

vShield Zones Administration Guide

vShield Zones 1.0 Update 1

EN-000167-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 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 is a registered trademark or trademark 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	9
1 Overview of vShield Zones	11
vShield Zones Components	11
vShield Manager	11
vShield Agent	11
2 vShield Manager User Interface Basics	13
Logging in to the vShield Manager	13
Accessing the Online Help	13
vShield Manager User Interface	13
vShield Manager Inventory Panel	14
Refreshing the Inventory Panel	14
Searching the Inventory Panel	14
vShield Manager Configuration Panel	14
3 Management System Settings	15
Identifying Your vCenter Server	15
Identifying DNS Services	16
Setting the vShield Manager Date and Time	16
Identifying a Proxy Server	16
Downloading a Technical Support Log from a Component	17
Backing Up vShield Manager Data	17
Viewing vShield Manager System Status	17
Installing a vShield Agent Manually	17
Registering the vShield Manager as a vSphere Client Plug-in	17
4 Backing Up vShield Manager Data	19
Backing Up Your vShield Manager Data on Demand	19
Scheduling a Backup of vShield Manager Data	20
Restoring a Backup	20
5 Updating the System Software	21
Viewing Current System Software	21
Uploading an Update	21
Reviewing the Update History	22
6 User Management	23
Managing User Rights	23
Managing the Default User Account	24
Adding a User	24
Assigning a Role and Rights to a User	24
Editing a User Account	24
Deleting a User Account	25

7 System Events 27

- Viewing the System Event Report 27
- System Event Notifications 27
 - vShield Manager Virtual Appliance Events 27
 - vShield Agent Virtual Appliance Events 28
- Syslog Format 28

8 Viewing the Audit Log 29**9 vShield Agent Installation 31**

- Installing vShield Agents 31
- Install a vShield Agent by Using the vShield Agent Template 31
- Installing a vShield Agent Manually on a vSwitch 33
 - Create a Second vSwitch 33
 - Create the Protected Port Group on the First vSwitch 33
 - Create the Unprotected Port Group on the Second vSwitch 33
 - Add the vShield Agent to the ESX Host 34
 - Assign the vShield Agent Interfaces to Port Groups 34
 - Set Up the vShield Agent 34
 - Add the vShield Agent to the vShield Manager 36
 - Move the Virtual Machines from First vSwitch to the Second vSwitch 36
- Installing a vShield Agent Manually on a vNetwork Distributed Switch 36
 - Create a Second vNetwork Distributed Switch 37
 - Create the Protected dvPort Group on the First vNetwork Distributed Switch 37
 - Create the Unprotected dvPort Group on Second vNetwork Distributed Switch 37
 - Install the vShield Agent 38
 - Assign the vShield Agent Interfaces to the dvPort Groups 38
 - Set Up the vShield Agent 39
 - Add the vShield Agent to the vShield Manager 40
 - Power Off the vShield Agent Virtual Machine 40
 - Move the Physical NICs from vNDS-1 to vNDS-2 40
 - Power On the vShield Agent Virtual Machine 41
- Uninstalling a vShield Agent 41
 - Uninstall a Template-Based vShield Agent 41
 - Uninstall a Manually Installed vShield Agent from a vSwitch 41
 - Uninstall a Manually Installed vShield Agent from a vNDS 41
- Powering Off vShield Zones Virtual Machines 42

10 vShield Agent Management 43

- Sending vShield Agent System Events to a Syslog Server 43
- Backing Up the Running CLI Configuration of a vShield Agent 43
- Viewing the Current System Status of a vShield Agent 44
 - Forcing a vShield Agent to Synchronize with the vShield Manager 44
 - Restarting a vShield Agent 44
 - Viewing Traffic Statistics by vShield Agent Interface 44
 - Downloading the Firewall Logs of a vShield Agent 45

11 Firewall Management 47

- Using VM Wall 47
 - Default Rules 47
 - Layer 4 Rules and Layer 2/Layer 3 Rules 47
 - Hierarchy of VM Wall Rules 48
 - Planning VM Wall Rule Enforcement 48
- Creating a Layer 4 Firewall Rule 48

Creating a Layer 2/Layer 3 Firewall Rule	49
Reverting to a Previous VM Wall Configuration	50
Deleting a VM Wall Rule	50
12 Traffic Analysis	51
Using VM Flow	51
Viewing a Specific Application in the VM Flow Charts	52
Changing the Date Range of the VM Flow Charts	52
Viewing the VM Flow Report	52
Adding VM Wall Rules from the VM Flow Report	53
Deleting All Recorded Flows	54
Editing Port Mappings	54
Adding an Application-Port Pair Mapping	54
Deleting an Application-Port Pair Mapping	55
Hiding the Port Mappings Table	55
13 Virtual Machine Discovery and Inventory	57
Reading the Discovery Results Table	57
Enabling Continuous Discovery	58
Running an On-Demand Discovery of Virtual Machines	58
Scheduling Periodic Discovery of Virtual Machines	59
Terminating an In-Progress Discovery	59
Stopping a Scheduled Discovery Scan	60
Using VM Inventory to View Virtual Machine Details	60
A Command Line Interface	61
Logging In and Out of the CLI	61
CLI Command Modes	61
CLI Syntax	62
Moving Around in the CLI	62
Getting Help within the CLI	62
Securing CLI User Accounts and the Privileged Mode Password	63
Adding a CLI User Account	63
Delete the admin User Account from the CLI	63
Change the CLI Privileged Mode Password	64
Command Reference	64
Administrative Commands	65
list	65
reboot	65
shutdown	65
CLI Mode Commands	66
configure terminal	66
disable	66
enable	66
end	67
exit	67
interface	67
quit	68
Configuration Commands	68
clear vmwall rules	68
copy running-config startup-config	69
database erase	69
enable password	69

hostname	70
ip address	70
ip name server	71
ip route	71
manager key	72
set clock	72
ntp server	73
setup	73
syslog	74
write	74
write erase	75
write memory	75
Debug Commands	75
debug copy	75
debug packet capture	76
debug packet display interface	76
debug remove	77
debug <i>service</i>	77
debug <i>service</i> flow src	78
debug show files	79
Show Commands	79
show alerts	79
show arp	80
show clock	80
show debug	80
show ethernet	81
show filesystem	81
show gateway rules	81
show hardware	82
show interface	82
show ip route	83
show log	83
show log alerts	84
show log events	84
show log last	84
show manager log	85
show manager log last	85
show ntp	86
show running-config	86
show services	86
show session-manager counters	87
show session-manager sessions	87
show slots	88
show stacktrace	88
show startup-config	88
show syslog	89
show system memory	89
show system uptime	89
show version	90
show vmwall log	90
show vmwall rules	90
Diagnostics and Troubleshooting Commands	91
export tech-support scp	91

link-detect	91
ping	91
show tech support	92
ssh	92
telnet	92
traceroute	93
User Administration Commands	93
default web-manager password	93
user	93
web-manager	94
Terminal Commands	94
clear vty	94
reset	95
terminal length	95
terminal no length	95
Deprecated Commands	96
B Using vMotion with vShield Zones	97
Preventing vMotion from Moving vShield Zones Virtual Appliances	97
Permitting vMotion to Move Protected Virtual Machines	98
C Using vShield Zones with Cisco Nexus 1000V Series Switches	99
About the Cisco Nexus 1000V	99
Prerequisites	100
Deploying vShield Zones	100
Configure the Management Port Profile	100
Configure VSD Port Profiles	100
Configure VSD Member Virtual Machine Port Profiles	101
Deploy the vShield Manager OVF	101
Deploy the vShield Agent from OVF	102
Assign the vShield Agent Interfaces to Port Profiles	102
Set Up the vShield Agent	103
Add the vShield Agent to the vShield Manager	104
D Troubleshooting	105
Troubleshooting Installation Issues	105
vShield Zones OVF Files Extracted to a PC Where vSphere Client Is Not Installed	105
vShield Zones OVF File Cannot Be Installed in vSphere Client	105
vShield Agent Virtual Machine Does Not Power On After OVF Is Installed	105
Cannot Log In to CLI After the vShield Manager Virtual Machine Starts	106
Cannot Log In to the vShield Manager User Interface	106
Cannot See the vShield Agent Template from the vShield Manager User Interface	106
vShield Agent Installation from vShield Manager User Interface Fails	106
vShield Manager Cannot Communicate with a vShield Agent	106
Troubleshooting Operation Issues	107
Cannot Configure a vShield Agent	107
Firewall Block Rule Not Blocking Matching Traffic	107
No Flow Data Displaying in VM Flow	107
Index	109

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 agent 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 agents. A vShield Manager can run on a different ESX host from your vShield agents and still control many vShield agents 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 13.

vShield Agent

The vShield agent is the active security component, inspecting traffic and providing firewall protection. You can install a vShield agent on a vSwitch that homes a physical NIC. As an ESX host can have multiple vSwitches and physical NICs, you can install multiple vShield agents on a single ESX host. Each installed vShield agent monitors all incoming and outgoing traffic on the host vSwitch. As traffic passes through a vShield agent, 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 agent 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 agent 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 agent as a template. The template allows you to install multiple vShield agents 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 13
- [“Accessing the Online Help”](#) on page 13
- [“vShield Manager User Interface”](#) on page 13

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 24.
- 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 agents. 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 agents between the vShield Manager and the vSphere Client inventory panels. Custom icons are used to show the difference between vShield agents and virtual machines, and the difference between protected and unprotected virtual machines.


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

Icon	Description
	A powered on vShield agent in active protection state.
	A powered off vShield agent.
	A powered on virtual machine that is protected by a vShield agent.
	A powered on virtual machine that is not protected by a vShield agent.
	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 15
- [“Identifying DNS Services”](#) on page 16
- [“Setting the vShield Manager Date and Time”](#) on page 16
- [“Identifying a Proxy Server”](#) on page 16
- [“Downloading a Technical Support Log from a Component”](#) on page 17
- [“Viewing vShield Manager System Status”](#) on page 17
- [“Installing a vShield Agent Manually”](#) on page 17
- [“Registering the vShield Manager as a vSphere Client Plug-in”](#) on page 17

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 19.

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 21.

Installing a vShield Agent Manually

You can use the **Manual Install** option to install a vShield agent. See [“Installing vShield Agents”](#) on page 31.

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 19
- [“Scheduling a Backup of vShield Manager Data”](#) on page 20
- [“Restoring a Backup”](#) on page 20

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 21
- [“Uploading an Update”](#) on page 21
- [“Reviewing the Update History”](#) on page 22

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

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 agent. All vShield agents have been upgraded when the status of the last vShield agent 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 23
- [“Adding a User”](#) on page 24
- [“Assigning a Role and Rights to a User”](#) on page 24
- [“Editing a User Account”](#) on page 24
- [“Deleting a User Account”](#) on page 25

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 24.

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

This chapter includes the following topics:

- [“Viewing the System Event Report”](#) on page 27
- [“System Event Notifications”](#) on page 27
- [“Syslog Format”](#) on page 28

Viewing the System Event Report

The vShield Manager aggregates system events into a report that can be filtered by vShield agent 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 agents from the **vShield** field.
All vShield agents 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 17.	See “Viewing vShield Manager System Status” on page 17.	See “Viewing vShield Manager System Status” on page 17.

vShield Agent 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 28.	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 27.	See “Viewing the Current System Status of a vShield Agent” on page 44.	See “Viewing the Current System Status of a vShield Agent” on page 44.	See “Viewing the Current System Status of a vShield Agent” on page 44.

	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 28.
GUI	See “Viewing the Current System Status of a vShield Agent” on page 44.	See “Viewing the Current System Status of a vShield Agent” on page 44.	See “Viewing the Current System Status of a vShield Agent” on page 44.	Refer to the System Event Log. See “Viewing the System Event Report” on page 27.

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 the 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 Agent Installation

You must add each vShield agent to your vShield Manager for configuration and management.

This chapter includes the following topics:

- [“Installing vShield Agents”](#) on page 31
- [“Uninstalling a vShield Agent”](#) on page 41
- [“Powering Off vShield Zones Virtual Machines”](#) on page 42

Installing vShield Agents

Installing a vShield agent adds an agent to the vCenter Server inventory and the vShield Manager. You must name the vShield agent and specify an IP address for the management interface.

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

There are three methods for installing a vShield agent.

