-in. After the plug-in is registered, you can open the vShield Manager user interface from the vSphere Client.

To register the vShield Manager as a vSphere Client plug-in

- 1 If you are logged in to the vSphere Client, log out.
- 2 Log in to the vShield Manager.
- 3 Click **Settings & Reports** from the vShield Manager inventory panel.
- 4 Click the **Configuration** tab.
- 5 Click **vSphere Plug-in**.
- 6 Click **Register**.
- 7 Log in to the vSphere Client.
Verify that **vShield** appears as a vSphere Client option.
- 8 Click **vShield** to connect to the vShield Manager.
The vShield Manager login screen appears in the vSphere Client window.

Backing Up vShield Manager Data

You can back up and restore your vShield Manager data, which can include system configuration, events, and audit log tables. Configuration tables are included in every backup. You can, however, exclude system and audit log events. Backups are saved to a remote location that must be accessible by the vShield Manager.

Backups can be executed according to a schedule or on demand.

This chapter includes the following topics:

- [“Backing Up Your vShield Manager Data on Demand”](#) on page 17
- [“Scheduling a Backup of vShield Manager Data”](#) on page 18
- [“Restoring a Backup”](#) on page 18

Backing Up Your vShield Manager Data on Demand

You can back up vShield Manager data at any time by performing an on-demand backup.

To back up the vShield Manager database

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Backups**.
- 4 (Optional) Select the **Exclude System Events** check box if you do not want to back up system event tables.
- 5 (Optional) Select the **Exclude Audit Logs** check box if you do not want to back up audit log tables.
- 6 Type the **Host IP Address** of the system where the backup will be saved.
- 7 (Optional) Type the **Host Name** of the backup system.
- 8 Type the **User Name** required to log in to the backup system.
- 9 Type the **Password** associated with the user name for the backup system.
- 10 In the **Backup Directory** field, type the absolute path where backups are to be stored.
- 11 Type a text string in **Filename Prefix**.

This text is prepended to the 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**.
- 12 From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**.
- 13 Click **Backup**.

Once complete, the backup appears in a table below this form.
- 14 Click **Save Settings** to save the configuration.

Scheduling 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.

To schedule periodic backups of your vShield Manager data

- 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**.

Restoring a Backup

To restore an available backup, the **Host IP Address**, **User Name**, **Password**, and **Backup Directory** fields in the **Backups** screen must have values that identify the location of the backup to be restored. When you restore a backup, the current configuration is overridden. If the backup file contains system event and audit log data, that data is also restored.

IMPORTANT Back up your current data before restoring a backup file.

To restore an available vShield Manager backup

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Backups**.
- 4 Click **View Backups** to view all available backups saved to the backup server.
- 5 Select the check box for the backup to restore.
- 6 Click **Restore**.
- 7 Click **OK** to confirm.

Updating the System Software

vShield Zones software requires periodic updates to maintain system performance. Using the **Updates** tab options, you can install and track system updates.

This chapter includes the following topics:

- [“Viewing Current System Software”](#) on page 19
- [“Uploading an Update”](#) on page 19
- [“Reviewing the Update History”](#) on page 20

Viewing Current System Software

The current versions of vShield Zones component software display under the **Update Status** tab.

To view the current system software

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Updates** tab.
- 3 Click **Update Status**.

Uploading an Update

vShield Zones updates are available as offline updates. When an update is made available, you can download the update to your PC, and then upload the update by using the vShield Manager user interface.

When the update is uploaded, the vShield Manager is updated first, after which, all vShield instances are updated. If a reboot of either the vShield Manager or a vShield is required, the **Update Status** screen prompts you to reboot the component. In the event that both the vShield Manager and all vShield instances must be rebooted, you must reboot the vShield Manager first, and then reboot the vShield instances.

To upload an update

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Updates** tab.
- 3 Click **Upload Settings**.
- 4 Click **Browse** to locate the update.
- 5 After locating the file, click **Upload File**.

- 6 Click **Confirm Install** to confirm update installation.

There are two tables on this screen. During installation, you can view the top table for the description, start time, success state, and process state of the current update. View the bottom table for the update status of each vShield. All vShield instances have been upgraded when the status of the last vShield is displayed as Finished.

- 7 After the vShield Manager reboots, click the **Update Status** tab.
- 8 Click **Reboot Manager** if prompted.
- 9 Click **Finish Install** to complete the system update.
- 10 Click **Confirm**.

Reviewing the Update History

The **Update History** tab lists the updates that have already been installed, including the installation date and a brief description of each update.

To view a history of installed updates

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Updates** tab.
- 3 Click **Update History**.

User Management

Security operations are often managed by multiple individuals. Management of the overall system is delegated to different personnel according to some logical categorization. However, permission to carry out tasks is limited only to users with appropriate rights to specific resources. From the Users section, you can delegate such resource management to users by granting applicable rights.

User management in the vShield Manager user interface is separate from user management in the CLI of any vShield Zones component.

This chapter includes the following topics:

- [“Managing User Rights”](#) on page 21
- [“Adding a User”](#) on page 22
- [“Assigning a Role and Rights to a User”](#) on page 22
- [“Editing a User Account”](#) on page 22
- [“Deleting a User Account”](#) on page 23

Managing User Rights

Within the vShield Manager user interface, a user’s rights define the actions the user is allowed to perform on a given resource. Rights determine the user’s authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. This allows domain control over specific resources, or system-wide control if your right encompasses the System resource.

The following rules are enforced:

- A user can only have one right to one resource.
- A user cannot add to or remove assigned rights and resources.

Table 6-1. vShield Manager User Rights

| Right | Description |
|-------|----------------|
| R | Read only |
| CRUD | Read and Write |

Table 6-2. vShield Manager User Resources

| Resource | Description |
|----------|---------------------------------------|
| System | Access to entire vShield Zones system |
| Firewall | Access to the VM Wall component only |
| None | Access to no resources |

Managing the Default User Account

The vShield Manager user interface includes one default user account, user name **admin**, which has rights to all resources. You cannot edit the rights of or delete this user. The default password for admin is **default**.

Change the password for this account upon initial login to the vShield Manager. See [“Editing a User Account”](#) on page 22.

Adding a User

Basic user account creation requires assigning the user a login name and password.

To create a new user account

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Users** tab.
- 3 Click **Create User**.

The New User screen opens.

- 4 Type a **User Name**.

This is used for login to the vShield Manager user interface. This user name and associated password cannot be used to access the vShield or vShield Manager CLIs.

- 5 (Optional) Type the user's **Full Name** for identification purposes.
- 6 (Optional) Type an **Email Address**.
- 7 Type a **Password** for login.
- 8 Re-type the password in the **Retype Password** field.
- 9 Click **OK**.

After account creation, you configure right and resource assignment separately.

Assigning a Role and Rights to a User

After creating a user account, you can assign the user a role and rights to system resources. The role defines the resource, and the right defines the user's access to that resource.

To assign a role and right to a user

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Users** tab.
- 3 Double-click the **User Role** cell for the user.
- 4 From the drop-down menu that opens, select an available resource.
- 5 Double-click the **Access Right** cell for the resource.
- 6 From the drop-down menu that opens, select an available right.

Editing a User Account

You can edit a user account to change the password.

To edit an existing user account

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Users** tab.
- 3 Click a cell in the table row that identifies the user account.

4 Click **Update User**.

5 Make changes as necessary.

If you are changing the password, confirm the password by typing it a second time in the **Retype Password** field.

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

Deleting a User Account

You can delete any created user account. You cannot delete the **admin** account. Audit records for deleted users are maintained in the database and can be referenced in an Audit Log report.

To delete a user account

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

2 Click the **Users** tab.

3 Click a cell in the table row that identifies the user account.

4 Click **Delete User**.

System Events

System events are events that are related to vShield operation. They are raised to detail every operational event, such as a vShield reboot or a break in communication between a vShield and the vShield Manager. Events might relate to basic operation (Informational) or to a critical error in vShield operation (Critical).

This chapter includes the following topics:

- [“Viewing the System Event Report”](#) on page 25
- [“System Event Notifications”](#) on page 26
- [“Syslog Format”](#) on page 27

Viewing the System Event Report

The vShield Manager aggregates system events into a report that can be filtered by vShield and event severity.

To view the System Event report

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **System Events** tab.
- 3 (Optional) Select one or more vShield instances from the **vShield** field.
All vShield instances are selected by default.
- 4 From the **and Severity** drop-down menu, select a severity by which to filter results.
All severities are included by default. You can select one or more severities at a time.
- 5 Click **View Report**.
- 6 In the report output, click an **Event Time** link to view details about a specific event.

System Event Notifications

vShield Manager Virtual Appliance Events

| | Power Off | Power On | Interface Down | Interface Up |
|------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| Local CLI | Run show log follow command. | Run show log follow command. | Run show log follow command. | Run show log follow command. |
| GUI | NA | NA | NA | NA |

| | CPU | Memory | Storage |
|------------------|---|---|---|
| Local CLI | Run show process monitor command. | Run show system memory command. | Run show filesystem command. |
| GUI | See “Viewing vShield Manager System Status” on page 15. | See “Viewing vShield Manager System Status” on page 15. | See “Viewing vShield Manager System Status” on page 15. |

vShield Virtual Appliance Events

| | Power Off | Power On | Interface Down | Interface Up |
|------------------|--|--|---|---|
| Local CLI | Run show log follow command. | Run show log follow command. | Run show log follow command. | Run show log follow command. |
| Syslog | NA | See “Syslog Format” on page 27. | e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex. For scripting on the syslog server, search for NIC Link is . | e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex. For scripting on the syslog server, search for NIC Link is . |
| GUI | “Heartbeat failure” event in System Event log. See “Viewing the System Event Report” on page 25. | See “Viewing the Current System Status of a vShield” on page 38. | See “Viewing the Current System Status of a vShield” on page 38. | See “Viewing the Current System Status of a vShield” on page 38. |

| | CPU | Memory | Storage | Session reset due to DoS, inactivity, or data timeouts |
|------------------|--|--|--|--|
| Local CLI | Run show process monitor command. | Run show system memory command. | Run show filesystem command. | Run show log follow command. |
| Syslog | NA | NA | NA | See “Syslog Format” on page 27. |
| GUI | See “Viewing the Current System Status of a vShield” on page 38. | See “Viewing the Current System Status of a vShield” on page 38. | See “Viewing the Current System Status of a vShield” on page 38. | Refer to the System Event Log. See “Viewing the System Event Report” on page 25. |

Syslog Format

The system event message logged in the syslog has the following structure:

```

syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter '::' (double colons)
Each name/value pair separated by delimiter ';;' (double semi-colons)

```

The fields and types of the system event are:

```

Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer (possible values: 10007 10016 10043 20019)
Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)
Message ::

```


Viewing the Audit Log

The **Audit Logs** tab provides a view into the actions performed by all vShield Manager users. The vShield Manager retains audit log data for one year, after which time the data is discarded.