- [“Install a vShield Agent by Using the vShield Agent Template”](#) on page 31
- [“Installing a vShield Agent Manually on a vSwitch”](#) on page 33
- [“Installing a vShield Agent Manually on a vNetwork Distributed Switch”](#) on page 36

Install a vShield Agent by Using the vShield Agent Template

To use a template for the installation, you must have established a vShield agent template, as detailed in the *vShield Zones Quick Start Guide*.

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

- 1 In the vShield Manager, click the ESX host to protect in the inventory panel.
- 2 On the **Install vShield** tab, click **Configure Install Parameters**.

3 Complete the form:

Field	Action
Select from available vShields	Leave this field blank.
Select template to clone	Select the vShield agent template.
Select a datastore to place clone	Select the datastore on which to store the vShield agent virtual machine data.
Enter a name for the clone	Type a unique name for the vShield agent. This name appears in your vSphere Client and vShield Manager inventories.
Specify IP Address of vShield VM	Type the IP address to be assigned to the vShield agent's management interface.
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 associated VLAN ID (optional)	Type the VLAN ID to assign to the management interface of the vShield agent. This is required if the vShield Manager management interface has been tagged with a VLAN ID. These management interfaces must be able to communicate to complete installation.
Specify Secure Key for vShield (leave blank for default)	(Optional) Type a key to be used between the vShield agent and the vShield Manager for secure communication. By default, this entry in this field is masked. This key is used for encrypted communication between the vShield agent and the vShield Manager. Keys are not shared across the network.
Select a vSwitch to shield	Select the vSwitch to protect. The vSwitches eligible for protection are highlighted in green in the accompanying table.

4 Click **Continue**.

The summary page displays before and after illustrations of vShield agent 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.

5 Click **Install**.

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

6 After installation is complete, open the vSphere Client.

7 Locate the vShield agent in your inventory.

The vShield agent virtual machine is already powered on.

8 If vMotion is enabled, disable it for the vShield agent virtual machine.

See [“Using vMotion with vShield Zones”](#) on page 97.

9 Ensure that continuous discovery is enabled. See [“Enabling Continuous Discovery”](#) on page 58.

Installing a vShield Agent Manually on a vSwitch

You can manually install a vShield agent onto a vSwitch that is associated with a physical NIC. Manual vShield agent installation requires creating a second vSwitch and two port groups. After you create these items, you can install the vShield agent and move the virtual machines to the second vSwitch for protection.



CAUTION When installing a vShield agent manually, the virtual machines have network downtime while they are transitioning between vSwitches.

Installing an agent manually involves the following process, assuming that you have deployed a vSwitch with at least one attached vNIC.

- 1 Create a second vSwitch. Keep the vNIC on the original vSwitch. See [“Create a Second vSwitch”](#) on page 33.
- 2 Create a protected port group and an unprotected port group.
See [“Create the Protected Port Group on the First vSwitch”](#) on page 33, and see [“Create the Unprotected Port Group on the Second vSwitch”](#) on page 33.
- 3 Install the vShield agent, connecting the vShield agent network adapters to the protected and unprotected port groups. You must also connect the management interface of the vShield agent to a port group that is reachable from the vShield Manager. See [“Install the vShield Agent”](#) on page 38.
- 4 Move the virtual machines from the first vSwitch to the second vSwitch. See [“Move the Virtual Machines from First vSwitch to the Second vSwitch”](#) on page 36.

Create a Second vSwitch

Create a second vSwitch on the target ESX host. This switch is referred to as vSwitch-2. Do not assign a physical adapter to vSwitch-2.

Create the Protected Port Group on the First vSwitch

You must add the protected port group to the first vSwitch, referred to as vSwitch-1.

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

To create the protected port group

- 1 Click **Properties** for vSwitch-1.
- 2 Create a port group.
Include a string such as **protected** or **prot** in the name for quick identification.
- 3 (Optional) Identify the VLAN IDs that can pass through the port group.
- 4 After the protected port group has been created, enable promiscuous mode for the port group.

Create the Unprotected Port Group on the Second vSwitch

You must add the unprotected port group to the second vSwitch, referred to as vSwitch-2.

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

To create the Unprotected port group

- 1 Click **Properties** for vSwitch-2.
- 2 Create a port group.

- Include a string such as **unprotected** or **unprot** in the name for quick identification.
- 3 (Optional) Identify the VLAN IDs that can pass through the port group.
- 4 After the unprotected port group has been created, enable promiscuous mode for the port group.

Add the vShield Agent to the ESX Host

You must install the vShield agent using the vSphere Client before adding the vShield agent to the vShield Manager user interface. Manual vShield agent installation requires a vShield agent OVF.

To add a vShield agent manually to an ESX host

- 1 Log in to the vSphere Client and select the target ESX host from the inventory panel.
- 2 Select **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 agent OVF file.
- 4 Complete the wizard.
The vShield agent is installed into your inventory. You can follow the vShield agent installation steps from the Recent Tasks status pane located at the bottom of the vSphere Client window.
- 5 Install VMware Tools on the vShield agent virtual machine.

Assign the vShield Agent Interfaces to Port Groups

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

To assign the vShield agent interfaces to port groups

- 1 Log in to the vSphere Client.
- 2 Right-click the vShield agent virtual machine and click **Edit Settings**.
- 3 Click **Network adapter 1**.
This is the management interface of the vShield agent.
- 4 Assign a network label to Network adapter 1 that is reachable from the vShield Manager.
- 5 Click **Network adapter 2** and perform the following steps.
 - a Ensure that the **Connected** and **Connect at Power on** check boxes are selected.
 - b Under Network Connection, select the **Protected** port group from the **Network Label** drop-down list.
- 6 Click **Network adapter 3** and perform the following steps.
 - a Ensure that the **Connected** and **Connect at Power on** check boxes are selected.
 - b Under Network Connection, select the **Unprotected** port group from the **Network Label** drop-down list.
- 7 Click **OK**.

Set Up the vShield Agent

After assigning vShield agent interfaces, power on the vShield agent virtual machine and configure basic settings using the CLI.

To set up the vShield agent

- 1 Log in to the vSphere Client and power on the vShield agent.

The booting process might take a few minutes.

- 2 After a power up is complete, select the vShield agent from the inventory panel and click the **Console** tab.
- 3 At the `localhost` login prompt, log in to the CLI with the username **admin** and the password **default**.
- 4 Run the `setup` command to launch the CLI setup wizard.

The CLI setup wizard guides you through assigning an IP address for the management interface and identifying the default gateway IP address. The management interface IP address of the vShield agent 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.
```

```
vshield> exit
```

- 5 Log in to the CLI.
- 6 Ping the default gateway to verify network connectivity.

```
vShield> ping 10.115.219.253
```

- 7 Enter configuration mode.

```
vShield> enable
password:
vShield#
vShield# configure terminal
vShield(config)#
```

- 8 Enter interface configuration mode for the p0 interface.

```
vShield(config)# interface p0
vShield(config-if)#
```

- 9 Run the `no shutdown` command to activate the p0 interface.

```
vShield(config-if)# no shutdown
```

- 10 Quit interface configuration mode for the p0 interface.

```
vShield(config-if)# quit
```

- 11 Enter interface configuration mode for the u0 interface.

```
vShield(config)# interface u0
vShield(config-if)#
```

- 12 Run the `no shutdown` command to activate the u0 interface.

```
vShield(config-if)# no shutdown
```

- 13 Exit the CLI session.

Add the vShield Agent to the vShield Manager

You must add the vShield agent to the vShield Manager for configuration and data monitoring.

- 1 Open a Web browser and log in to the vShield Manager.
- 2 In the inventory panel, click **Settings & Reports**.
- 3 On the **Configuration** tab, click **Manual Install**.
- 4 Click **Add**.
- 5 Complete the form.

Field	Action
Name	Type the name you entered for the vShield agent when you deployed the OVF in the vSphere Client.
IP Address	Type the IP address assigned to the vShield agent.
Location	Type a description of where the vShield agent resides.
Key	Type the Manager key value entered using the CLI setup command. If you did not enter a key during CLI setup, leave this field blank.
Clustering Settings	Select Standalone to add a vShield agent that is not within a cluster.

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

The vShield Manager communicates with the vShield agent to complete the installation.

Move the Virtual Machines from First vSwitch to the Second vSwitch

After vShield agent installation is complete, move the virtual machines from vSwitch-1 to vSwitch-2 for protection.

Installing a vShield Agent Manually on a vNetwork Distributed Switch

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



CAUTION When installing a vShield agent in a vNDS environment, there will be network downtime for virtual machines during the transition of the physical NICs.

The following overview describes the manual installation process. The overview assumes you have deployed a vNetwork Distributed Switch with at least one attached vNIC, 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. See [“Create a Second vNetwork Distributed Switch”](#) on page 37.
- 2 Create two dvPort groups:
 - Protected: See [“Create the Protected dvPort Group on the First vNetwork Distributed Switch”](#) on page 37.
 - Unprotected: See [“Create the Unprotected dvPort Group on Second vNetwork Distributed Switch”](#) on page 37.
- 3 Install the vShield agent. See [“Install the vShield Agent”](#) on page 38.
- 4 Connect the vShield agent network adapters to the Protected and Unprotected dvPort groups. You must also connect the management interface of the vShield agent to a port group that is reachable from the vShield Manager. See [“Assign the vShield Agent Interfaces to the dvPort Groups”](#) on page 38.

- 5 Power off the vShield agent virtual machine. [“Power Off the vShield Agent Virtual Machine”](#) on page 40.
- 6 Remove the physical NICs from vNDS-1 and add them to vNDS-2. [“Move the Physical NICs from vNDS-1 to vNDS-2”](#) on page 40.
- 7 Power on the vShield agent virtual machine. See [“Power On the vShield Agent Virtual Machine”](#) on page 41

Create a Second vNetwork Distributed Switch

You must create a second vNetwork Distributed Switch. This switch is referred to as vNDS-2.

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 On the **Getting Started** tab, click **Add a vNetwork Distributed Switch** under Basic Tasks.
- 3 In the **Name** text box, enter a name for the new vNetwork Distributed Switch.
- 4 For the **Number of Uplink Ports** option, select **1** and click **Next**.
When creating the uplink port group, create enough slots for all hosts and participating NICs.
- 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**.
When the warning appears to verify your decision to not include any physical adapters, click **Yes**.
- 7 Click **Finish**.

Create the Protected dvPort Group on the First vNetwork Distributed Switch

You must add the protected dvPort group on the first vNetwork Distributed Switch. This switch is referred to as vNDS-1.

To create the protected dvPort group

- 1 Log in to the vSphere Client and select vNDS-1 from the inventory panel.
- 2 On the **Getting Started** tab, click **Create a new port group**.
- 3 In the **Name** text box, enter a name for the dvport group.
Include a string such as **protected** or **prot** in the name for quick identification.
- 4 (Optional) Identify the VLAN IDs that can pass through the port group.
- 5 Click **Next** and then click **Finish**.
- 6 After the protected port group has been created, enable promiscuous mode for the port group.

Create the Unprotected dvPort Group on Second vNetwork Distributed Switch

You must add the unprotected dvPort group on the second vNetwork Distributed Switch.

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 agent to see all passing traffic.

To create the unprotected dvPort group

- 1 Log in to the vSphere Client and select vNDS-2 from the inventory panel.
- 2 On the **Getting Started** tab, click **Create a new port group**.

- 3 In the **Name** text box, enter a name for the dvPort group.
Include a string such as **unprotected** or **unprot** in the name for quick identification.
- 4 (Optional) Identify the VLAN IDs that can pass through the port group.
- 5 Click **Next** and then click **Finish**.
- 6 After the unprotected port group has been created, enable promiscuous mode for the port group.

Install the vShield Agent

You must install the vShield agent by using the vSphere Client before adding the agent to the vShield Manager user interface. The installation requires a vShield agent OVF.

To add a vShield agent manually

- 1 Log in to the vSphere Client and select an ESX host from the inventory panel.
- 2 Select **File > Deploy OVF Template**.
- 3 Click **Deploy from file** and click **Browse** to locate the folder on your client machine containing the vShield agent OVF file.
- 4 Complete the wizard.
The vShield agent is installed into your inventory. You can follow the vShield agent installation steps from the Recent Tasks status pane located at the bottom of the vSphere Client window.
- 5 Install VMware Tools on the vShield agent virtual machine.

Assign the vShield Agent Interfaces to the dvPort Groups

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

To assign the vShield agent interfaces to port groups

- 1 Log in to the vSphere Client.
- 2 Right-click the vShield agent virtual machine and click **Edit Settings**.
- 3 Click **Network adapter 1**.
This is the management interface of the vShield agent.
- 4 Assign a network label to Network adapter 1 that is reachable from the vShield Manager.
- 5 Click **Network adapter 2** and perform the following steps:
 - a 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.
- 6 Click **Network adapter 3** and perform the following steps:
 - a 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.
- 7 Click **OK**.

Set Up the vShield Agent

After assigning vShield agent interfaces, power on the vShield agent virtual machine and configure basic settings by using the CLI.

To set up the vShield agent

- 1 Log in to the vSphere Client and power on the vShield agent.

The booting process might take a few minutes.

- 2 After a power up is complete, select the vShield agent from the inventory panel and click the **Console** tab.
- 3 At the `localhost login` prompt, log in to the CLI with the username **admin** and the password **default**.
- 4 Run the `setup` command to launch the CLI setup wizard.

The CLI setup wizard guides you through assigning an IP address to the management interface and identifying the default gateway IP address. The management interface IP address of the vShield agent 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.
```

```
vshield> exit
```

- 5 Log in to the CLI.
- 6 Ping the default gateway to verify network connectivity.

```
vShield> ping 10.115.219.253
```

- 7 Enter configuration mode.

```
vShield> enable
password:
vShield#
vShield# configure terminal
vShield(config)#
```

- 8 Enter interface configuration mode for the p0 interface.

```
vShield(config)# interface p0
vShield(config-if)#
```

- 9 Run the `no shutdown` command to activate the p0 interface.

```
vShield(config-if)# no shutdown
```

- 10 Quit interface configuration mode for the p0 interface.

```
vShield(config-if)# quit
```

- 11 Enter interface configuration mode for the u0 interface.

```
vShield(config)# interface u0
vShield(config-if)#
```

- 12 Run the `no shutdown` command to activate the u0 interface.

```
vShield(config-if)# no shutdown
```

- 13 Exit the CLI session.

Add the vShield Agent to the vShield Manager

You must add the vShield agent to the vShield Manager to manage the vShield agent and activate enforcement of firewall rules.

- 1 Open a Web browser and log in to the vShield Manager.
- 2 In the inventory panel, click **Settings & Reports**.
- 3 On the **Configuration** tab, click **Manual Install**.
- 4 Click **Add**.
- 5 Complete the form.

Field	Action
Name	Type the name you entered for the vShield agent when you deployed the OVF in the vSphere Client.
IP Address	Type the IP address assigned to the vShield agent.
Location	Type a description of where the vShield agent resides.
Key	Type the Manager key value entered using the CLI setup command. Leave this field blank to use the default key.
Clustering Settings	Select Standalone to add a vShield agent that is not within a cluster.

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

The vShield Manager communicates with the vShield agent to complete the installation.

Power Off the vShield Agent Virtual Machine

After the vShield agent installation is complete, power off the vShield agent virtual machine to prevent a network loop.

Move the Physical NICs from vNDS-1 to vNDS-2

After the vShield agent has been installed and connected, you move the physical NICs from vNDS-1 to vNDS-2. To do this, you must remove the NICs from vNDS-1 and add them to vNDS-2.

To you move the virtual machines from vNDS-1 to vNDS-2

- 1 Log in to the vSphere Client and select vNDS-1 from the inventory panel.
 - 2 On the **Configuration** tab, click **Networking**.
 - 3 Select the vNetwork Distributed Switch view.
 - 4 Click **Manage Physical Adapters**.
 - 5 Click **Remove** next to the uplink to remove.
 - 6 Click **OK**.
- Repeat for each physical NIC that must be moved.
- 7 Select vNDS-2 from the inventory panel.
 - 8 On the **Configuration** tab, click **Networking**.
 - 9 Select the vNetwork Distributed Switch view.
 - 10 Click **Manage Physical Adapters**.
 - 11 Click **Click to Add NIC** next to the uplink port to which to add an uplink.
 - 12 Select the physical adapter to add.

If you select an adapter that is attached to another switch, it is removed from that switch and reassigned to this vNetwork Distributed Switch.

13 Click **Select**.

14 Click **OK**.

Repeat for each physical NIC that must be moved.

Power On the vShield Agent Virtual Machine

After all of the NICs have been moved, power on the vShield agent virtual machine.

Uninstalling a vShield Agent

Uninstalling a vShield agent removes the agent from the network. There are three methods for installing a vShield agent.

- [“Uninstall a Template-Based vShield Agent”](#) on page 41
- [“Uninstall a Manually Installed vShield Agent from a vSwitch”](#) on page 41
- [“Uninstall a Manually Installed vShield Agent from a vNDS”](#) on page 41

Uninstall a Template-Based vShield Agent

Each template-based vShield agent has an **Uninstall vShield** tab.

To uninstall a template-based vShield agent

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

The vShield agent is uninstalled.

Uninstall a Manually Installed vShield Agent from a vSwitch

You must manually uninstall a manually installed vShield agent. Uninstalling includes removing the agent from vSwitches.

To uninstall a manually installed vShield agent

- 1 Log in to the vSphere Client.
- 2 Move the virtual machines from the protected vSwitch to the unprotected vSwitch.
- 3 Log in to the vShield Manager.
- 4 Click the root folder from the inventory panel.
- 5 On the **Configuration** tab, click **Manual Install**.
- 6 Select the check box for the vShield agent and click **Remove**.
- 7 Click **OK** in the pop-up window.

The vShield agent is uninstalled.

- 8 In the vSphere Client, remove the protected and unprotected port groups.

Uninstall a Manually Installed vShield Agent from a vNDS

You must manually uninstall a manually installed vShield agent. Uninstalling includes removing the agent from vNetwork Distributed Switch environments.

To uninstall a manually installed vShield agent

- 1 Log in to the vSphere Client.
- 2 Move the physical NICs from vNDS-2 to vNDS-1.
- 3 Log in to the vShield Manager.
- 4 Click the root folder from the inventory panel.
- 5 On the **Configuration** tab, click **Manual Install**.
- 6 Select the check box for the vShield agent and click **Remove**.
- 7 Click **OK** in the pop-up window.
The vShield agent is uninstalled.
- 8 In the vSphere Client, remove the protected and unprotected port groups.
- 9 Remove vNDS-2.

Powering Off vShield Zones Virtual Machines

You can power off vShield Zones virtual machines at any time. The last saved configuration is used when the virtual machine is powered on again.



CAUTION If you power off a vShield agent, the traffic to virtual machines behind the vShield agent is blocked until the vShield agent is powered on or uninstalled.

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 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**.

vShield Agent Management

You can monitor the health of vShield agents by using the vShield Manager user interface and by sending vShield agent system events to a syslog server.

This chapter includes the following topics:

- [“Sending vShield Agent System Events to a Syslog Server”](#) on page 43
- [“Backing Up the Running CLI Configuration of a vShield Agent”](#) on page 43
- [“Viewing the Current System Status of a vShield Agent”](#) on page 44

Sending vShield Agent System Events to a Syslog Server

You can send vShield agent events to a syslog server.

To send vShield agent system events to a syslog server

- 1 Select a vShield agent 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 agent 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 agent events to up to five syslog instances.

Backing Up the Running CLI Configuration of a vShield Agent

The **CLI Configuration** option displays the running configuration of the vShield agent. 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 agent

- 1 Select a vShield agent 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 agent CLI at the Configuration mode prompt.

Viewing the Current System Status of a vShield Agent

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

To view the health of a vShield agent

- 1 Select a vShield agent 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 Agent to Synchronize with the vShield Manager”](#) on page 44
- [“Restarting a vShield Agent”](#) on page 44
- [“Viewing Traffic Statistics by vShield Agent Interface”](#) on page 44
- [“Downloading the Firewall Logs of a vShield Agent”](#) on page 45

Forcing a vShield Agent to Synchronize with the vShield Manager

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

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

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

Restarting a vShield Agent

You can restart a vShield agent to troubleshoot an operational issue.

To restart a vShield agent

- 1 Select a vShield agent 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 Agent Interface

You can view the traffic statistics for each vShield interface.

To view traffic statistics by vShield port

- 1 Select a vShield agent from the inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **System Status**.
- 4 Click an interface under the **Port** column to view traffic statistics.

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

Downloading the Firewall Logs of a vShield Agent

You can download a log of the firewall activity from a vShield agent. 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 agent

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

The vShield agent uploads the log to the vShield Manager.

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

Firewall Management

The primary function of a vShield agent 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:

- [“Using VM Wall”](#) on page 47
- [“Creating a Layer 4 Firewall Rule”](#) on page 48
- [“Creating a Layer 2/Layer 3 Firewall Rule”](#) on page 49
- [“Reverting to a Previous VM Wall Configuration”](#) on page 50
- [“Deleting a VM Wall Rule”](#) on page 50

Using VM Wall

VM Wall is a centralized, hierarchical firewall for virtual machine environments. VM Wall enables you to create rules that allow or deny access to and from your virtual machines. Each installed vShield agent enforces the VM Wall rules.

You can manage VM Wall rules at the datacenter and cluster levels to provide a consistent set of rules across multiple vShield agents 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 agents. 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 agent enforces VM Wall rules in top-to-bottom ordering. A vShield agent 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 agents therein. A cluster-level rule is only applied to the vShield agents 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 agents 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 agent 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 agent drops the session before it reaches its destination. If you change all of the default rules to deny any traffic, the vShield agent 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/nn)	IP address with netmask (nn) from which the communication originated
Source Port	Port or range of ports from which the communication originated. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.
Destination (A.B.C.D/nn)	IP address with netmask (nn) which the communication is targeting
Destination Application	The application on the destination the source is targeting
Destination Port	Port or range of ports which the communication is targeting. To enter a port range, separate the low and high end of the range with a colon. For example, 1000:1100.
Protocol	Transport protocol used for communication

You can add destination and source port ranges to a rule for dynamic services such as FTP and RPC, which require multiple ports to complete a transmission. If you do not allow all of the ports that must be opened for a transmission, the transmission fails.

To create a Layer 4 firewall rule

- 1 Select a datacenter or cluster resource from the inventory panel.
- 2 Click the **VM Wall** tab. By default, the **L4 Rules** option is selected.
- 3 Click an existing row in the appropriate section of the table.
The available sections are based on the resource selected from the inventory panel.
- 4 Click **Add**.
A new row is added at the bottom of the section.
- 5 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.
- 6 (Optional) With the new row selected, click **Up** to move the row up in priority.
- 7 (Optional) Select the **Log** check box to log all sessions matching this rule.
- 8 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 53.

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.

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

Criteria	Description
Source (A.B.C.D/nn)	IP address with netmask (nn) from which the communication originated
Destination (A.B.C.D/nn)	IP address with netmask (nn) which the communication is targeting
Protocol	Transport protocol used for communication

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 53.

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**.
- 5 Click **Commit**.

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 agent. 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 Layer 2/Layer 3 sessions.

This chapter includes the following topics:

- [“Using VM Flow”](#) on page 51
- [“Viewing a Specific Application in the VM Flow Charts”](#) on page 52
- [“Changing the Date Range of the VM Flow Charts”](#) on page 52
- [“Viewing the VM Flow Report”](#) on page 52
- [“Adding VM Wall Rules from the VM Flow Report”](#) on page 53
- [“Editing Port Mappings”](#) on page 54
- [“Deleting All Recorded Flows”](#) on page 54

Using VM Flow

The **VM Flow** tab displays throughput statistics as returned by all of the active vShield agents 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.