To view the Audit Log

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Audit Logs** tab.
- 3 Narrow the output by clicking one or more of the following column filters:

| Column | Description |
|----------------|---|
| User Name | Select the login name of a user who performed the action. |
| Module | Select the vShield Zones resource on which action was performed. |
| Operation | Select the type of action performed. |
| Status | Select the result of action as either Success or Failure. |
| Operation Span | Select the vShield Zones component on which the action was performed. Local refers to the vShield Manager. |

vShield Management

A vShield monitors the traffic on your virtual network by tracking the details and statistics of each session. Each vShield must be added to your vShield Manager to be configured and monitored.

This chapter includes the following topics:

- [“Installing a vShield”](#) on page 31
- [“Uninstalling a vShield”](#) on page 36
- [“Sending vShield System Events to a Syslog Server”](#) on page 37
- [“Backing Up the Running CLI Configuration of a vShield”](#) on page 37
- [“Viewing the Current System Status of a vShield”](#) on page 38
- [“Powering off vShield Zones Virtual Machines”](#) on page 39

Installing a vShield

Installing a vShield enables you to add a vShield to the vCenter Server inventory and manage the vShield configuration from the vShield Manager. vShield addition requires naming the vShield instance and specifying an IP address for the vShield management port.

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

There are two methods for installing a vShield.

- [“Installing a vShield Using the vShield Template”](#) on page 31
- [“Installing a vShield Manually on a vNetwork Distributed Switch”](#) on page 32

Installing a vShield Using the vShield Template

This procedure assumes you have established a vShield template as detailed in the *vShield Zones Quick Start Guide*.

To add a vShield to the vShield Manager using the vShield template

- 1 Log in to the vShield Manager.
- 2 Click the ESX host to protect from the inventory panel.
- 3 Click the **Install vShield** tab.
- 4 Click **Configure Install Parameters**.

The Select/Clone a Virtual Shield to Install screen appears.

- 5 Complete the form:

| Field | Action |
|--|---|
| Select from available vShields | Leave this field blank. |
| Select template to clone | From this drop-down menu, select the vShield template. |
| Select a datastore to place clone | From this drop-down menu, select the datastore on which to store the vShield virtual machine data. |
| Enter a name for the clone | Type a unique name for the vShield. 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's management port. |
| Specify IP Mask for vShield | Type the IP subnet mask associated with the assigned IP address in A.B.C.D (255.255.255.0) format. |
| 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 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 and the vShield Manager. Keys are not shared across the network. |
| Select a vSwitch to shield | From this drop-down menu, select the vSwitch to protect. The vSwitches eligible for protection are highlighted in green in the accompanying table. |

- 6 Click **Continue** (located above the form).

The summary page displays before and after illustrations of vShield installation on the ESX host.

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

- 7 Click **Install**.

You can follow vShield installation steps from the Recent Tasks status pane located at the bottom of the vSphere Client window.

- 8 After installation is complete, open the vSphere Client.

- 9 Locate the vShield in your inventory.

The vShield virtual machine is already powered on.

- 10 If VMotion is enabled, disable VMotion for the vShield virtual machine.

See [“Appendix: Using VMotion with vShield Zones”](#) on page 63.

- 11 Ensure continuous discovery is enabled. See [“Enabling Continuous Discovery”](#) on page 52.

Installing a vShield Manually on a vNetwork Distributed Switch

For vNetwork Distributed Switch environments, you must install a vShield manually. Manual vShield installation requires the creation of a second vNetwork Distributed Switch and two distributed virtual port (dvPort) groups. Once you create these items, you install the vShield and move the virtual machines to the second vNetwork Distributed Switch for protection.

The following overview describes the manual installation process. The overview assumes you have deployed a vNetwork Distributed Switch with at least one attached NIC, and an uplink port group.

- 1 Create a second vNetwork Distributed Switch, called vNDS-2 in this scenario. Keep all vNICs on the original vNetwork Distributed Switch, vNDS-1. Add ESX hosts to vNDS-2, but do not connect any vNICs.
- 2 Create two dvPort groups: Protected and Unprotected.

- 3 Install the vShield, connecting the vShield network adapters to the Protected and Unprotected dvPort groups. You must also connect the management interface of the vShield to a port group that is reachable from the vShield Manager.
- 4 Move the virtual machine vNICs from vNDS-1 to vNDS-2.

Create a Second vNetwork Distributed Switch

Use the Create vNetwork Distributed Switch wizard to create a second vNetwork Distributed Switch.

To create the second vNetwork Distributed Switch

- 1 Log in to the vSphere Client and select the cluster from the inventory panel where your existing vNetwork Distributed Switch resides.
- 2 From the **Getting Started** tab, click **Add a vNetwork Distributed Switch** under Basic Tasks.
The Create vNetwork Distributed Switch wizard appears.
- 3 In the **Name** field, enter a name for the new vNetwork Distributed Switch.
- 4 For **Number of Uplink Ports**, select **1** and click **Next**.
- 5 Select **Add now** and select the check box for each ESX host in the list.
Do not select any physical adapters.
- 6 Click **Next**.
A warning appears to verify your decision to not include any physical adapters. Click **Yes**.
- 7 Click **Finish**.

Create the Protected dvPort Group

Use the Create Distributed Virtual Port Group wizard to add the protected dvPort group.

IMPORTANT Do not add virtual machines to the protected dvPort group. This port group is configured with promiscuous mode turned on, which allows the vShield to see all passing traffic.

To create the Protected dvPort group

- 1 Log in to the vSphere Client and select vNDS-2 from the inventory panel.
- 2 From the **Getting Started** tab, click **Create a new port group**.
The Create Distributed Virtual Port Group wizard appears.
- 3 In the **Name** field, enter a name for the dvport group.
Include a string such as **protected** or **prot** in the name for quick identification.
- 4 (Optional) To identify only specific VLAN IDs to pass through:
 - a For the **VLAN type** field, select **VLAN Trunking**.
The **VLAN Trunk Range** field appears.
 - b In the **VLAN Trunk Range** field, type the VLAN IDs you want to route.
- 5 Click **Next** and then click **Finish**.
- 6 After the protected port group has been created, right-click the port group from the inventory panel and select **Edit Settings**.
- 7 In the dvPortGroup Settings dialog box, click **Security** under **Policies**.
- 8 Select **Accept** from the **Promiscuous Mode** drop-down list.
- 9 Click **OK**.

Create the Unprotected dvPort Group

Use the Create Distributed Virtual Port Group wizard to add the unprotected dvPort group.

IMPORTANT Do not add virtual machines to the unprotected dvPort group. This port group is configured with promiscuous mode turned on, which allows the vShield to see all passing traffic.

To create the Unprotected dvPort group

- 1 Log in to the vSphere Client and select vNDS-1 from the inventory panel.
- 2 From the **Getting Started** tab, click **Create a new port group**.
The Create Distributed Virtual Port Group wizard appears.
- 3 In the **Name** field, enter a name for the dvPort group.
Include a string such as **unprotected** or **unprot** in the name for quick identification.
- 4 (Optional) To identify only specific VLAN IDs to pass through:
 - a For the **VLAN type** field, select **VLAN Trunking**.
The **VLAN Trunk Range** field appears.
 - b In the **VLAN Trunk Range** field, type the VLAN IDs you want to route.
- 5 Click **Next** and then click **Finish**.
- 6 After the protected port group has been created, right-click the port group from the inventory panel and select **Edit Settings**.
- 7 In the dvPortGroup Settings dialog box, click **Security** under **Policies**.
- 8 Select **Accept** from the **Promiscuous Mode** drop-down list.
- 9 Click **OK**.

Install the vShield

Manual vShield installation requires a vShield image, running the **setup** command in the CLI, and adding the vShield to the vShield Manager using the **Manual Install** option. You must install the vShield using the vSphere Client before adding the vShield to the vShield Manager user interface.

To add a vShield manually

- 1 Log in to the vSphere Client and select an ESX host from the inventory panel.
- 2 Go to **File > Deploy OVF Template**.
The Deploy OVF Template wizard opens.
- 3 Click **Deploy from file** and click **Browse** to locate the folder on your client machine containing the vShield OVF file.
- 4 Complete the wizard.
The vShield is installed into your inventory.
- 5 After installation completes, select the vShield from the inventory panel and select the **Console** tab.
The booting process might take a couple of minutes.
- 6 After the `localhost login` prompt appears, log in to the CLI by using the username **admin** and the password **default**.

- 7 Run the **setup** command to launch the CLI setup wizard.

The CLI setup wizard guides you through IP address assignment for the management interface of the vShield and identification of the default gateway IP address. The management interface IP address of the vShield must be reachable by the vShield Manager.

```
vShield> setup
```

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

```
Hostname [vShield]:
Manager key [bluelane]:
IP Address:
Default gateway:
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.

- 8 Ping the default gateway to verify network connectivity.

```
vShield> ping 10.115.219.253
```

- 9 Open a Web browser and log in to the vShield Manager.

- 10 Click **Settings & Reports** from the inventory panel.

- 11 Click the **Configuration** tab.

- 12 Click **Manual Install**.

- 13 Click **Add**.

- 14 Complete the form:

| Field | Action |
|----------------------------|--|
| Name | Type the name you entered for the vShield when you deployed the OVF in the vSphere Client. |
| IP Address | Type the IP address assigned to the vShield. |
| Location | Type a description of where the vShield instance resides. |
| Key | Type the Manager key value entered using the CLI setup command. The default key is bluelane . |
| Clustering Settings | <ul style="list-style-type: none"> ■ Select Standalone to add a vShield instance that is not within a cluster. ■ From the Add to Cluster drop-down menu, select the cluster wherein the vShield was installed. |

- 15 Click **Ok** (located above the form).

You can follow the vShield installation steps from the **Recent Tasks** status pane located at the bottom of the vSphere Client window.

Assign the vShield Interfaces to Port Groups

You must edit the virtual machine settings of the installed vShield to assign the vShield interfaces to port groups. The vShield management interface must be in a port group that is reachable from the vShield Manager. This can be a basic port group or a dvPort group. You can create a new port group or assign the management interface to an existing port group.

To assign the vShield interfaces to port groups

- 1 Log in to the vSphere Client.
- 2 Right-click the vShield virtual machine and click **Edit Settings**.

3 Click **Network adapter 1**.

This is the management interface of the vShield. Assign a network label that is reachable from the vShield Manager.

4 Click **Network adapter 2** and perform the following steps:

- a Verify the **Device Status** settings for Network adapter 2 to ensure that the **Connected** and **Connect at Power on** check boxes are selected.
- b Under Network Connection, select the protected dvPort group from the **Network Label** drop-down list.

5 Click **Network adapter 3** and perform the following steps:

- a Verify the **Device Status** settings for Network adapter 3 to ensure that the **Connected** and **Connect at Power on** check boxes are selected.
- b Under Network Connection, select unprotected dvPort group from the **Network Label** drop-down list.

6 Click **Ok**.

Move the Virtual Machines from vNDS-1 to vNDS-2

After the vShield has been installed and connected, move the virtual machines from vNDS-1 to vNDS-2. You must create a new dvPort group on vNDS-2 for the virtual machines. Once you move the virtual machines, delete the empty dvPort group from vNDS-1.

You cannot have two dvPort groups with the same name at any given time. If you want to keep the name of the dvPort group from vNDS-1, you must move the virtual machines to a temporary vNetwork Distributed Switch and then re-create the dvPort group on vNDS-2.

To maintain the name of the dvPort group from vNDS-1 when you move the virtual machines to vNDS-2

- 1 Create a temporary dvPort group on vNDS-2.
- 2 Move the virtual machine VNICS from vNDS-1 to the temporary dvPort group on vNDS-2.
- 3 Delete the original dvPort group from vNDS-1.
- 4 Create a dvPort group on vNDS-2 with the same name as the original dvPort group.
- 5 Move the virtual machine vNICs from the temporary dvPort group to the new dvPort group.
- 6 Delete the temporary dvPort group.

Uninstalling a vShield

Uninstalling a vShield instance removes the vShield from the network. There are two methods for installing a vShield.

- [“Uninstalling a Template-Based vShield”](#) on page 36
- [“Uninstalling a Manually Installed vShield”](#) on page 37

Uninstalling a Template-Based vShield

After addition to the vShield Manager, each template-based vShield instance has an **Uninstall vShield** tab.

To uninstall a template-based vShield

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Uninstall vShield** tab.

The Uninstall vShield screen displays the process the system will follow to uninstall the vShield from your virtual network.

- 3 Click **Uninstall**.

The vShield is uninstalled.

Uninstalling a Manually Installed vShield

A manually installed vShield instance must be uninstalled manually.

To uninstall a manually installed vShield

- 1 Log in to the vSphere Client.
- 2 Move the virtual machine vNICs from vNDS-2 to vNDS-1.
- 3 Log in to the vShield Manager.
- 4 Click the root folder from the inventory panel.
- 5 Click the **Configuration** tab.
- 6 Click **Manual Install**.
- 7 Select the check box for the vShield.
- 8 Click **Remove**.
- 9 Click **Ok** in the pop-up window.
The vShield is uninstalled.
- 10 In the vSphere Client, remove the protected and unprotected dvPort groups and the second vNetwork Distributed Switch.

Sending vShield System Events to a Syslog Server

You can send vShield events to a syslog server.

To send vShield system events to a syslog server

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Syslog Servers**.
- 4 Type the **IP Address** of the syslog server.
- 5 From the **Log Level** drop-down menu, select the event level at and above which to send vShield events to the syslog server.

For example, if you select **Emergency**, then only emergency-level events are sent to the syslog server. If you select **Critical**, then critical-, alert-, and emergency-level events are sent to the syslog server.
- 6 Click **Add** to save new settings. You send vShield events to up to five syslog instances.

Backing Up the Running CLI Configuration of a vShield

The **CLI Configuration** option displays the running configuration of the vShield. You can back up the running configuration to the vShield Manager to preserve the configuration.

To back up the running CLI configuration of a vShield

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **CLI Configuration**.
- 4 Click **Backup Configuration**.

The configuration is populated in the **Backup Configuration** field. You can cut and paste this text into the vShield CLI at the Configuration mode prompt.

Viewing the Current System Status of a vShield

The **System Status** option lets you view and influence the health of a vShield. Details include system statistics, status of ports, software version, and environmental variables.

To view the health of a vShield

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **System Status**.

From the System Status screen, you can perform the following actions:

- [“Forcing a vShield to Synchronize with the vShield Manager”](#) on page 38
- [“Restarting a vShield”](#) on page 38
- [“Viewing Traffic Statistics by vShield Port”](#) on page 38
- [“Downloading the Firewall Logs of a vShield”](#) on page 39

Forcing a vShield to Synchronize with the vShield Manager

The **Force Sync** option forces a vShield to re-synchronize with the vShield Manager. This might be necessary after a software upgrade.

To force a vShield to re-synchronize with the vShield Manager

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **System Status**.
- 4 Click **Force Sync**.

Restarting a vShield

You can restart a vShield to troubleshoot an operational issue.

To restart a vShield

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **System Status**.
- 4 Click **Restart**.
- 5 Click **OK** in the pop-up window to confirm reboot.

Viewing Traffic Statistics by vShield Port

You can view the traffic statistics for each vShield interface.

To view traffic statistics by vShield port

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **System Status**.

- 4 Click a port name to view traffic statistics for the port.

For example, to view the traffic statistics for the vShield management port, click **mgmt**.

Downloading the Firewall Logs of a vShield

You can download a log of the firewall activity from a vShield. The firewall log details the results of the firewall operation based on matching firewall rules against traffic.

To download and view the firewall log for a vShield

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **System Status**.
- 4 Under **VM Wall**, click **Show Logs**.

The vShield uploads the log to the vShield Manager.

- 5 To download the log from the vShield Manager to your PC, click **Download VM Wall Logs**.

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 Log in to the vSphere Client.
- 2 Select a vShield Zones virtual machine from the inventory panel.
- 3 Click the **Console** tab to open the vShield Zones CLI.
- 4 Log in to the CLI.
- 5 After logging in, type **enable** to enter Privileged mode.
- 6 Type **shutdown**.
- 7 After CLI shutdown is completed, right-click the virtual machine from the inventory panel and select **Power > Power Off**.

Firewall Management

The primary function of a vShield is to provide insight into the traffic on your virtual network by inspecting each session and returning details to the vShield Manager. Traffic details include sources, destinations, direction of sessions, applications, and ports being used. Traffic details can be used to create firewall allow or deny rules.

This chapter includes the following topics:

- [“Configuring Firewall Settings Using VM Wall”](#) on page 41
- [“Hierarchy of VM Wall Rules”](#) on page 42
- [“Planning VM Wall Rule Enforcement”](#) on page 42
- [“Creating a Layer 4 Firewall Rule”](#) on page 42
- [“Creating a Layer 2/Layer 3 Firewall Rule”](#) on page 43
- [“Reverting to a Previous VM Wall Configuration”](#) on page 44
- [“Deleting a VM Wall Rule”](#) on page 44

Configuring Firewall Settings Using VM Wall

VM Wall is a centralized, hierarchical firewall for virtual machine environments. You can manage VM Wall rules at the datacenter and cluster levels to provide a consistent set of rules across multiple vShield instances under these containers. As membership in these containers can change dynamically, VM Wall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, VM Wall effectively has a continuous footprint on each ESX host under the managed containers.

When creating VM Wall rules, you can create general rules based on incoming or outgoing traffic at the container level. For example, you can create a rule to deny any traffic from outside of a datacenter that targets a destination within the datacenter. You can create a rule to deny any incoming traffic that is not tagged with a VLAN ID.

Default Rules

By default, the VM Wall enforces a set of rules allowing traffic to pass through all vShield instances. These rules appear in the **Default Rules** section of the VM Wall table. The default rules cannot be deleted or added to. However, you can change the **Action** element of each rule from **Allow** to **Deny**.

Layer 4 Rules and Layer 2/Layer 3 Rules

The **VM Wall** tab offers two sets of configurable rules: L4 (Layer 4) rules and L2/L3 (Layer 2/Layer 3) rules. Layers refer to layers of the Open Systems Interconnection (OSI) Reference Model.

Layer 4 rules govern TCP and UDP transport of Layer 7, or application-specific, traffic. Layer 2/Layer 3 rules monitor traffic from ICMP, ARP, and other Layer 2 and Layer 3 protocols. You can configure Layer 2/Layer 3 rules at the datacenter level only. By default, all Layer 4 and Layer 2/Layer 3 traffic is allowed to pass.

Hierarchy of VM Wall Rules

Each vShield instance enforces VM Wall rules in top-to-bottom ordering. A vShield checks each traffic session against the top rule in the VM Wall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. In the VM Wall table, the rules are enforced in the following hierarchy:

- 1 **Data Center High Precedence Rules**
- 2 **Cluster Level Rules**
- 3 **Data Center Low Precedence Rules** (seen as **Rules below this level have lower precedence than cluster level rules** when a datacenter resource is selected)
- 4 **Default Rules**

VM Wall offers container-level and custom priority precedence configurations:

- Container-level precedence refers to recognizing the datacenter level as being higher in priority than the cluster level. When a rule is configured at the datacenter level, the rule is inherited by all clusters and vShield instances therein. A cluster-level rule is only applied to the vShield instances within the cluster.
- Custom priority precedence refers to the option of assigning high or low precedence to rules at the datacenter level. High precedence rules work as noted in the container-level precedence description. Low precedence rules include the Default Rules and the configuration of Data Center Low Precedence rules. This flexibility allows you to recognize multiple layers of applied precedence.

At the cluster level, you configure rules that apply to all vShield instances within the cluster. Because Data Center High Precedence Rules are above Cluster Level Rules, ensure your Cluster Level Rules are not in conflict with Data Center High Precedence Rules.