Application	Sessions	Packets	Bytes	VMWall
BLOCKED	62	11,987	5,982,523	
TCP	0	11,919	5,968,786	
DYNAMIC_TCP	0	6	288	
UDP	62	62	13,449	
ALLOWED	1387	472,821	34,862,050	
TCP	288	55,069	9,897,153	
INCOMING	118	6,622	1,917,119	
CATEGORIZED	118	6,622	1,917,119	
HTTPS	118	6,622	1,917,119	
CRM-WWW-01(192.168.100.111)	118	6,622	1,917,119	
192.168.100.21	118	6,622	1,917,119	
UNCATEGORIZED	0	0	0	
OUTGOING	0	0	0	
INTRA	170	48,447	7,980,034	
INTRA_HOST	0	0	0	
UDP	1091	1,325	107,549	
DYNAMIC_TCP	8	224	12,788	
ICMP	0	414,076	24,844,560	
ARP	0	2,127	0	

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 Layer 4 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.
The charts update to display the most current information for the last seven days. This might take several seconds.
- 3 Click **Show Report**.
- 4 Expand the firewall action list.
- 5 Expand the Layer 4 protocol list.
- 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 resource from the inventory panel.
- 2 Click the **VM Flow** tab.
- 3 Click **Delete All Flows**.
- 4 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, and provides a model for you to follow. You cannot edit or delete the default entries.

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

13

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

This chapter includes the following topics:

- [“Reading the Discovery Results Table”](#) on page 57
- [“Enabling Continuous Discovery”](#) on page 58
- [“Running an On-Demand Discovery of Virtual Machines”](#) on page 58
- [“Scheduling Periodic Discovery of Virtual Machines”](#) on page 59
- [“Terminating an In-Progress Discovery”](#) on page 59
- [“Stopping a Scheduled Discovery Scan”](#) on page 60
- [“Using VM Inventory to View Virtual Machine Details”](#) on page 60

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 compliment 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 agent. When continuous discovery is enabled, the vShield agent 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 agent 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 agent and the server being scanned.

To run an on-demand discovery of virtual machines

- 1 Select a vShield agent 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 agent 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 agent 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 agent from the inventory panel.
- 2 Click the **VM Discovery** tab.
- 3 Click **Results**.

- 4 In the **Status** column, search for an In Progress scan.
- 1 Select the check box next to the in-progress scan.
- 2 Click **Terminate** below the table.
- 3 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 agent 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 agent, 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 agent to identify the virtual machines and services in the protected zone. A vShield agent 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 agent 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 agents 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 Zones virtual machine contains a command line interface (CLI). This appendix details CLI usage and commands.

User management in the CLI is separate from user management in the vShield Manager user interface.

This appendix includes the following topics:

- [“Logging In and Out of the CLI”](#) on page 61
- [“CLI Command Modes”](#) on page 61
- [“CLI Syntax”](#) on page 62
- [“Moving Around in the CLI”](#) on page 62
- [“Getting Help within the CLI”](#) on page 62
- [“Securing CLI User Accounts and the Privileged Mode Password”](#) on page 63
- [“Command Reference”](#) on page 64

Logging In and Out of the CLI

Before you can run CLI commands, you must initiate a console session to a vShield Zones virtual machine. To open a console session within the vSphere Client, select the vShield Zones virtual machine from the inventory panel and click the **Console** tab. You can log in to the CLI by using the default user name **admin** and password **default**.

After you have assigned an IP address to the management interface of a vShield Zones virtual machine, you can also use SSH and Telnet to access the CLI.

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 the mode you are currently in.

- **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 system diagnostics. 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 utilities on a vShield Zones virtual machine. You can access Configuration mode from Privileged mode. From Configuration mode, you can enter Interface configuration mode.
- **Interface Configuration:** Interface Configuration mode commands allow you to change the configuration of virtual machine interfaces. For example, you can change the IP address and IP route for the management 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) <0-512> [word]
```

- Text and numerical values that must be entered are italicized.
- Multiple, required keywords or values are enclosed in parentheses and separated by a pipe character.
- Numerical ranges are enclosed in angle brackets.
- An 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 the pointer to beginning of the line.
CTRL+B or the left arrow key	Moves the 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 the pointer to end of the line.
CTRL+F or the right arrow key	Moves the pointer forward one character.
CTRL+K	Deletes all characters from the 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 the pointer to beginning of the line.
CTRL+W	Deletes the word to the left of pointer.
ENTER	Scrolls down one line.
ESC+B	Moves the pointer back one word.
ESC+D	Deletes all characters from the pointer to the end of the word.
ESC+F	Moves the 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 the pointer to the 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 the associated arguments of a keyword.
list	Displays the verbose options of all commands for the current mode.

Securing CLI User Accounts and the Privileged Mode Password

You must manage CLI user accounts separately on each vShield Zones virtual machine. By default, you use the admin user account to log in to the CLI of each vShield Zones virtual machine. The CLI admin account and password are separate from the vShield Manager user interface admin account and password. You should create a new CLI user account and remove the admin account to secure access to the CLI on each vShield Zones virtual machine.

User account management in the vShield Zones CLI conforms to the following rules.

- You can create CLI user accounts. Each created user account has administrator-level access to the CLI.
- You cannot change the password for any CLI user account. If you need to change a CLI user account password, you must delete the user account, and then re-add it with a new password.

The CLI admin account password and the Privileged mode password are managed separately. The default Privileged mode password is the same for each CLI user account. You should change the privileged mode password to secure access to the CLI configuration options.

IMPORTANT Each vShield Zones virtual machine has two built-in CLI user accounts for system use: nobody and vs_comm. Do not delete or modify these accounts. If these accounts are deleted or modified, the virtual machine will not work.

Adding a CLI User Account

You can add a user account with a strong password to secure CLI access to each vShield Zones virtual machine. After adding a user account, you should delete the admin user account.

- 1 Log in to the vSphere Client.
- 2 Select a vShield Zones virtual machine from the inventory.
- 3 Click the **Console** tab to open a CLI session.
- 4 Log in by using the admin account.


```
manager login: admin
password:
manager>
```
- 5 Switch to Privileged mode.


```
manager> enable
password:
manager#
```
- 6 Switch to Configuration mode.


```
manager# configure terminal
```
- 7 Add a user account.


```
manager(config)# user root password plaintext password
```
- 8 Save the configuration.


```
manager(config)# write memory
Building Configuration...
Configuration saved.
[OK]
```
- 9 Exit the CLI.


```
manager(config)# exit
manager# exit
```

Delete the admin User Account from the CLI

After adding a CLI user account, you can delete the admin user account to secure access to the CLI.

IMPORTANT Do not delete the admin user account until you add a user account to replace the admin account. This prevents you from being locked out of the CLI.

To delete the admin user account

- 1 Log in to the vSphere Client.
- 2 Select a vShield Zones virtual machine from the inventory.
- 3 Click the **Console** tab to open a CLI session.
- 4 Log in by using a user account other than admin.
- 5 Switch to Privileged mode.
- 6 Switch to Configuration mode.
- 7 Delete the admin user account.

```
manager(config)# no user admin
```
- 8 Save the configuration.
- 9 Run the exit command twice to log out of the CLI.

Change the CLI Privileged Mode Password

You can change the Privileged mode password to secure access to the configuration options of the CLI.

To change the Privileged mode password

- 1 Log in to the vSphere Client.
- 2 Select a vShield Zones virtual machine from the inventory.
- 3 Click the **Console** tab to open a CLI session.
- 4 Log in to the CLI.
- 5 Switch to Privileged mode.
- 6 Switch to Configuration mode.
- 7 Change the Privileged mode password.

```
manager(config)# enable password (hash | plaintext) password
```
- 8 Save the configuration.
- 9 Run the exit command twice to log out of the CLI.
- 10 Log in to the CLI.
- 11 Switch to Privileged mode by using the new password.

Command Reference

The command reference details each CLI command, including syntax, usage, and related commands.

- [Administrative Commands](#)
- [CLI Mode Commands](#)
- [Configuration Commands](#)
- [Debug Commands](#)
- [Show Commands](#)
- [Diagnostics and Troubleshooting Commands](#)
- [User Administration Commands](#)

- [Terminal Commands](#)
- [Deprecated Commands](#)

Administrative Commands

list

Lists all in-mode commands.

Syntax

list

CLI Mode

Basic, Privileged, Configuration, Interface Configuration

Example

```
vShieldMgr> list
enable
exit
list
ping WORD
quit
show interface
show ip route
ssh WORD
telnet WORD
telnet WORD PORT
traceroute WORD
...
```

reboot

Reboots a vShield Zones virtual machine. You can also reboot a vShield agent from the vShield Manager user interface. See [“Restarting a vShield Agent”](#) on page 44.

Syntax

reboot

CLI Mode

Privileged

Example

```
vShield# reboot
```

Related Commands

[shutdown](#)

shutdown

In Privileged mode, the `shutdown` command powers off the virtual machine. In Interface Configuration mode, the `shutdown` command disables the interface.

To enable a disabled interface, use “no” before the `command`.

Syntax

[no] shutdown

CLI Mode

Privileged, Interface Configuration

Example

```
vShield# shutdown
```

or

```
vShield(config)# interface mgmt
vShield(config-if)# shutdown
vShield(config-if)# no shutdown
```

Related Commands

[reboot](#)

CLI Mode Commands**configure terminal**

Switches to Configuration mode from Privileged mode.

Syntax

```
configure terminal
```

CLI Mode

Privileged

Example

```
vShield# configure terminal
vShield(config)#
```

Related Commands

[interface](#)

disable

Switches to Basic mode from Privileged mode.

Syntax

```
disable
```

CLI Mode

Basic

Example

```
vShield# disable
vShield>
```

Related Commands

[enable](#)

enable

Switches to Privileged mode from Basic mode.

Syntax

```
enable
```

CLI Mode

Basic

Example

```
vShield> enable
password:
vShield#
```

Related Commands

[disable](#)

end

Ends the current CLI mode and switches to the previous mode.

Syntax

```
end
```

CLI Mode

Basic, Privileged, Configuration, and Interface Configuration

Example

```
vShield# end
vShield>
```

Related Commands

■ [exit](#)

■ [quit](#)

exit

Exits from the current mode and switches to the previous mode, or exits the CLI session if run from Privileged or Basic mode.

Syntax

```
exit
```

CLI Mode

Basic, Privileged, Configuration, and Interface Configuration

Example

```
vShield(config-if)# exit
vShield(config)# exit
vShield#
```

Related Commands

■ [end](#)

■ [quit](#)

interface

Switches to Interface Configuration mode for the specified interface.

To delete the configuration of an interface, use “no” before the command.

Syntax

```
[no] interface (mgmt | p0 | u0)
```

Option	Description
mgmt	The management port on a vShield Zones virtual machine.
p0	vShield agent p0 interface.
u0	vShield agent u0 interface.

CLI Mode

Configuration

Example

```
vShield# configure terminal
vShield(config)# interface mgmt
vShield(config-if)#
or
vShield(config)# no interface mgmt
```

Related Commands

[show interface](#)

quit

Quits Interface Configuration mode and switches to Configuration mode, or quits the CLI session if run from Privileged or Basic mode.

Syntax

```
quit
```

CLI Mode

Basic, Privileged, and Interface Configuration

Example

```
vShield(config-if)# quit
vShield(config)#
```

Related Commands

- [end](#)
- [exit](#)

Configuration Commands**clear vmwall rules**

Resets the firewall rule set on a vShield agent to the default rule set. This is a temporary condition that can be used to troubleshoot firewall issues. You can restore the firewall rule set by performing a force sync operation for the vShield agent from the vShield Manager. For more information on forcing synchronization, see [“Forcing a vShield Agent to Synchronize with the vShield Manager”](#) on page 44.

Syntax

```
clear vmwall rules
```

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
manager# clear vmwall rules
```

Related Commands

- [show vmwall log](#)
- [show vmwall rules](#)

copy running-config startup-config

Copies the current system configuration to the startup configuration. You can also copy and save the running CLI configuration of a vShield agent from the vShield Manager user interface. See [“Backing Up the Running CLI Configuration of a vShield Agent”](#) on page 43.

Syntax

```
copy running-config startup-config
```

CLI Mode

Privileged

Example

```
manager# copy running-config startup-config
Building Configuration...
Configuration saved.
[OK]
```

Related Commands

- [show running-config](#)
- [show startup-config](#)

database erase

Erases the vShield Manager database, resetting the database to factory defaults. This command clears all configuration data from the vShield Manager user interface, including vShield agent configurations, event data, and so forth. The vShield Manager CLI configuration is not affected by this command.

Syntax

```
database erase
```

CLI Mode

Privileged

Usage Guidelines

vShield Manager CLI

Example

```
manager# database erase
```

enable password

Changes the Privileged mode password. You should change the Privileged mode password for each vShield Zones virtual machine. CLI user passwords and the Privileged mode password are managed separately. The Privileged mode password is the same for each CLI user account.

Syntax

enable password (hash | plaintext) *password*

Option	Description
hash	Masks the password by using the MD5 hash. You can view and copy the provided MD5 hash by running the <code>show running-config</code> command.
plaintext	Keeps the password unmasked.
<i>password</i>	Password to use. The default password is default.

CLI Mode

Configuration

Example

```
vShield# configure terminal
vShield(config)# enable password plaintext abcd123
```

Related Commands

- [enable](#)
- [show running-config](#)

hostname

Changes the name of the CLI prompt. The default prompt name for the vShield Manager is `manager`, and the default prompt name for the vShield agent is `vShield`.

Syntax

hostname *word*

Option	Description
<i>word</i>	Prompt name to use.

CLI Mode

Configuration

Example

```
vShield(config)# hostname vs123
vs123(config)#
```

ip address

Assigns an IP address to an interface. On the vShield Zones virtual machines, you can assign an IP addresses to the mgmt interface only.

To remove an IP address from an interface, use “no” before the command.

Syntax

[no] ip address *A.B.C.D/M*

Option	Description
<i>A.B.C.D</i>	IP address to use.
<i>M</i>	Subnet mask to use.

CLI Mode

Interface Configuration

Example

```
vShield(config)# interface mgmt
vShield(config-if)# ip address 192.168.110.200/24
```

or

```
vShield(config)# interface mgmt
vShield(config-if)# no ip address 192.168.110.200/24
```

Related Commands[show interface](#)**ip name server**

Identifies a DNS server to provide address resolution service. You can also identify one or more DNS servers by using the vShield Manager user interface. See [“Identifying DNS Services”](#) on page 16.

To remove a DNS server, use “no” before the command.

Syntax

```
[no] ip name server A.B.C.D
```

Option	Description
<i>A.B.C.D</i>	IP address to use.

CLI Mode

Configuration

Example

```
vShield(config)# ip name server 192.168.1.3
```

or

```
vShield(config)# no ip name server 192.168.1.3
```

ip route

Adds a static route.

To delete an IP route, use “no” before the command.

Syntax

```
[no] ip route A.B.C.D/M W.X.Y.Z
```

Option	Description
<i>A.B.C.D</i>	IP address to use.
<i>M</i>	Subnet mask to use.
<i>W.X.Y.Z</i>	IP address of network gateway.

CLI Mode

Configuration

Example

```
vShield# configure terminal
vShield(config)# ip route 0.0.0.0/0 192.168.1.1
```

or

```
vShield(config)# no ip route 0.0.0.0/0 192.168.1.1
```

Related Commands

[show ip route](#)

manager key

Sets a shared key for authenticating communication between a vShield agent and the vShield Manager. You can set a shared key on any vShield agent. This key must be entered in the vShield Manager user interface during vShield agent installation. If the shared key between a vShield agent and the vShield Manager is not identical, the agent cannot install and is inoperable.

Syntax

```
manager key key
```

Option	Description
<i>key</i>	The key that the vShield agent and vShield Manager must match.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# manager key abc123
```

Related Commands

[setup](#)

set clock

Sets the date and time. From the vShield Manager user interface, you can connect to an NTP server for time synchronization. All vShield agents use the NTP server configuration of the vShield Manager. You should use this command if you meet one of the following conditions.

- You cannot connect to an NTP server.
- You frequently power off and power on a vShield agent, such as in a lab environment. A vShield agent can become out of sync with the vShield Manager when it is frequently power on and off.

Syntax

```
set clock HH:MM:SS MM DD YYYY
```

Option	Description
<i>HH:MM:SS</i>	Hours:minutes:seconds
<i>MM</i>	Month
<i>DD</i>	Day
<i>YYYY</i>	Year

CLI Mode

Privileged

Example

```
vShield(config)# set clock 00:00:00 08 28 2009
```

Related Commands

- [ntp server](#)
- [show clock](#)
- [show ntp](#)

ntp server

Identifies a Network Time Protocol (NTP) server for time synchronization service. Initial NTP server synchronization might take up to 15 minutes. From the vShield Manager user interface, you can connect to an NTP server for time synchronization. See [“Setting the vShield Manager Date and Time”](#) on page 16.

All vShield agents use the NTP server configuration of the vShield Manager. You can use this command to connect a vShield agent to an NTP server not used by the vShield Manager.

To remove the NTP server, use “no” before the command.

Syntax

```
[no] ntp server (hostname|A.B.C.D)
```

Option	Description
<i>hostname</i>	Hostname of the NTP server.
<i>A.B.C.D</i>	IP address of NTP server.

CLI Mode

Configuration

Usage Guidelines

vShield agent CLI

Example

```
vShield# configure terminal
vShield(config)# ntp server 10.1.1.113
```

or

```
vShield# configure terminal
vShield(config)# no ntp server
```

Related Commands

[show ntp](#)

setup

Opens the CLI initialization wizard for vShield Zones virtual machine installation. You configure multiple settings by using this command. You run the **setup** command during vShield Manager installation and manual installation of vShield agents. Press ENTER to accept a default value.

Syntax

```
setup
```

CLI Mode

Basic

Usage Guidelines

The `Manager` key option is applicable to vShield agent setup only.

Example

```
manager(config)# setup
Default settings are in square brackets '[]'.
Hostname [manager]:
IP Address (A.B.C.D or A.B.C.D/MASK): 192.168.0.253
Default gateway (A.B.C.D): 192.168.0.1
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.

manager>
```

syslog

Identifies a syslog server to which a vShield Zones virtual machine can send system events. You can also identify one or more syslog servers by using the vShield Manager user interface. See [“Sending vShield Agent System Events to a Syslog Server”](#) on page 43.

To disable syslog export, use “no” before the command.

Syntax

```
[no] syslog (host | A.B.C.D)
```

Option	Description
<i>hostname</i>	Hostname of the syslog server.
<i>A.B.C.D</i>	IP address of syslog server.

CLI Mode

Configuration

Example

```
vShield(config)# syslog 192.168.1.2
```

Related Commands

[show syslog](#)

write

Writes the running configuration to memory. This command performs the same operation as the `write memory` command.

Syntax

```
write
```

CLI Mode

Privileged

Example

```
manager# write
```

Related Commands

[write memory](#)

write erase

Resets the CLI configuration to factory default settings.

Syntax

```
write erase
```

CLI Mode

Privileged

Example

```
manager# write erase
```

write memory

Writes the current configuration to memory. This command is identical to the `write` command.

Syntax

```
write memory
```

CLI Mode

Privileged, Configuration, and Interface Configuration

Example

```
manager# write memory
```

Related Commands

[write](#)

Debug Commands

debug copy

Copies one or all packet trace or tcpdump files and exports them to a remote server. You must enable the `debug packet capture` command before you can copy and export files.

Syntax

```
debug copy (scp|ftp) URL (packet-traces | tcpdumps) (filename | all)
```

Option	Description
scp	Use SCP as transport protocol.
ftp	Use FTP as transport protocol.
URL	Add a URL in the format <code>userid@<ip_address>:<directory></code> . For example: <code>admin@10.10.1.10:/tmp</code>
packet-traces	Copy and export packet traces.
tcpdumps	Copy and export system tcpdumps.
filename	Identify a specific packet trace or tcpdump file to export.
all	Copy and export all packet trace or tcpdump files.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# debug copy ftp 192.168.1.1 tcpdumps all
```

Related Commands

- [debug packet capture](#)
- [debug remove](#)
- [debug show files](#)

debug packet capture

Captures all packets processed by a vShield agent, similar to a tcpdump. Enabling this command can slow vShield agent performance. Packet debug capture is disabled by default.

To disable packet capture, use “no” before the command.

Syntax

```
[no] debug packet capture (segment 0 | interface (mgmt | u0 | p0)) [expression]
```

Option	Description
segment 0	The segment on the vShield agent for which the debug function captures tcpdump information. Segment 0 is the only active segment. Segments 1 and 2 have been deprecated.
interface (mgmt u0 p0)	The specific interface from which to capture packets. Interface p1, u1, p2, u2, p3, and u3 have been deprecated.
<i>expression</i>	A tcpdump-formatted string. You must use an underscore between words in the expression.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# debug packet capture segment 0 host_10.10.11.11_port_8
```

Related Commands

- [debug copy](#)
- [debug packet display interface](#)

debug packet display interface

Displays all packets captured by a vShield agent interface, similar to a tcpdump. Enabling this command can impact vShield agent performance.

To disable the display of packets, use “no” before the command.

Syntax

```
[no] debug packet display interface (mgmt | u0 | p0) [expression]
```

Option	Description
mgmt u0 p0	The specific interface from which to capture packets.
<i>expression</i>	A tcpdump-formatted string. You must use an underscore between words in the expression.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI.

Example

```
vShield# debug packet display interface mgmt host_10.10.11.11_and_port_80
```

Related Commands

[debug packet capture](#)

debug remove

Removes one or all packet trace or tcpdump files from a vShield agent.

Syntax

```
debug remove (packet-traces|tcpdumps) (filename|all)
```

Option	Description
packet-traces	Remove one or all packet trace files.
tcpdumps	Remove one or all tcpdump files.
<i>filename</i>	Identify a specific packet trace or tcpdump file to export.
all	Remove all packet trace or tcpdump files.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# debug remove tcpdumps all
```

Related Commands

- [debug copy](#)
- [debug packet capture](#)
- [debug show files](#)

debug service

Enables logging for a service, noting the specific engine for the service and the severity of events to log. You can run the `show services` command to view the list of running services.

To disable logging for a specific service, use “no” before the command.

Syntax

```
[no] debug service (ice|sysmgr|vdb|word) (low|medium|high)
```

Option	Description
<i>service</i>	Name of the service.
ice	vShield agent protocol decoding engine.

Option	Description
sysmgr	vShield agent system manager.
vdb	Deprecated.
<i>word</i>	Reserved for technical support.
low	Low severity events.
medium	Medium severity events.
high	High severity events.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# debug 2050001_SAFLOW-FTPD-Dynamic-Port-Detection sysmgr high
```

Related Commands

[show services](#)

debug service flow src

Debugs messages for a service that is processing traffic between a specific source-to-destination pair. You can run the `show services` command to view the list of running services.

To disable logging, use “no” before the command.

Syntax

```
[no] debug service flow src A.B.C.D/M:P dst W.X.Y.Z/M:P
```

Option	Description
<i>service</i>	The name of the service.
<i>A.B.C.D</i>	Source IP address to use.
<i>M</i>	Source subnet mask to use.
<i>P</i>	Source port to use.
<i>W.X.Y.Z</i>	Destination IP address of use.
<i>M</i>	Destination subnet mask to use.
<i>P</i>	Destination port to use.

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI. A source or destination value of 0.0.0.0/0:0 matches all values.

Example

```
vShield# debug 2050001_SAFLOW-FTPD-Dynamic-Port-Detection src 192.168.110.199/24:1234 dst
192.168.110.200/24:4567
```

Related Commands

[show services](#)

debug show files

Shows the packet trace or tcpdump files that have been saved.

Syntax

debug show files (packet-traces|tcpdumps)

Option	Description
packet-traces	copy and export packet traces
tcpdumps	copy and export system tcpdumps

CLI Mode

Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# debug show files tcpdumps
total 8.0K
-rw-r--r--  1 514 Jan 20 18:31 tcpdump.unprot
-rw-r--r--  1 514 Jan 20 18:31 tcpdump.prot
```

Related Commands

- [debug copy](#)
- [debug remove](#)

Show Commands**show alerts**

Shows system alerts as they relate to the protocol decoders or network events. If no alerts have been raised, no output is returned.

Syntax

show alerts (vulnerability|decoder|events)

Option	Description
vulnerability	Deprecated.
decoder	Alerts raised by protocol decoder errors.
events	Alerts raised by network events.