Planning VM Wall Rule Enforcement

Using VM Wall, you can configure allow and deny rules based on your network policy. The following examples represent two common firewall policies:

- Allow all traffic by default. You keep the default allow all rules and add deny rules based on VM Flow data or manual VM Wall configuration. In this scenario, if a session does not match any of the deny rules, the vShield allows the traffic to pass.
- Deny all traffic by default. You can change the **Action** status of the default rules from **Allow** to **Deny**, and add allow rules explicitly for specific systems and applications. In this scenario, if a session does not match any of the allow rules, the vShield drops the session before it reaches its destination. If you change all of the default rules to deny any traffic, the vShield drops all incoming and outgoing traffic.

Creating a Layer 4 Firewall Rule

Layer 4 firewall rules allow or deny traffic based on the following criteria:

| Criteria | Description |
|---------------------------------|---|
| Source (A.B.C.D/nm) | IP address with netmask from which the communication originated |
| Source Port | Port from which the communication originated |
| Destination (A.B.C.D/nm) | IP address with netmask which the communication is targeting |
| Destination Application | The application on the destination the source is targeting |
| Destination Port | Port which the communication is targeting |
| Protocol | Transport protocol used for communication |

To create a Layer 4 firewall rule

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Wall** tab.
- 3 If you are adding a rule at the datacenter level, click **L4 Rules**.
- 4 Click an existing row in the appropriate section of the table.
The available sections are based on the resource selected from the inventory panel.
- 5 Click **Add**.
A new row is added at the bottom of the section.
- 6 Double-click each cell in the new row to select the appropriate information.
You can type IP addresses in the **Source** and **Destination** fields, or select from the default direction-container options.
- 7 (Optional) With the new row selected, click **Up** to move the row up in priority.
- 8 (Optional) Select the **Log** check box to log all sessions matching this rule.
- 9 Click **Commit** to save the rule.

NOTE Layer 4 firewall rules can also be created from the VM Flow report. See [“Adding VM Wall Rules from the VM Flow Report”](#) on page 47.

Creating a Layer 2/Layer 3 Firewall Rule

The Layer 2/Layer 3 firewall enables configuration of allow or deny rules for common Data Link Layer and Network Layer requests, such as ICMP pings and traceroutes.

You can change the default Layer 2/Layer 3 rules from allow to deny based on your network security policy.

To create a Layer 2/Layer 3 firewall rule

- 1 Select a datacenter resource from the inventory panel.
- 2 Click the **VM Wall** tab.
- 3 Click **L2/L3 Rules**.
- 4 Click an existing row in the **Data Center Rules** section of the table.
- 5 Click **Add**.
A new row is added at the bottom of the Datacenter Rules section.
- 6 Double-click each cell in the new row to type or select the appropriate information.
- 7 (Optional) Select the **Log** check box to log all sessions matching this rule.
- 8 Click **Commit**.

NOTE Layer 2/Layer 3 firewall rules can also be created from the VM Flow report. See [“Adding VM Wall Rules from the VM Flow Report”](#) on page 47.

Reverting to a Previous VM Wall Configuration

The vShield Manager saves a snapshot of VM Wall settings each time you commit a new rule. Clicking **Commit** causes the vShield Manager to save the previous configuration with a timestamp before adding the new rule. These snapshots are available from the **Revert to Snapshot** drop-down menu.

To revert to a previous VM Wall configuration

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Wall** tab.
- 3 From the **Revert to Snapshot** drop-down menu, select a snapshot.

Snapshots are presented in the order of timestamps, with the most recent snapshot listed at the top.

View the snapshot configuration details. To return to the current configuration, select the - option from the **Revert to Snapshot** drop-down menu.

- 4 Click **Commit** to overwrite the current configuration with the snapshot configuration.

Deleting a VM Wall Rule

You can delete any VM Wall rule you have created. You cannot delete the any rules in the Default Rules section of the table.

To delete a VM Wall rule

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Wall** tab.
- 3 Click an existing row in the DataCenter Rules or Cluster Level Rules section of the table. The available sections are based on the resource selected from the inventory panel.
- 4 Click **Delete**.

Traffic Analysis

VM Flow is a traffic analysis tool that provides a detailed view of the traffic on your virtual network that passed through a vShield instance. The VM Flow output defines which machines are exchanging data and over which application. This data includes the number of sessions, packets, and bytes transmitted per session. VM Flow is useful as a forensic tool to detect rogue services and examine outbound sessions, and can be used to create VM Wall rules.

The vShield Manager maintains up to one million Layer 4 sessions and one million Layer2/Layer 3 sessions.

This chapter includes the following topics:

- [“Reading the VM Flow Charts”](#) on page 45
- [“Changing the Date Range of the VM Flow Charts”](#) on page 46
- [“Viewing the VM Flow Report”](#) on page 46
- [“Adding VM Wall Rules from the VM Flow Report”](#) on page 47
- [“Editing Port Mappings”](#) on page 48
- [“Deleting All Recorded Flows”](#) on page 47

Reading the VM Flow Charts

The **VM Flow** tab displays throughput statistics as returned by all of the active vShield instances within a datacenter, cluster, or folder container, or at the individual port-group or virtual-machine level. VM Flow displays traffic statistics in three charts:

- Sessions/hr: Total number of sessions per hour
- Server KBytes/hr: Number of outgoing kilobytes per hour
- Client /hr: Number of incoming kilobytes per hour

VM Flow organizes statistics by the application protocols used in client-server communications, with each color in a chart representing a different application protocol. This charting method enables you to track your server resources per application.

Traffic statistics display all inspected sessions within the time span specified. The last seven days of data are displayed by default.

Viewing a Specific Application in the VM Flow Charts

You can select a specific application to view in the charts by clicking the **Application** drop-down menu.

To view the data for a specific application in the VM Flow charts

- 1 Select a datacenter, cluster, folder, port group, or virtual machine instance from the inventory panel.
- 2 Click the **VM Flow** tab.
- 3 From the **Application** drop-down menu, select the application to view.

The VM Flow charts are refreshed to show data corresponding to the selected application.

Changing the Date Range of the VM Flow Charts

You can change the date range of the VM Flow charts for an historical view of traffic data.

To change the date range of the VM Flow chart

- 1 Select a datacenter, cluster, folder, port group, or virtual machine instance from the inventory panel.
- 2 Click the **VM Flow** tab.

The charts are updated to display the most current information for the last seven days. This might take several seconds.

- 3 In the **Start Date** field, type a new date.

This date represents the date furthest in the past on which to start the query.

- 4 Type a new date in the **End Date** field.

This represents the most recent date on which to stop the query.

- 5 Click **Update Chart**.

Viewing the VM Flow Report

The VM Flow report presents the traffic statistics in tabular format. The report supports drilling down into traffic statistics based on the following hierarchy:

- 1 Select the firewall action: Allowed or Blocked.
- 2 Select an L4 or L2/L3 protocol.
 - L4: TCP or UDP
 - L2/L3: ICMP, Other-IPv4, or ARP
- 3 If an L2/L3 protocol was selected, select an L2/L3 protocol or message type.
- 4 Select the traffic direction: Incoming, Outgoing, or Intra (between virtual machines).
- 5 Select the port type: Categorized (standardized ports) or Uncategorized (non-standardized ports).
- 6 Select an application protocol or port.
- 7 Select a destination IP address.
- 8 Source a source IP address.

At the source IP address level, you can create a VM Wall rule based on the specific source and destination IP addresses.

To view the VM Flow report

- 1 Select a datacenter, cluster, folder, port group, or virtual machine instance from the inventory panel.
- 2 Click the **VM Flow** tab.
The charts update to display the most current information for the last seven days. This might take several seconds.
- 3 Click **Show Report**.
- 4 Drill down into the report.
- 5 Click **Show Latest** to update the report statistics.

Adding VM Wall Rules from the VM Flow Report

By drilling down into the traffic data, you can evaluate the use of your resources and send session information to VM Wall to create a new allow or deny rule. VM Wall rule creation from VM Flow data is available at the datacenter and cluster levels only.

To add a firewall rule from the VM Flow report output

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Flow** tab.
- 3 Expand the firewall action list.
- 4 Expand the L4 or L2/L3 protocol list.
- 5 If an L2/L3 protocol was selected, select the L2/L3 protocol or message type.
- 6 Expand the traffic direction list.
- 7 Expand the port type list.
- 8 Expand the application or port list.
- 9 Expand the destination IP address list.
- 10 Review the source IP addresses.
- 11 Select the **VM Wall** column radio button for a source IP address to create a VM Wall rule.

A pop-up window opens. Click **Ok** to proceed.

The VM Wall table appears. A new table row is displayed at the bottom of the Data Center Low Precedence Rules or Cluster Level Rules section with the session information completed.

- 12 (Optional) Double-click the **Action** column cell to change the value to **Allow** or **Deny**.
- 13 (Optional) With the new row selected, click **Up** to move the rule up in priority.
- 14 (Optional) Select the **Log** check box to log all sessions matching this rule.
- 15 Click **Commit** to save the rule.

Deleting All Recorded Flows

At the datacenter level, you can delete the data for all recorded traffic sessions within the datacenter. This clears the data from charts, the report, and the database. Typically, this is only used when moving your vShield Zones deployment from a lab environment to a production environment. If you must maintain a history of traffic sessions, do not use this feature.

To delete traffic statistics for a datacenter

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Flow** tab.
- 3 Select a datacenter resource from the inventory panel.
- 4 Click **Delete All Flows**.
- 5 Click **Ok** in the pop-up window to confirm deletion.



CAUTION You cannot recover traffic data after you click **Delete All Flows**.

Editing Port Mappings

When you click **Edit Port Mappings**, a table appears, listing well-known applications and protocols, their respective ports, and a description. vShield Zones recognizes common protocol and port mappings, such as HTTP over port 80. Your organization might employ an application or protocol that uses a non-standard port. In this case, you can use Edit Port Mappings to identify a custom protocol-port pair. Your custom mapping appears in the VM Flow report output.

The Edit Port Mappings table offers complete management capabilities. You can edit or delete any row in the table, including the default entries. The table provides a model for you to follow.

Adding an Application-Port Pair Mapping

You can add a custom application-port mapping to the port mappings table.

To add an application port-pair mapping

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Flow** tab.
- 3 Click **Edit Port Mappings**.
- 4 Click a row in the table.
- 5 Click **Add**.
A new row is inserted above the selected row.
- 6 Double-click the **Application** cell and type the application name.
- 7 Double-click the **Port Number** cell and type the port number.
- 8 Double-click the **Protocol** cell to select the transport protocol.
- 9 Double-click the **Resource** cell to select the container in which to enforce the new mapping.
The **ANY** value adds the port mapping to all containers.
- 10 Double-click the **Description** cell and type a brief description.
- 11 Click **Hide Port Mappings**.