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show alerts events
IP address      HW type  Flags  HW address      Mask  Device
192.0.2.130     0x1      0x6    00:00:00:00:00:81  *    virteth1
192.168.110.1   0x1      0x2    00:0F:90:D5:36:C1  *    mgmt
```

show arp

Shows the contents of the ARP cache.

Syntax

```
show arp
```

CLI Mode

Basic, Privileged

Example

```
vShield# show arp
IP address      HW type      Flags      HW address      Mask      Device
192.0.2.130     0x1          0x6        00:00:00:00:00:81  *         virteth1
192.168.110.1   0x1          0x2        00:0F:90:D5:36:C1  *         mgmt
```

show clock

Shows the current time and date of the virtual machine. If you use an NTP server for time synchronization, the time is based on Coordinated Universal Time (UTC).

Syntax

```
show clock
```

CLI Mode

Basic, Privileged

Example

```
vShield# show clock
Wed Feb  9 13:04:50 UTC 2005
```

Related Commands

- [ntp server](#)
- [set clock](#)

show debug

Show the debug processes that are enabled. You must enable a debug path by running the `debug packet` or one of the `debug service` commands.

Syntax

```
show debug
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show debug
No debug logs enabled
```

Related Commands

- [debug service](#)
- [debug service flow src](#)

show ethernet

Shows Ethernet information for virtual machine interfaces.

Syntax

```
show ethernet
```

CLI Mode

Basic, Privileged

Example

```
vShield# show ethernet
Settings for mgmt:
  Supported ports: [ TP ]
  Supported link modes:  10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
  Supports auto-negotiation: Yes
  Advertised link modes:  10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
  Advertised auto-negotiation: Yes
  Speed: 100Mb/s
  Duplex: Full
```

show filesystem

Shows the hard disk drive capacity for a vShield Zones virtual machine. vShield agents have one disk drive; the vShield Manager has two disk drives.

Syntax

```
show filesystem
```

CLI Mode

Basic, Privileged

Example

```
vShield# show filesystem
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda3        4.9G  730M  3.9G  16% /
/dev/hda6        985M   17M  919M   2% /tmp
/dev/hda7        24G   1.7G  21G   8% /common
```

show gateway rules

Shows the current IP rules running on the vShield agent.

Syntax

```
show gateway rules
```

CLI Mode

Privileged

Example

```
vShield# show gateway rules
bufsz:8192 inadequate for all rules; new bufsz = 9980
size of rule_details = 36
Kernel Rules Begin

Proxy Id = 0, Service Name = proxy-unused, Num Threads = 0 ACTION=FORWARD
```

```

Proxy Id = 1, Service Name = proxy-zombie, Num Threads = 0 ACTION=FORWARD

Proxy Id = 2, Service Name = vproxy-forward-allow, Num Threads = 0 ACTION=VPROXY

Proxy Id = 3, Service Name = vproxy-reverse-allow, Num Threads = 0 ACTION=UNKNOWN

Proxy Id = 4, Service Name = vproxy-inverse-allow, Num Threads = 0 ACTION=UNKNOWN
...

```

show hardware

Shows the components of the vShield Zones virtual machine.

Syntax

```
show hardware
```

CLI Mode

Basic, Privileged

Example

```

manager# show hardware
-[0000:00]--+-00.0 Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge
              +-01.0-[0000:01]--
              +-07.0 Intel Corporation 82371AB/EB/MB PIIX4 ISA
              +-07.1 Intel Corporation 82371AB/EB/MB PIIX4 IDE
              +-07.3 Intel Corporation 82371AB/EB/MB PIIX4 ACPI
              +-07.7 VMware Inc Virtual Machine Communication Interface
              +-0f.0 VMware Inc Abstract SVGA II Adapter
              +-10.0 BusLogic BT-946C (BA80C30) [MultiMaster 10]
              +-11.0-[0000:02]----00.0 Intel Corporation 82545EM Gigabit Etherne
t Controller (Copper)
              +-15.0-[0000:03]--
...

```

show interface

Shows the status and configuration for all interfaces or a single interface. You can also view interface statistics for a vShield agent from the vShield Manager user interface. See [“Viewing the Current System Status of a vShield Agent”](#) on page 44.

Syntax

```
show interface [mgmt | p0 | u0]
```

Option	Description
mgmt	Management interface
p0	vShield agent P0 interface
u0	vShield agent port U0 interface

CLI Mode

Basic, Privileged

Example

```

manager# show interface mgmt
Interface mgmt is up, line protocol is up
index 1 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:9e:7a:60
inet 10.115.216.63/22 broadcast 10.115.219.255
Auto-duplex (Full), Auto-speed (1000Mb/s)
input packets 5492438, bytes 2147483647, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0

```

```
output packets 2754582, bytes 559149291, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

Related Commands

[interface](#)

show ip route

Shows the IP routing table.

Syntax

```
show ip route [A.B.C.D/M]
```

Option	Description
<i>A.B.C.D</i>	IP address to use.
<i>M</i>	Subnet mask to use.

CLI Mode

Basic, Privileged

Example

```
vShield# show ip route
Codes: K - kernel route, C - connected, S - static,
       > - selected route, * - FIB route
```

```
S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt
```

Related Commands

[ip route](#)

show log

Shows the system log of all vShield agent activity.

Syntax

```
show log [follow | reverse]
```

Option	Description
follow	Update the displayed log every 5 seconds.
reverse	Show the log in reverse chronological order.

CLI Mode

Basic, Privileged

Example

```
vShield# show log
Aug  7 17:32:37 vShield_118 syslog-ng[27397]: Configuration reload request received, reloading
configuration;
Aug  7 17:32:37 vShield_118 udev[21427]: removing device node '/dev/vcsa12'
Aug  7 17:32:37 vShield_118 udev[21429]: removing device node '/dev/vcsa12'
Aug  7 17:32:37 vShield_118 udev[21432]: creating device node '/dev/vcs12'
Aug  7 17:32:37 vShield_118 udev[21433]: creating device node '/dev/vcsa12'
Aug  7 17:33:37 vShield_118 ntpdate[21445]: adjust time server 10.115.216.84 offset 0.011031 sec
Aug  7 17:34:37 vShield_118 ntpdate[21466]: adjust time server 10.115.216.84 offset 0.002739 sec
Aug  7 17:35:37 vShield_118 ntpdate[21483]: adjust time server 10.115.216.84 offset 0.010884 sec
```

...

Related Commands

- [show log alerts](#)
- [show log events](#)
- [show log last](#)

show log alerts

Shows the log of firewall rule alerts.

Syntax

```
show log alerts
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show log alerts
```

Related Commands

[show log](#)

show log events

Shows the log of vShield agent system events.

Syntax

```
show log events
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show log events
```

Related Commands

[show log](#)

show log last

Shows last *n* lines of the log.

Syntax

```
show log last n
```

Option	Description
<i>n</i>	number of log lines to display

CLI Mode

Basic, Privileged

Example

```
vShield# show log last 2
Feb  9 12:30:55 localhost ntpdate[24503]: adjust time server 192.168.110.199 off
set -0.000406 sec
Feb  9 12:31:54 localhost ntpdate[24580]: adjust time server 192.168.110.199 off
set -0.000487 sec
```

Related Commands

[show log](#)

show manager log

Shows the system log of the vShield Manager.

Syntax

```
show manager log [follow | reverse]
```

Option	Description
follow	Update the displayed log every 5 seconds.
reverse	Show the log in reverse chronological order.

CLI Mode

Basic, Privileged

Usage Guidelines

vShield Manager CLI

Example

```
vShield# show manager log
SEM Debug Nov 15, 2005 02:46:23 PM PropertyUtils Prefix:applicationDir

SEM Debug Nov 15, 2005 02:46:23 PM PropertyUtils Props Read:[]
SEM Info Nov 15, 2005 02:46:23 PM RefreshDb UpdateVersionNumbers info does not exist

SEM Debug Nov 15, 2005 02:46:23 PM RefreshDb Applications: []
SEM Info Nov 15, 2005 02:46:23 PM RefreshDb Compiler version pairs found: []
```

Related Commands

[show manager log last](#)

show manager log last

Shows the last *n* number of events in the vShield Manager log.

Syntax

```
show manager log last n
```

Option	Description
<i>n</i>	Number of events to display.

CLI Mode

Basic, Privileged

Usage Guidelines

vShield Manager CLI

Example

```
manager# show manager log last 10
```

Related Commands

[show manager log](#)

show ntp

Shows the IP address of the network time protocol (NTP) server. You set the NTP server IP address by using the vShield Manager user interface.

Syntax

```
show ntp
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield Manager CLI

Example

```
manager# show ntp
NTP server: 192.168.110.199
```

Related Commands

[ntp server](#)

show running-config

Shows the current running configuration.

Syntax

```
show running-config
```

CLI Mode

Basic, Privileged

Example

```
vShield# show running-config
Building configuration...
```

```
Current configuration:
!
segment 0 default bypass
!
```

Related Commands

- [copy running-config startup-config](#)
- [show startup-config](#)

show services

Shows the services protected by a vShield agent.

Syntax

```
show services
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI. In the example, 2050001_SAFLOW-FTPD-Dynamic-Port-Detection is the full name of a service. You must copy and paste this string into the `debug service` command as the service name.

Example

```
vShield# show services
nproxy_D_T_0001 is ACTIVE
 56 - 2050001_SAFLOW-FTPD-Dynamic-Port-Detection
 57 - 2050001_SAFLOW-MSRPC-Dynamic-Port-Detection
 58 - 2050001_SAFLOW-ORACLE-Dynamic-Port-Detection-Reverse
 59 - 2050001_SAFLOW-FTPD-Dynamic-Port-Detection-Reverse
 60 - 2050001_SAFLOW-SUNRPC-Dynamic-Port-Detection
 61 - 2050001_SAFLOW-MSRPC-Dynamic-Port-Detection-Reverse
 62 - 2050001_SAFLOW-SUNRPC-Dynamic-Port-Detection-Reverse
 63 - 2050001_SAFLOW-ORACLE-Dynamic-Port-Detection
 64 - 2050001_SAFLOW-Generic-Single-Session-Inverse-Attached
 65 - 2050001_SAFLOW-Generic-Single-Session-Forward-Attached
```

Related Commands

- 1 [debug service](#)
- 2 [debug service flow src](#)

show session-manager counters

Shows historical statistics on the sessions processed by a vShield agent, such as the number of SYNs received, the number of re-transmitted SYNs, and so forth.

Syntax

```
show session-manager counters
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show session-manager counters
sa_tcp_sockets_allocated_high_water_mark 8
sa_tcp_tw_count_high_water_mark 3
SA_TCP_STATS_OpenreqCreated 61
SA_TCP_STATS_SockCreated 61
SA_TCP_STATS_NewSynReceived 61
SA_TCP_STATS_RetransSynReceived 0
```

Related Commands

[show session-manager sessions](#)

show session-manager sessions

Shows the current sessions in process on a vShield agent.

Syntax

```
show session-manager sessions
```

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show session-manager sessions
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:2601            0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:7060            0.0.0.0:*              LISTEN
V_Listen
tcp        0      0 192.168.110.229:46132   0.0.0.0:*              LISTEN
```

Related Commands

[show session-manager counters](#)

show slots

Shows the software images on the slots of a vShield Zones virtual machine. Boot indicates the image that is used to boot the virtual machine.

Syntax

```
show slots
```

CLI Mode

Basic, Privileged

Example

```
manager# show slots

Recovery: System Recovery v0.3.2
Slot 1:   13Aug09-09.49PDT
Slot 2:   * 16Aug09-23.52PDT (Boot)
```

show stacktrace

Shows the stack traces of failed components. If no components have failed, no output is returned.

Syntax

```
show stacktrace
```

CLI Mode

Basic, Privileged

Example

```
vShield# show stacktrace
```

show startup-config

Shows the startup configuration.

Syntax

```
show startup-config
```


CLI Mode

Basic, Privileged

Example

```
vShield# show startup-config
```

Related Commands

- [copy running-config startup-config](#)
- [show running-config](#)

show syslog

Shows the syslog configuration.

Syntax

```
show syslog
```

CLI Mode

Basic, Privileged

Example

```
vShield# show syslog
*.* -/var/log/messages
*.emerg /dev/tty1
```

Related Commands

[syslog](#)

show system memory

Shows the summary of memory utilization.

Syntax

```
show system memory
```

CLI Mode

Basic, Privileged

Example

```
vShield# show system mem
MemTotal:      2072204 kB
MemFree:       1667248 kB
Buffers:       83120 kB
```

show system uptime

Shows the length of time the virtual machine has been operational since last reboot.

Syntax

```
show system uptime
```

CLI Mode

Basic, Privileged

Example

```
vShield# show system uptime
```

0 day(s), 8 hour(s), 50 minute(s), 26 second(s)

show version

Shows the software version currently running on the virtual machine.

Syntax

show version

CLI Mode

Basic, Privileged

Example

```
vShield# show version
```

show vmwall log

Shows the sessions that matched a firewall rule.

Syntax

show vmwall log [follow | reverse]

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show vmwall log
```

Related Commands

[show vmwall rules](#)

show vmwall rules

Shows the firewall rules that are active on the vShield agent.

Syntax

show vmwall rules

CLI Mode

Basic, Privileged

Usage Guidelines

vShield agent CLI

Example

```
vShield# show vmwall rules
Printing VMWall Rules and IP Lists...
```

Related Commands

- [clear vmwall rules](#)
- [show vmwall log](#)

Diagnostics and Troubleshooting Commands

export tech-support scp

Exports the system diagnostics to a specific location via Secure Copy Protocol (SCP). You can also export system diagnostics for a vShield Zones virtual machine from the vShield Manager user interface. See [“Downloading a Technical Support Log from a Component”](#) on page 17.

Syntax

```
export tech-support scp URL
```

Option	Description
<i>URL</i>	Enter the complete path of the destination.

CLI Mode

Basic and Privileged

Example

```
vShield# export tech-support scp user123@host123:file123
```

link-detect

Enables link detection for an interface. Link detection checks the status of an interface as enabled or disabled. Link detection is enabled by default.

To disable link detection for an interface, use “no” before the command.

Syntax

```
[no] link-detect
```

CLI Mode

Interface Configuration

Example

```
vShield(config-if)# link-detect
```

or

```
vShield(config-if)# no link-detect
```

ping

Pings a destination by its hostname or IP address.

Syntax

```
ping (hostname | A.B.C.D)
```

Option	Description
<i>hostname</i> <i>A.B.C.D</i>	The hostname or IP address of the target system.

CLI Mode

Basic, Privileged

Usage Guidelines

Enter CTRL+C to end ping replies.

Example

```
vShield# ping 192.168.1.1
```

show tech support

Shows the system diagnostic log that can be sent to technical support by running the `export tech-support scp` command.

Syntax

```
show tech support
```

CLI Mode

Basic, Privileged

Example

```
vShield# show tech support
```

Related Commands

[export tech-support scp](#)

ssh

Opens an SSH connection to a remote system.

Syntax

```
ssh (hostname | A.B.C.D)
```

Option	Description
<i>word</i>	Hostname or IP address of the target host.

CLI Mode

Basic, Privileged

Example

```
vShield# ssh server123
```

telnet

Opens a telnet session to a remote system.

Syntax

```
telnet (hostname | A.B.C.D) [port]
```

Option	Description
<i>hostname</i> <i>A.B.C.D</i>	The hostname or IP address of the target system.
<i>port</i>	Listening port on remote system.

CLI Mode

Basic, Privileged

Example

```
vShield# telnet server123
```

or

```
vShield# telnet server123 1221
```

traceroute

Traces the route to a destination.

Syntax

`traceroute (hostname | A.B.C.D)`

Option	Description
<i>hostname A.B.C.D</i>	The hostname or IP address of the target system.

CLI Mode

Basic, Privileged

Example

```
vShield# traceroute 10.16.67.118
traceroute to 10.16.67.118 (10.16.67.118), 30 hops max, 40 byte packets
 1  10.115.219.253 (10.115.219.253)  128.808 ms  74.876 ms  74.554 ms
 2  10.17.248.51 (10.17.248.51)  0.873 ms  0.934 ms  0.814 ms
 3  10.16.101.150 (10.16.101.150)  0.890 ms  0.913 ms  0.713 ms
 4  10.16.67.118 (10.16.67.118)  1.120 ms  1.054 ms  1.273 ms
```

User Administration Commands**default web-manager password**

Resets the vShield Manager user interface admin user account password to `default`.

Syntax

`default web-manager password`

CLI Mode

Privileged mode

Usage Guidelines

vShield Manager CLI

Example

```
manager# default web-manager password
Password reset
```

user

Adds a CLI user account. The user `admin` is the default user account. The CLI admin account and password are separate from the vShield Manager user interface admin account and password.

You cannot change the password for a CLI user. You must delete a user account and re-add it to change the password. If you must change a password, create a new user account to prevent CLI lockout.

IMPORTANT Each vShield Zones virtual machine has two built-in CLI user accounts for system use: `nobody` and `vs_comm`. Do not delete or modify these accounts. If these accounts are deleted or modified, the virtual machine will not work.

To remove a CLI user account, use “no” before the command.

Syntax

`[no] user username password (hash | plaintext) password`

Option	Description
<i>username</i>	Login name of the user.
<i>hash</i>	Masks the password by using the MD5 hash. You can view and copy the provided MD5 hash by running the <code>show running-config</code> command.
<i>plaintext</i>	Keeps the password unmasked.
<i>password</i>	Password to use.

CLI Mode

Configuration

Example

```
vShield(config)# user newuser1 password plaintext abcd1234
```

or

```
vShield(config) no user newuser1
```

web-manager

Starts the Web service on the vShield Manager. The Web service is started after the vShield Manager is installed.

To stop the web service (HTTP daemon) on the vShield Manager, use “no” before the command. This command makes the vShield Manager unavailable to Web Console browser sessions.

Syntax

```
[no] web-manager
```

CLI Mode

Configuration

Usage Guidelines

vShield Manager CLI. You can use this command after you have run the `no web-manager` command to stop and then restart the HTTP services of the vShield Manager.

Example

```
manager(config)# no web-manager
manager(config)# web-manager
```

Terminal Commands**clear vty**

Clears all other VTY connections to the CLI.

Syntax

```
clear vty
```

CLI Mode

Privileged

Example

```
manager# clear vty
```

reset

Resets the terminal settings to remove the current screen output and return a clean prompt.

Syntax

```
reset
```

CLI Mode

Basic, Privileged, Configuration

Example

```
manager# reset
```

Related Commands

- [terminal length](#)
- [terminal no length](#)

terminal length

Sets the number of rows to display at a time in the CLI terminal.

Syntax

```
terminal length <0-512>
```

Option	Description
0-512	Enter the number of rows to display. If length is 0, no display control is performed.

CLI Mode

Privileged

Example

```
manager# terminal length 50
```

Related Commands

- [reset](#)
- [terminal no length](#)

terminal no length

Negates the `terminal length` command.

Syntax

```
terminal no length
```

CLI Mode

Privileged

Example

```
manager# terminal no length
```

Related Commands

- [reset](#)
- [terminal length](#)

Deprecated Commands

The vShield Zones CLI contains commands that have been deprecated. The following table lists deprecated commands.

Table A-1. Deprecated Commands

Command
close support-tunnel
copy http URL slot (1 2)
copy http URL temp
copy scp URL slot (1 2)
copy scp URL temp
debug export snapshot
debug import snapshot
debug snapshot list
debug snapshot remove
debug snapshot restore
duplex auto
duplex (half full) speed (10 100 1000)
ip policy-address
linkwatch interval <5-60>
mode policy-based-forwarding
open support-tunnel
set support key
show raid
show raid detail

Using vMotion with vShield Zones

VMware 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 agent virtual machines.

This chapter includes the following topics.

- [“Preventing vMotion from Moving vShield Zones Virtual Appliances”](#) on page 97
- [“Permitting vMotion to Move Protected Virtual Machines”](#) on page 98

Preventing vMotion from Moving vShield Zones Virtual Appliances

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

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

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

- 1 Log in to the vSphere Client.
- 2 Right-click the cluster containing your vShield agent virtual machines and click **Edit Properties**.
The Admin Settings dialog box opens.
- 3 Under VMware HA, click **Virtual Machine Options**.
Locate the vShield agents in the list.
- 4 For each vShield agent, 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 agents in the list.
- 6 For each vShield agent virtual machine, select **Disabled** for **Automation Level**.
- 7 Click **OK** after all vShield agents have been configured.

Permitting vMotion to Move Protected Virtual Machines

By default, vShield agent 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 agents 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 agent 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 on the protected side of the vShield agent, and which does not home a physical NIC. In this case, the vShield agent 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**.

Using vShield Zones with Cisco Nexus 1000V Series Switches



You can deploy vShield Zones with Cisco® Nexus™ 1000V Series Switches. vShield Zones provides firewall protection to the virtual machines in Nexus 1000V Virtual Service Domains.

This chapter includes the following topics:

- [“About the Cisco Nexus 1000V”](#) on page 99
- [“Prerequisites”](#) on page 100
- [“Deploying vShield Zones”](#) on page 100

About the Cisco Nexus 1000V

Cisco Nexus 1000V Series Switches are virtual machine access switches that operate inside the ESX hypervisor of VMware vSphere environments. Developed in collaboration with VMware, the Cisco Nexus 1000V Series is certified by VMware to be compatible with VMware vSphere, vCenter, ESX, and ESXi, and with many other VMware vSphere features.

NOTE For more information on the Cisco Nexus 1000V, see http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/data_sheet_c78-492971.html.

The key components of the Nexus 1000V for vShield Zones integration are port profiles and Virtual Service Domains.

- *Port profiles* enable you to define and apply network policy to a group of virtual machines. You can use a port-profile, which is similar to a port group, to define configuration options as well as security and service level characteristics.
- *Virtual Service Domains (VSDs)* allows for grouping of one or more port profiles into one logical domain. The VSD allows for services that work in conjunction with Nexus 1000V, such as vShield Zones, to be integrated into the virtual environment and accessed by the individual VSDs.

Any set of port profiles can be separated using a VSD. The VSD can then be used to direct traffic to any service or entity within the environment.

The VSD feature allows insertion of the vShield agent in the forwarding path between protected guest virtual machines and the physical network outside of the ESX host. To accomplish this, you must configure port profiles that identify outside and inside virtual ports of the vShield agent, and the port profiles that home the guest virtual machines requiring firewall protection. The virtual switch ports on the Nexus 1000V that connect to the unprotected (outside) and protected (inside) interfaces of the vShield are marked with a given VSD name configuration. You can selectively mark port profiles to home virtual machines to participate in the newly configured VSD. If a VSD configuration is not tagged to a port profile, the traffic continues to forward normally.

After a virtual machine is placed into a protected zone, it does not have direct connectivity to the physical network. Every packet traversing the virtual machine passes through the vShield agent. The vShield agent has two logical interfaces: one in the VSD Inside interface, the other in the VSD Outside interface. These inside and outside interfaces as well as the ports connected to the virtual machines are the members of the VSD. This allows the vShield agent to provide firewall protection between the isolated inside network (where the virtual machines now reside) and the outside network.

A single VSD can service multiple VLANs to create logical zones using the same firewall appliance set. While a single VSD configuration addresses most environments, multiple VSD instances can be created on the Nexus 1000V to enable secure separation that requires more isolation by leveraging multiple vShield agents and separate physical network adapters for additional security.

Prerequisites

Before using vShield Zones in a Cisco Nexus 1000V environment, you must meet these requirements:

- You have already installed the Cisco Nexus 1000V software in a vCenter Server.
- You have already installed Cisco Nexus 1000V Virtual Ethernet Module (VEM) software on each ESX host.
- You have already verified that traffic is flowing to and from the virtual machines in your Nexus 1000V environment.

Deploying vShield Zones

You must complete the following steps to deploy the vShield Manager and at least one vShield agent in a Nexus 1000V environment.

- 1 [“Configure the Management Port Profile.”](#)
- 2 [“Configure VSD Port Profiles.”](#)
- 3 [“Configure VSD Member Virtual Machine Port Profiles.”](#)
- 4 [“Deploy the vShield Manager OVF.”](#)
- 5 [“Deploy the vShield Agent from OVF.”](#)
- 6 [“Assign the vShield Agent Interfaces to Port Profiles.”](#)
- 7 [“Set Up the vShield Agent.”](#)
- 8 [“Add the vShield Agent to the vShield Manager.”](#)

Configure the Management Port Profile

You must create a port profile, in this example vShield_mgmt, for the management interfaces of the vShield Manager and all deployed vShield agents. This port profile enables the vShield agents to communicate with the vShield Manager.