Deleting an Application-Port Pair Mapping

You can delete any application-port pair mapping from the table. When you delete a mapping, any traffic to the application-port pair is listed as Uncategorized in the VM Flow statistics.

To delete an application-port pair mapping

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Flow** tab.
- 3 Click **Edit Port Mappings**.
- 4 Click a row in the table.
- 5 Click **Delete** to delete it from the table.

Hiding the Port Mappings Table

When you click **Edit Port Mappings**, the label changes from Edit Port Mappings to Hide Port Mappings. Click **Hide Port Mappings**.

Virtual Machine Discovery and Inventory

12

The discovery feature enables a vShield to inspect and provide details on the traffic sessions to and from your virtual machines. Discovery also enables a vShield to scan your virtual machines to identify the operating system and open services. After discovering a virtual machine, a vShield provides details about the virtual machine in the **VM Inventory** table.

This chapter includes the following topics:

- [“Reading the Discovery Results Table”](#) on page 51
- [“Enabling Continuous Discovery”](#) on page 52
- [“Running an On-Demand Discovery of Virtual Machines”](#) on page 52
- [“Scheduling Periodic Discovery of Virtual Machines”](#) on page 53
- [“Terminating an In-Progress Discovery”](#) on page 53
- [“Stopping a Scheduled Discovery Scan”](#) on page 54
- [“Using VM Inventory to View Virtual Machine Details”](#) on page 54

Reading the Discovery Results Table

The **Results** table presents the following information:

| Column | Description |
|----------------------|---|
| Check box | Selecting the top check box selects check boxes below. You can use the check box option in conjunction with the Terminate or Remove actions. |
| Start/Scheduled Time | The time a current discovery started or the time a scheduled discovery will start. |
| IPs in Subnet | The number of IP addresses covered by a manual or scheduled discovery operation. If you run discovery on a single host, this value is displayed as 1. If you run discovery on servers in a subnet, this value reflects the number of logical IP addresses in that subnet. |
| Servers Discovered | The number of hosts found in the discovery. If you are performing discovery on a single host, this value is displayed as 1. If you are discovering applications in a subnet, this value reflects the number of hosts discovered in that subnet. This value can differ from the IPs in Subnet value if a full complement of hosts do not exist in the subnet. |
| Duration (sec) | The total time, in seconds, elapsed during the discovery operation. |
| Status | The current status of the discovery operation: <ul style="list-style-type: none">■ In Progress denotes the discovery is running.■ Completed denotes discovery has completed.■ Scheduled denotes the discovery is not currently active, but will commence at the scheduled time. |

Enabling Continuous Discovery

Continuous discovery enables active inspection and identification of all traffic passing through a vShield. When continuous discovery is enabled, the vShield inspects all incoming and outgoing traffic to identify the virtual machines in your network by IP address. The discovery process identifies the operating system, open applications, and application ports for each virtual machine. The vShield Manager presents this information in the **VM Flow** charts and the **VM Inventory** tables. Using the information in the **VM Flow** charts, you can create firewall rules to allow or deny further communication based on discovered criteria.

Continuous discovery takes precedence over a manual discovery operation.

To enable continuous discovery

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **VM Discovery** tab.
- 3 Click **Automated**.
- 4 From the **Scheduled Discovery Status** drop-down menu, select **Continuous**.
- 5 Click **OK**.

Running an On-Demand Discovery of Virtual Machines

Manual discovery provides a view-only look into the operating system, applications, and open ports on a single virtual machine or multiple virtual machines in a subnet. As in a vulnerability scan, you can use manual discovery to identify potential security issues from applications or ports that should not be open.

vShield Zones does not support a manual discovery operation where the target server resides outside of a physical firewall, proxy, or any similar device that impedes direct communication between the vShield and the server being scanned.

To run an on-demand discovery of virtual machines

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **VM Discovery** tab.
- 3 Click **Manual**.
- 4 Type the **Network Address** of the subnet or virtual machine to scan.
- 5 Type the **Mask** of the subnet or virtual machine.
- 6 Click **Add**.
- 7 Repeat steps 4-6 to specify more subnets or virtual machines to scan.
- 8 Click **Start**.

A progress dialog box displays discovery details. Note the following fields:

- **Status:** The following status stages detail the progress of the discovery operation.
 - **In Progress** denotes discovery is running.
 - **Processing Results** indicates that the search is complete and is currently processing data for display.
 - **Completed** denotes discovery is complete.
- **Servers Discovered:** The number of servers found within the parameters
- **Scheduled Start Time:** When the discovery operation commenced
- **Duration:** Length of completed discovery process
- **Target Subnets:** IP address of subnet or virtual machine being searched

The discovery details remain in the **Results** table until removed.

Scheduling Periodic Discovery of Virtual Machines

Periodic discovery enables you to set a schedule by which your vShield scans a single virtual machine or multiple virtual machines in a subnet. Providing the same feedback as a manual discovery, periodic discovery can assist you in identifying potential security issues from applications or ports that should not be open. Upon completion, any discovered virtual machines are entered into the VM Inventory table.

Periodic discovery conflicts with continuous discovery. If you choose to schedule a periodic discovery, continuous discovery is terminated and does not resume until you re-enable continuous discovery.

You can schedule only one periodic discovery operation at a time. However, you can search multiple subnets and servers within this one scheduled operation.

To schedule periodic discovery of virtual machines

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **VM Discovery** tab.
- 3 Click **Automated**.
- 4 From the **Scheduled Discovery Status** drop-down menu, select **Periodic**.
- 5 Type a value in the **Maximum Discovery Duration (min)** field to limit the number of minutes the discovery operation can run before it must be terminated.
The default is 90 minutes.
- 6 From the **Discover 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.
- 7 Type the **Network Address** of the subnet or virtual machine to process.
- 8 Type the **Mask** of the subnet or virtual machine.
For an individual virtual machine, type **255.255.255.255**.
- 9 Click **Add**.
- 10 (Optional) Repeat Steps 7-9 to add more subnets virtual machines.
- 11 Click **OK**.
The discovery operation runs according to the schedule. When the scheduled time arrives, the discovery operation starts and changes the Status field in the **Results** table to In Progress.
- 12 Under the **VM Discovery** tab, click **Results**.
- 13 When Status is displayed as Completed, click the **Start/Scheduled Time** link for the operation to view the results.

Terminating an In-Progress Discovery

You can terminate a discovery scan that is in progress.

To terminate an in-progress discovery

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **VM Discovery** tab.
- 3 Click **Results**.
- 4 In the **Status** column, search for an In Progress scan.

- 5 Select the check box next to the in-progress scan.
- 6 Click **Terminate** below the table.
- 7 Click **OK** to confirm termination.

Stopping a Scheduled Discovery Scan

You can stop a scheduled discovery scan before it starts.

To remove a scheduled discovery scan

- 1 Select a vShield instance from the inventory panel.
- 2 Click the **VM Discovery** tab.
- 3 Click **Automated**.
- 4 From the **Scheduled Discovery Status** drop-down list, select **Off**.
- 5 Select the check box next to each subnet or virtual machine under **Network Address**, and click **Remove**.
- 6 Click **OK**. The scheduled scan is removed.

Using VM Inventory to View Virtual Machine Details

vShield Zones profiles each virtual machine in your inventory through continuous discovery of the traffic sessions to and from your virtual machines. After traffic has been scanned by a vShield, a profile is created detailing the operating system, applications, and open ports for each virtual machine. These profiles are presented under the **VM Inventory** tab.

After initial vShield Zones setup, the inventory is empty, awaiting continuous discovery by each vShield instance to identify the virtual machines and services in the protected zone. A vShield discovers all of the open services on a virtual machine by examining incoming and outgoing sessions, or through a directed discovery scan. Each virtual machine is listed under the vShield that performed the discovery.

The **VM Inventory** tab appears at the datacenter, cluster, folder, and port group levels, as well as at the individual virtual machine level. At the container level, the **VM Inventory** tab lists all of the virtual machines being protected by all of the vShield instances in the selected container.

The VM Inventory table presents the following information:

| Column | Description |
|-------------------------|---|
| VM/Application | Displays three levels of information. At first glance, the IP address of the virtual machine displays nesting further information. When the virtual machine IP address is expanded, the operating system of that virtual machine appears. When the operating system is expanded, the open applications discovered on that virtual machine appear. |
| Version/Ports | Displays two pieces of information. The OS version for the virtual machine displays along the same row as the virtual machine IP address. When the OS is expanded in the first column, the Version/Ports column displays the open ports related to each discovered application. |
| Last Update Time | Displays the date when the virtual machine details were last updated. |

Command Line Interface

Each vShield and vShield Manager contains a command line interface (CLI) for virtual appliance initialization and maintenance. This interface provides direct execution of commands, whether using a vSphere Client console session or by way of remote access such as SSH or Telnet.

User management in the CLI for any vShield Zones component is separate from user management in the vShield Manager user interface .

This chapter includes the following topics:

- [“Logging In and Out of the CLI”](#) on page 55
- [“CLI Command Modes”](#) on page 55
- [“CLI Syntax”](#) on page 56
- [“Moving Around in the CLI”](#) on page 56
- [“Getting Help within the CLI”](#) on page 56
- [“CLI Command Reference”](#) on page 57

Logging In and Out of the CLI

Before you can run CLI commands, you must initiate a vSphere Client console session to a vShield Zones virtual appliance. You can log in using the default user name **admin** and password **default**.

To log out, type `exit` from either Basic or Privileged mode.

CLI Command Modes

The commands available to you at any given time depend on which mode you are currently in. The CLI has two main modes, Basic and Privileged, and two sub-modes, Configuration and Interface Configuration.

- **Basic:** Basic mode is a read-only mode. To have access to all commands, you must enter Privileged mode.
- **Privileged:** Privileged mode commands allow support-level options such as debugging and opening and closing of support tunnels. Privileged mode configurations are not saved upon reboot. You must run the `write memory` command to save Privileged mode configurations.
- **Configuration:** Configuration mode commands allow you to change the current configuration of vShield Zones virtual appliance utilities. You can access the Configuration mode from within Privileged mode. From the Configuration mode, you can enter Interface configuration mode.
- **Interface Configuration:** By running Interface Configuration mode commands, you can change the configuration of virtual appliance interfaces. For example, you can change the IP address and default IP route for the management (MGMT) port of the vShield Manager.

CLI Syntax

Run commands at the prompt as shown. Do not type the <>, (), or [] symbols.

```
command <A.B.C.D> (option1|option2) [WORD]
```

- Text and numerical values that must be entered are enclosed in angle brackets.
- Multiple, optional keywords or values are enclosed in parentheses.
- Options are shown separated by a pipe character.
- A single, optional keyword or value is enclosed in square brackets.

Moving Around in the CLI

The following commands move the pointer around on the command line:

| Keystrokes | Description |
|----------------------------------|---|
| CTRL+A | Moves pointer to beginning of the line. |
| CTRL+B or the left arrow key | Moves pointer back one character. |
| CTRL+C | Ends any operation that continues to propagate, such as a ping. |
| CTRL+D | Deletes the character at the pointer. |
| CTRL+E | Moves pointer to end of the line. |
| CTRL+F or the right arrow key | Moves pointer forward one character. |
| CTRL+K | Deletes all characters from pointer to the end of the line. |
| CTRL+N or the down arrow key | Displays more recent commands in the history buffer after recalling commands with CTRL+P (or the up arrow key). Repeat to recall other recently run commands. |
| CTRL+P or the up arrow key | Recalls commands in the history, starting with the most recent completed command. Repeat to recall successively older commands. |
| CTRL+U | Deletes all characters from pointer to beginning of the line. |
| CTRL+W | Deletes word to the left of pointer. |
| ENTER | Scrolls down one line. |
| ESC+B | Moves pointer back one word. |
| ESC+D | Deletes from pointer to the end of the word. |
| ESC+F | Moves pointer forward one word. |
| SPACE | Scrolls down one screen. |

Getting Help within the CLI

The CLI contains the following commands for assisting your use:

| Command | Description |
|------------|--|
| ? | Moves pointer to beginning of the line. |
| sho? | Displays a list of commands that begin with a particular character string. |
| exp+TAB | Completes a partial command name. |
| show ? | Lists the associated keywords of a command. |
| show log ? | Lists associated arguments of a keyword. |
| list | Displays the verbose options of all commands for the current mode. |

CLI Command Reference

The following tables details the available CLI commands as if the `list` command were run in each CLI command mode.

A (vS) preceding a description indicates a vShield-only command. A (M) preceding a description indicates a vShield-Manager-only command.

Table 13-1. Basic Mode Commands

| Command | Description |
|--|--|
| <code>close support-tunnel</code> | Deprecated. Do not use. |
| <code>debug snapshot list</code> | (M) Display the list of snapshots currently on the Manager. |
| <code>enable</code> | Enter Privileged mode. |
| <code>exit</code> | Exit CLI. |
| <code>list</code> | List commands in verbose form. |
| <code>open support-tunnel</code> | Deprecated. Do not use. |
| <code>open support-tunnel publisher ip <A.B.C.D> port <1-65535></code> | Deprecated. Do not use. |
| <code>open support-tunnel publisher ip <A.B.C.D> port <1-65535> proxy ip <A.B.C.D> port <1-65535></code> | Deprecated. Do not use. |
| <code>open support-tunnel publisher ip <A.B.C.D> port <1-65535> proxy ip <A.B.C.D> port <1-65535> username <USERNAME> password <PASSWORD></code> | Deprecated. Do not use. |
| <code>ping <A.B.C.D></code> | Ping destination IP address or host name. |
| <code>quit</code> | Exit current mode and down to previous mode. |
| <code>reset</code> | Reset terminal settings. |
| <code>setup</code> | Launch the CLI setup wizard to configure basic settings. |
| <code>show arp</code> | Show contents of the ARP cache. |
| <code>show clock</code> | Show system clock. |
| <code>show debug</code> | (vS) List debug paths that are enabled. |
| <code>show esx-watchdog</code> | (vS) Display the ESX Watchdog for the vShield. |
| <code>show ethernet</code> | Show Ethernet information about vShield Zones component interfaces. |
| <code>show filesystems</code> | Show capacity information for the hard disk on the vShield Zones component. |
| <code>show hardware</code> | Show information about any hardware components not functioning properly. |
| <code>show interface [IFNAME]</code> | Show status of all interfaces or a specific interface. |
| <code>show ip route</code> | Show the IP routing table. |
| <code>show log (follow reverse)</code> | <ul style="list-style-type: none"> ■ follow: Display and continuously update system event log. ■ reverse: Show event log in reverse time order. |
| <code>show log alerts</code> | (vS) Display vulnerability alerts generated by a vShield. |
| <code>show log events</code> | (vS) Display system events. |
| <code>show log last <N></code> | Show last <i>n</i> lines of the log. |
| <code>show manager log</code> | (M) Show management system log. |
| <code>show manager log (follow reverse)</code> | <ul style="list-style-type: none"> ■ (M) follow: Display and continuously update management system log. ■ (M) reverse: Show management system log in reverse time order. |

Table 13-1. Basic Mode Commands (Continued)

| Command | Description |
|-------------------------------|---|
| show manager log last <N> | (M) Show last <i>n</i> lines of the management system log. |
| show process (list monitor) | Display running processes. <ul style="list-style-type: none"> ■ list: List all processes. ■ monitor: Continuously monitor processes. |
| show raid | Deprecated. Do not use. |
| show raid detail | Deprecated. Do not use. |
| show services | (vS) List services which are being protected by profiles. |
| show session-manager counters | (vS) Display historical statistics on the sessions processed by a vShield. |
| show session-manager sessions | (vS) Display stats on current sessions maintained by a vShield. |
| show slots | Deprecated. Do not use. |
| show stacktrace | Show stack traces of failed components. |
| show system memory | Display the summary of memory utilization. |
| show tech-support | Show the system log. |
| show version | Show serial number and software versions running on an vShield Zones component. |
| ssh <A.B.C.D> | Open an SSH connection. |
| telnet <A.B.C.D> | Open a Telnet connection. |
| telnet <A.B.C.D> <PORT> | Open a Telnet connection to a host specifying a destination port. |
| traceroute <A.B.C.D> | Trace the route to a destination address or host name. |

Table 13-2. Privileged Mode Commands

| Command | Description |
|---|--|
| clear slot (1 2) | Deprecated. Do not use. |
| clear vty | Clear all the other vty connections. |
| close support-tunnel | Deprecated. Do not use. |
| configure terminal | Enter Configuration mode. |
| copy http URL slot (1 2) | Deprecated. Do not use. |
| copy http URL temp | Deprecated. Do not use. |
| copy running-config startup-config | Copy from current system configuration to startup configuration. |
| copy scp URL slot (1 2) | Deprecated. Do not use. |
| copy scp URL temp | Deprecated. Do not use. |
| database erase | (M) Erase the vShield Manager database and refresh the database to factory defaults. |
| debug copy (scp ftp) URL (packet-traces tcpdumps) (<FILENAME> all) | Copy packet-trace or tcpdump files and export to a remote server. |
| debug export snapshot <FILENAME> scp <URL> | Deprecated. Do not use. |
| debug import snapshot <FILENAME> scp <URL> | Deprecated. Do not use. |
| debug packet capture | (vS) Capture all processed packets for retrieval. |
| debug packet capture interface (mgmt scan u0 p0) | (vS) Capture all processed packets for a specific interface for retrieval. |
| debug packet capture interface (mgmt scan u0 p0) <EXPRESSION> | (vS) Capture all processed packets for retrieval from the selected interface, expressing results using an underscore ('_') instead of a space (' '). |

Table 13-2. Privileged Mode Commands (Continued)

| Command | Description |
|---|--|
| debug packet capture segment 0 | (vS) Capture all processed packets for retrieval for the U0-P0 segment. |
| debug packet capture segment 0 <EXPRESSION> | (vS) Capture all processed packets for retrieval for the U0-P0 segment. EXPRESSION enables you to express results using an underscore ('_') instead of a space (' '). |
| debug packet display interface (mgmt scan u0 p0 u1 p1) | (vS) Display all processed packets for a particular interface. |
| debug packet display interface (mgmt scan u0 p0 u1 p1) <EXPRESSION> | (vS) Display all processed packets for a particular interface. EXPRESSION enables you to express results using an underscore ('_') instead of a space (' '). |
| debug remove (packet-traces tcpdumps) (<FILENAME> all) | Delete a packet trace or tcpdump debug log. |
| [no] debug <service> (ice sysmgr vdb <WORD>) (low medium high) | (vS) Enable (or disable) logging for a service within a profile, noting the specific engine and severity. |
| [no] debug <SERVICE> flow src <A.B.C.D/MASK:PORT> dst <W.X.Y.Z/MASK:PORT> | (vS) Enable (or disable) logging of messages for a session only from a source to a destination. A source or destination value of 0.0.0.0/0:0 matches all applicable values. |
| debug show files (packet-traces tcpdumps) | Show the packet trace or tcpdump files that have been saved. |
| debug snapshot list | Deprecated. Do not use. |
| debug snapshot remove <FILENAME> | Deprecated. Do not use. |
| debug snapshot restore (all config) <FILENAME> | Deprecated. Do not use. |
| default web-manager password | (M) Reset the admin vShield Manager user account password to the default value, default . |
| disable | Turn off Privileged mode. |
| end | End current mode and move down to previous mode. |
| exit | Exit CLI. |
| export tech-support scp <URL> | Export system diagnostics by using SCP to a specific URL. A system log file is created with the extension TXT. This file can be sent to technical support to determine potential vShield Zones component issues. You can also download and view this log from the vShield Manager user interface; see “Downloading a Technical Support Log from a Component” on page 15. |
| list | List commands in verbose form. |
| no debug <SERVICE> | (vS) Disable all logging for the specified service. |
| no debug packet | (vS) Disable packet capture. |
| open support-tunnel | Deprecated. Do not use. |
| open support-tunnel publisher ip <A.B.C.D> port <1-65535> | Deprecated. Do not use. |
| open support-tunnel publisher ip <A.B.C.D> port <1-65535> proxy ip <A.B.C.D> port <1-65535> | Deprecated. Do not use. |
| open support-tunnel publisher ip <A.B.C.D> port <1-65535> proxy ip <A.B.C.D> port <1-65535> username <USERNAME> password <PASSWORD> | Deprecated. Do not use. |
| ping <A.B.C.D> | Ping destination host name. |
| quit | Exit current mode and move down to previous mode. |
| reboot | Reboot the system. |
| reset | Reset terminal settings. |

Table 13-2. Privileged Mode Commands (Continued)

| Command | Description |
|--|--|
| set clock <HH:MM:SS> <MM DD YY> | Set system date and time as hour:minute:seconds month day year. |
| set support key <KEY> | Deprecated. Do not use. |
| show alerts (vulnerability decoder events) | Show system alerts as they relate to vulnerability engine, protocol decoders, or network events. |
| show arp | Show contents of the ARP cache. |
| show clock | Show system clock. |
| show database-backup | Deprecated. Do not use. |
| show debug | (vS) Debugging functions. |
| show ethernet | Show Ethernet information about vShield Zones component interfaces. |
| show esx-watchdog | (vS) Show ESX Watchdog information for the vShield. |
| show filesystems | Show capacity information for the hard disk on the vShield Zones component. |
| show hardware | Show information about any hardware components not functioning properly. |
| show interface [IFNAME] | Show status of all enabled interfaces or a specified interface. |
| show ip route | Show IP routing table. |
| show ip route <A.B.C.D/MASK> | Show IP routing table for specific IP. |
| show log (follow reverse) | <ul style="list-style-type: none"> ■ follow: Display and continuously update log. ■ reverse: Show log in reverse time order. |
| show log alerts | (vS) Display vulnerability alert. |
| show log events | (vS) Display system event. |
| show log last <N> | Show last <i>n</i> lines of the log. |
| show manager log | (M) Show management system log. |
| show manager log (follow reverse) | <ul style="list-style-type: none"> ■ (M) follow: Display and continuously update management system log. ■ (M) reverse: Show management system log in reverse time order. |
| show manager log last <N> | (M) Show last <i>n</i> lines of the management system log. |
| show policy-based-forwarding | Show the state and statistics (if enabled) of policy-based forwarding. |
| show process (list monitor) | Display running processes. |
| show raid | Deprecated. Do not use. |
| show raid detail | Deprecated. Do not use. |
| show running-config | Current operating configuration. |
| show services | (vS) List services which are being protected. |
| show session-manager counters | (vS) Display historical statistics on the sessions processed by a vShield. |
| show session-manager sessions | (vS) Display stats on current sessions maintained by a vShield. |
| show slots | Shows the images on the slots. |
| show stacktrace | Show stack traces of failed components. |
| show startup-config | Show contents of startup configuration. |
| show support-tunnel | Deprecated. Do not use. |
| show system memory | Display the summary of memory utilization. |
| show system uptime | Show the length of time the vShield Zones component has been operational since last reboot. |

Table 13-2. Privileged Mode Commands (Continued)

| Command | Description |
|-------------------------|--|
| show tech-support | Show the system log. |
| show version | Show software versions currently available. |
| shutdown | Shutdown vShield Zones component. |
| ssh <A.B.C.D> | Open an SSH connection. |
| telnet <A.B.C.D> | Telnet to host name of a remote system. |
| telnet <A.B.C.D> <PORT> | Telnet to specific port on a specified remote system. |
| terminal length <0-512> | Set terminal display length to <0-512>. If length is 0, no display control is performed. |
| terminal no length | Negate a terminal length command. |
| traceroute <A.B.C.D> | Trace a route to the destination address or host name. |
| write | Write running configuration to terminal. |
| write erase | Reset configuration to factory default settings. |
| write memory | Write running configuration to memory. |

Table 13-3. Configuration Mode Commands

| Command | Description |
|--|--|
| boot system slot (1 2) | Deprecated. Do not use. |
| enable-password (hash plaintext) <PASSWORD> | Change the Privileged mode password. |
| end | End current mode and down to previous mode. |
| esx-watchdog configure server ip <A.B.C.D> port <1-65535> protected <PROT> unprotected <UNPROT> interfaces <NIC> | (vS) Enable the vShield Watchdog. You must know the IP address and listening port of the ESX host, the name of the vSwitch that contains the Protected port group, the name of the vSwitch that contains the Unprotected port group, and the name of the NIC homed on the Unprotected vSwitch. |
| esx-watchdog configure server ip <A.B.C.D> protected <PROT> unprotected <UNPROT> interfaces <NIC> | (vS) Enable the vShield Watchdog. You must know the IP address of the ESX host, the name of the vSwitch that contains the Protected port group, the name of the vSwitch that contains the Unprotected port group, and the VMNIC names homed on this vSwitch. |
| esx-watchdog (enable disable) | Enable or disable the vShield Watchdog on the ESX server where a vShield resides. |
| exit | Exit current mode and down to previous mode. |
| gateway-failure-mode (bypass block) | Deprecated. Do not use. |
| hostname <HOSTNAME> | Set CLI prompt name. |
| interface <IFNAME> | Enter Interface Configuration mode for the specified interface. |
| [no] ip route <A.B.C.D/MASK> <W.X.Y.Z> | Add or remove a static route. |
| linkwatch interval <5-60> | Deprecated. Do not use. |
| list | List commands in verbose form. |
| manager key <KEY> | (vS) Set a shared key for vShield communication with the vShield Manager. |
| [no] mode policy-based-forwarding | Deprecated. Do not use. |
| [no] mode policy-based-forwarding cdp-hold-time <2-255> | Deprecated. Do not use. |
| no esx-watchdog configure | Clear the current ESX watchdog configuration. |
| no interface <IFNAME> | Remove an interface's configuration. |
| no linkwatch | Deprecated. Do not use. |

Table 13-3. Configuration Mode Commands (Continued)

| Command | Description |
|--|--|
| <code>no log syslog</code> | Cancel logging to the syslog server. |
| <code>no user <username></code> | Remove a user account. |
| <code>reset</code> | Reset terminal settings to return a clean prompt. |
| <code>set service manager access <A.B.C.D/MASK></code> | (M) Configure an access rules for vShield Manager access by identifying an IP address and subnet mask that can access the vShield Manager. You can add more than one entry. |
| <code>[no] user <USERNAME> password (hash plaintext) <PASSWORD></code> | Add or modify user information for Basic mode login. |
| <code>[no] web-manager</code> | (M) Starts (or stops) the Web service (HTTP daemon) on the Enterprise Manager. You can use this command after you've executed the <code>no web-manager</code> command to stop and restart the HTTP services of the Enterprise Manager. |
| <code>write memory</code> | Write running configuration to memory. |

Table 13-4. Interface Configuration Mode Commands

| Command | Description |
|---|---|
| <code>duplex auto</code> | Deprecated. Do not use. |
| <code>duplex (half full) speed (10 100 1000)</code> | Deprecated. Do not use. |
| <code>end</code> | End current mode and down to previous mode. |
| <code>exit</code> | Exit current mode and down to previous mode. |
| <code>[no] ip address <A.B.C.D/MASK></code> | Set (or remove) the IP address and subnet mask of an interface. |
| <code>ip policy-address <A.B.C.D> next-hop <W.X.Y.Z></code> | Deprecated. Do not use. |
| <code>[no] link-detect</code> | Deprecated. Do not use. |
| <code>list</code> | List commands in verbose form. |
| <code>quit</code> | Exit current mode and down to previous mode. |
| <code>[no] shutdown</code> | Shutdown (or activate) the selected interface. |
| <code>write memory</code> | Write running configuration to memory. |

Appendix: Using VMotion with vShield Zones

VMotion facilitates the live migration of running virtual machines from one physical server to another, often used for cases such as load balancing and fault tolerance. vShield Zones virtual appliances are subject to the same high availability rules as guest virtual machines. However, vShield Zones requires not moving the vShield Zones virtual appliances.

This chapter includes the following topics.

- [“Preventing VMotion from Moving vShield Zones Virtual Appliances”](#) on page 63
- [“Permitting VMotion to Move Protected Virtual Machines”](#) on page 64

Preventing VMotion from Moving vShield Zones Virtual Appliances

If you have enabled VMware HA or VMware DRS features, you must disable movement of vShield Zones virtual appliances. This must be performed after installation of each vShield Zones component into vCenter.

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

To disable VMware HA or VMware DRS from moving the vShield Zones virtual appliances

- 1 Log in to the vSphere Client.
- 2 Right-click the cluster containing your vShield Zones virtual appliances and click **Edit Properties**.
The Admin Settings dialog box opens.
- 3 Under VMware HA, click **Virtual Machine Options**.
Locate the vShield Manager and vShield instances in the list.
- 4 For each vShield Zones virtual appliance, select the following values:
 - **VM Restart Priority: Disabled**
 - **Host Isolation Response: Leave VM powered on**Do not click **OK** at this time if VMware DRS is also enabled.
- 5 Under VMware DRS, click **Virtual Machine Options**.
Locate the vShield Manager and vShield instances in the list.
- 6 For each vShield Zones virtual appliance, select **Disabled** for **Automation Level**.
- 7 Click **OK** after all vShield Zones virtual appliances have been configured.

Permitting VMotion to Move Protected Virtual Machines

By default, vShield operation prevents VMotion from moving protected virtual machines between ESX hosts.

When deploying vShield Zones, you might have more than one ESX host where one or more vShield instances are identically configured. For example, a virtual machine protected by vShield-1 on ESX-1 can be moved using VMotion to ESX-2. By explicitly permitting VMotion, the virtual machine can be protected on ESX-2 as it was on ESX-1.

By default, a vShield raises an error during attempted virtual machine migration. The error states that the virtual machine is connected to a virtual intranet. This intranet is the network that the virtual machine connects to through the vSwitch on the protected side of the vShield, and which does not have a physical NIC. In this case, the vShield is bridging traffic to the unprotected network that is connected to a physical NIC.

To enable VMotion to disable the virtual intranet check

- 1 Locate the `vpzd.cfg` file on the vCenter Server. This file is typically installed at `C:\Documents and Settings\All Users\Application Data\VMware\VMware vCenter` by default.

- 2 Edit the `vpzd.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 `vpzd` section.

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

- 3 Save the `vpzd.cfg` file.
- 4 Restart the VMware vCenter Server service. You can access the service menu by going to **Control Panel > Administrative Tools > Services**.

Index

A

- accessing online help **11**
- adding a user **22**
- admin user account **22**
- Audit Logs **29**

B

- Backup Configuration **37**
- Backups
 - on-demand **17**
 - restoring **18**
 - scheduling **18**
- basic mode of CLI **55**

C

- CLI
 - backing up configuration **37**
 - configuration mode **55**
 - help **56**
 - interface mode **55**
 - logging in **55**
 - modes **55**
 - privileged mode **55**
 - syntax **56**
- Cluster Level Rules **42**
- command syntax **56**
- configuration mode of CLI **55**
- connecting to vCenter Server **13**
- continuous discovery **52**
- Create User **22**

D

- data
 - on-demand backups **17**
 - restoring a backup **18**
 - scheduling backups **18**
- Data Center High Precedence Rules **42**
- Data Center Low Precedence Rules **42**
- date **14**
- date range for VM Flow **46**
- Default Rules **42**
- deleting a port mapping **49**
- deleting a user **23**
- discovery **51**
 - continuous **52**
 - manual **52**

- periodic **53**
- removing a result **54**
- terminating **53**

- DNS **14**
- downloads
 - firewall logs **39**

E

- Edit Port Mappings **48**
 - add a mapping **48**
 - deleting **49**
- Hide Port Mappings **49**
- editing a user account **22**
- events
 - sending as traps to SNMP server **37**
 - sending to syslog **37**
 - syslog format **27**
 - system events **25**
 - vShield events **26**
 - vShield Manager events **26**

F

- firewall
 - about **41**
 - adding L2/L3 rules **43**
 - adding L4 rules **42**
 - adding rules from VM Flow **47**
 - deleting rules **44**
 - logs **39**
 - planning rule enforcement **42**
- flow analysis date range **46**
- Force Sync **38**

H

- help **11**
 - CLI **56**
- Hide Port Mappings **49**
- hierarchy of VM Wall rules **42**
- history of updates **20**
- Hosts & Clusters view **12**
- HTTP Proxy **14**

I

- Install vShield **31**
- installation
 - vShield manually **32**

- installing
 - updates **19**
 - vShield from template **31**
- interface mode of CLI **55**
- inventory
 - panel **12**
 - VM Inventory **54**
- inventory panel **12**

L

- L2/L3 rules
 - about **41**
 - adding **43**
- L4 rules
 - about **41**
 - adding **42**
- login
 - CLI **55**
 - vShield Manager **11**
- logs
 - audit **29**
 - firewall **39**

M

- Manual Install **32**

N

- Networks view **12**
- NTP **14**

O

- on-demand discovery **52**
- online help **11**

P

- password **22**
- periodic discovery **53**
- plug-in **16**
- port mappings **48**
 - add **48**
 - deleting **49**
 - hiding **49**
- privileged mode of CLI **55**
- proxy service **14**

R

- removing a discovery result **54**
- reports
 - audit log **29**
 - system events **25**
- restarting a vShield **38**
- restoring backups **18**
- results of discovery **51**

- roles and rights
 - about **21**
 - assigning to a user **22**

rules

- adding L2/L3 rules to VM Wall **43**
- adding L4 rules to VM Wall **42**
- deleting VM Wall rules **44**

S

- scheduling backups **18**
- serial number of vShield Manager **15**
- services
 - DNS **14**
 - NTP **14**
 - proxy **14**
- Show Logs **39**
- Show Report **46**
- SNMP traps from a vShield **37**
- status
 - of a vShield **38**
 - of update **19**
 - of vShield Manager **15**
- syncing a vShield **38**
- syntax for CLI commands **56**
- syslog format **27**
- Syslog Servers **37**
- system events **25**
- System Status **38**
 - Force Sync **38**
 - Restart **38**
 - Show VM Wall Logs **39**
 - traffic stats **38**
- system time **14**

T

- terminating a discovery **53**
- time **14**
- traffic analysis date range **46**
- traffic stats for a vShield **38**
- Trap Destinations **37**

U

- Uninstall vShield **36**
- uninstalling a vShield **36**
- Update History **20**
- Update Status **19**
- Update User **22**
- Updates
 - installing **19**
 - Update History **20**
 - Update Status **19**

- user interface
 - logging in **11**
 - online help **11**
- Users
 - adding **22**
 - admin account **22**
 - assigning a role and rights **22**
 - changing a password **22**
 - deleting **23**
 - editing **22**
 - roles and rights **21**
- V**
- vCenter Server connection **13**
- vCenter tab **13**
- views
 - Hosts & Clusters **12**
 - Networks **12**
- VM Discovery
 - continuous **52**
 - manual **52**
 - periodic **53**
 - removing a result **54**
 - results **51**
 - terminating **53**
- VM Flow
 - adding a VM Wall rule **47**
 - date range **46**
 - show report **46**
- VM Inventory **54**
- VM Wall **41**
 - about L4 and L2/L3 rules **41**
 - adding L2/L3 rules **43**
 - adding L4 rules **42**
 - adding rules from VM Flow **47**
 - deleting rules **44**
 - hierarchy of rules **42**
 - planning rule enforcement **42**
- VMotion **63**
- vShield
 - about **10**
 - CLI configuration **37**
 - discovery **51**
 - firewall logs **39**
 - forcing sync **38**
 - installing from template **31**
 - manual installation **32**
 - notification based on events **26**
 - restarting **38**
 - sending events as traps to SNMP **37**
 - sending events to syslog **37**
 - System Status **38**
 - traffic stats **38**
 - uninstalling **36**
- vShield Manager
 - about **9**
 - accessing online help **11**
 - date and time **14**
 - DNS **14**
 - inventory panel **12**
 - logging in **11**
 - Manual Install **15**
 - notification based on events **26**
 - NTP **14**
 - on-demand backups **17**
 - proxy service **14**
 - restoring a backup **18**
 - scheduling a backup **18**
 - serial number **15**
 - status **15**
 - user interface panels **12**
 - vSphere Plug-in **16**
- vShield Zones
 - vShield **10**
 - vShield Manager **9**
- vSphere Plug-in **16**