This configuration is equivalent to the vsmgmt port group used in ESX vSwitch installations.

```
port-profile vShield_mgmt
vmware port-group
switchport access vlan 123
no shutdown
state enabled
```

Configure VSD Port Profiles

You must create port profiles to separate the outside network from the inside network. The vShield agent sits in the path between these port profiles to monitor all transmissions between your virtual machines and the outside network.

In the following configurations, vsd1 is the name of the Virtual Service Domain.

This configuration is equivalent to creating the Protected port group on an ESX vSwitch.

```
port-profile vShield_Protected
vmware port-group
switchport mode trunk
    switchport trunk allowed vlan all
    virtual-service-domain vsd1
    service-port inside default-action-drop
no shutdown
state enabled
```

This configuration is equivalent to creating the Unprotected port group on an ESX vSwitch.

```
port-profile vShield_Unprotected
vmware port-group
switchport mode trunk
    switchport trunk allowed vlan all
    virtual-service-domain vsd1
    service-port outside default-action-drop
no shutdown
state enabled
```

Configure VSD Member Virtual Machine Port Profiles

This configuration is equivalent to moving virtual machines to a vSwitch on the Protected side of a vShield agent. The Virtual Service Domain name is vsd1, placing the virtual machines in the same logical domain as the vShield agent for protection.

```
port-profile Protected_VMs
vmware port-group
switchport access vlan 20
    virtual-service-domain vsd1
no shutdown
state enabled
```

Deploy the vShield Manager OVF

- 1 Log in to the vSphere Client.
- 2 Select an ESX host from the inventory panel.
- 3 Go to **File > Deploy OVF Template**.
The Deploy OVF Template wizard opens.
- 4 Click **Deploy from file** and click **Browse** to locate the folder on your PC containing the vShield Manager OVF file.
- 5 Complete the wizard.
The vShield Manager is installed into your inventory.
- 6 Edit the settings of the vShield Manager virtual machine to connect at power on and set the network label.
 - a Right-click the vShield Manager virtual machine and click **Edit Settings**.
The vShield Manager - Virtual Machine Properties dialog box opens.
 - b Under the **Hardware** tab, click **Network Adapter 1**.
 - c Select **Connect at power on** under Device Status.
 - d In the **Network label** drop-down list and select **vShield_mgmt**.
 - e Click **OK** to close the window.
- 7 Power on the vShield Manager virtual machine.
- 8 Click the **Console** tab from the right-hand pane to open the vShield Manager CLI.
The booting process might take a couple of minutes.

- 9 After the **manager** login prompt appears, log in to the CLI by using the username **admin** and the password **default**.
- 10 Run the **setup** command to launch the CLI setup wizard.

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

```
manager> setup
```

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

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

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

- 11 Ping the default gateway to verify network connectivity.

```
manager> ping 10.115.219.253
```
- 12 From your PC, ping the vShield Manager IP address to validate that the IP address is reachable.

Deploy the vShield Agent from OVF

- 1 Log in to the vSphere Client and select the target ESX host from the inventory panel.
- 2 Select **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 agent OVF file.
- 4 Complete the wizard.
The vShield agent is installed into your inventory. You can follow the vShield agent installation steps from the Recent Tasks status pane located at the bottom of the vSphere Client window.

Assign the vShield Agent Interfaces to Port Profiles

You must edit the virtual machine settings of the installed vShield agent to assign the agent interfaces to the Nexus 1000V port profiles. The vShield agent management interface must be in a port profile that is reachable from the vShield Manager. You can create a port profile or assign the management interface to the existing port profile vShield_mgmt.

To assign the vShield agent interfaces to port groups

- 1 Log in to the vSphere Client.
- 2 Right-click the vShield agent virtual machine and click **Edit Settings**.
- 3 Click **Network adapter 1** and assign **vShield_mgmt** to Network adapter 1.
This is the management interface of the vShield agent.
- 4 Click **Network adapter 2** and perform the following steps.
 - a Ensure that the **Connected** and **Connect at Power on** check boxes are selected.
 - b Under Network Connection, select the **vShield_Protected** port profile from the **Network Label** drop-down list.

- 5 Click **Network adapter 3** and perform the following steps.
 - a Ensure that the **Connected** and **Connect at Power on** check boxes are selected.
 - b Under Network Connection, select the **vShield_Unprotected** port group from the **Network Label** drop-down list.
- 6 Click **OK**.

Set Up the vShield Agent

After assigning vShield agent interfaces, power on the vShield agent virtual machine and configure basic settings using the CLI.

To set up the vShield agent

- 1 Log in to the vSphere Client and power on the vShield agent.
The booting process might take a few minutes.
- 2 After a power up is complete, select the vShield agent from the inventory panel and click the **Console** tab.
- 3 At the `localhost login` prompt, log in to the CLI with the username **admin** and the password **default**.
- 4 Run the `setup` command to launch the CLI setup wizard.

The CLI setup wizard guides you through assigning an IP address for the management interface and identifying the default gateway IP address. The management interface IP address of the vShield agent 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.
```

```
vshield> exit
```

- 5 Log in to the CLI.
- 6 Ping the default gateway to verify network connectivity.

```
vShield> ping 10.115.219.253
```

- 7 Enter configuration mode.

```
vShield> enable
password:
vShield#
vShield# configure terminal
vShield(config)#
```

- 8 Enter interface configuration mode for the p0 interface.

```
vShield(config)# interface p0
vShield(config-if)#
```

- 9 Run the `no shutdown` command to activate the p0 interface.

```
vShield(config-if)# no shutdown
```

- 10 Quit interface configuration mode for the p0 interface.

```
vShield(config-if)# quit
```

- 11 Enter interface configuration mode for the u0 interface.

```
vShield(config)# interface u0
vShield(config-if)#
```

- 12 Run the `no shutdown` command to activate the u0 interface.

```
vShield(config-if)# no shutdown
```

- 13 Exit the CLI session.

Add the vShield Agent to the vShield Manager

You must add the vShield agent to the vShield Manager for configuration and data monitoring.

- 1 Open a Web browser and log in to the vShield Manager.
- 2 In the inventory panel, click **Settings & Reports**.
- 3 On the **Configuration** tab, click **Manual Install**.
- 4 Click **Add**.
- 5 Complete the form.

Field	Action
Name	Type the name you entered for the vShield agent when you deployed the OVF in the vSphere Client.
IP Address	Type the IP address assigned to the vShield agent.
Location	Type a description of where the vShield agent resides.
Key	Type the Manager key value entered using the CLI <code>setup</code> command. If you did not enter a key during CLI setup, leave this field blank.
Clustering Settings	Select Standalone to add a vShield agent that is not within a cluster.

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

The vShield Manager communicates with the vShield agent to complete the installation.

Troubleshooting

This section guides you through troubleshooting common vShield Zones issues.

This appendix covers the following topics:

- [“Troubleshooting Installation Issues”](#) on page 105
- [“Troubleshooting Operation Issues”](#) on page 107

Troubleshooting Installation Issues

vShield Zones OVF Files Extracted to a PC Where vSphere Client Is Not Installed

Problem

I obtained the vShield Zones OVF files and downloaded them to my PC. If I do not have the vSphere Client on my PC, how do I install vShield Zones?

Solution

You must have the vSphere Client to install vShield Zones.

vShield Zones OVF File Cannot Be Installed in vSphere Client

Problem

When I try to install a vShield Zones OVF file, the install fails.

Solution

If a vShield Zones OVF file cannot be installed, an error window in the vSphere Client notes the line where the failure occurred. Send this error information with the vSphere Client build information to VMware technical support.

vShield Agent Virtual Machine Does Not Power On After OVF Is Installed

Problem

After I installed the vShield agent OVF, I tried to power on the vShield agent virtual machine. However, the virtual machine does not power on.

Solution

The vShield agent virtual machine has been built to remain in a powered off stage after OVF installation. The initial vShield agent virtual machine must be converted into a template so that all vShield agent installations can be installed automatically from the vShield Manager.

Cannot Log In to CLI After the vShield Manager Virtual Machine Starts

Problem

I cannot log in to the vShield Manager CLI after I installed the OVF.

Solution

Wait a few minutes after completing the vShield Manager installation to log in to the vShield Manager CLI. In the Console tab view, press Enter to check for a command prompt if the screen is blank.

Cannot Log In to the vShield Manager User Interface

Problem

When I try to log in to the vShield Manager user interface from my Web browser, I get a Page Not Found exception.

Solution

The vShield Manager IP address is in a subnet that is not reachable by the Web browser. The IP address of the vShield Manager management interface must be reachable by the Web browser to use vShield Zones.

Cannot See the vShield Agent Template from the vShield Manager User Interface

Problem

I created a template from the vShield agent virtual machine. However, when I used the vShield Manager user interface to install a vShield agent, I could not find a reference to the vShield agent template.

Solution

In the vSphere Client, power off the template and then power it on. If this does not work, delete the template and repeat the vShield agent OVF installation and template conversion processes. If this does not work, obtain a new vShield agent OVF.

vShield Agent Installation from vShield Manager User Interface Fails

Problem

My attempt to install a vShield agent from the vShield Manager user interface failed.

Solution

Typically, this is the result of no communication between the vShield Manager and the vShield agent during the installation process. If the vShield Manager IP address cannot ping the vShield agent IP address that you assigned, installation fails. However, the vShield Manager added port groups and a new vSwitch before testing connectivity. Your virtual machines are not affected, but you must delete the port groups and vSwitch that were created manually.

vShield Manager Cannot Communicate with a vShield Agent

Problem

I cannot configure a vShield agent from the vShield Manager.

Solution

If you cannot configure the vShield agent from the vShield Manager, there is a break in connectivity between the two. The vShield management interface cannot talk to the vShield Manager management interface. Make sure that the management interfaces are in the same subnet. If VLANs are used, make sure that the management interfaces are in the same VLAN.

Another reason could be that the vShield agent or vShield Manager virtual machine is powered off.

Troubleshooting Operation Issues

Cannot Configure a vShield Agent

Problem

I cannot configure a vShield agent.

Solution

This might be the result of one of the following conditions.

- The vShield agent virtual machine is corrupt. Uninstall the vShield agent from the vShield Manager user interface. Install a new vShield agent to protect the vSwitch.
- The vShield Manager cannot communicate with the vShield agent.
- The storage/LUN hosting the vShield configuration file has failed. When this happens, you cannot make any configuration changes. However, the firewall continues to run. You can store vShield Zones virtual machines to local storage if remote storage is not reliable.

Take a snapshot or create a TAR of the affected vShield agent by using the vSphere Client. Send this information to VMware technical support.

Firewall Block Rule Not Blocking Matching Traffic

Problem

I configured a VM Wall rule to block specific traffic. I used VM Flow to view traffic, and the traffic I wanted to block is being allowed.

Solution

Check the ordering and scope of the rule. This includes the container level at which the rule is being enforced. Issues might occur when an IP address-based rule is configured under the wrong container.

Check where the affected virtual machine resides. Is the virtual machine behind a vShield agent? If not, then there is no agent to enforce the rule. Select the virtual machine in the resource tree. The VM Wall tab for this virtual machine displays all of the rules that affect this virtual machine.

Place any unprotected virtual machines onto a vShield-protected switch or protect the vSwitch that the VM is on by installing a vShield.

Enable logging for the VM Wall rule in question. This might slow network traffic through the vShield agent.

Verify vShield agent connectivity. Check for the vShield agent being out of sync on the System Status page. If out of sync, click **Force Sync**. If it is still not in sync, go to the System Event log to determine the cause.

No Flow Data Displaying in VM Flow

Problem

I have installed the vShield Manager and a vShield agent. When I opened the VM Flow tab, I did not see any data.

Solution

This might be the result of one or more of the following conditions.

- You did not allow enough time for the vShield agent to monitor traffic sessions. Allow a few minutes after vShield agent installation to collect traffic data. You can request data collection by clicking **Get Latest** on the VM Flow tab.

- Traffic is destined to virtual machines that are not protected by a vShield agent. Make sure your virtual machines are protected by a vShield agent. Virtual machines must be in the same port group as the vShield agent protected (p0) port.
- There is no traffic to the virtual machines protected by a vShield agent.
- Check the system status of each vShield agent for out-of-sync issues.

Index

A

accessing online help **13**
adding a user **24**
admin user account **24**
Audit Logs **29**

B

Backup Configuration **43**
Backups
 on-demand **19**
 restoring **20**
 scheduling **20**
basic mode of CLI **61**

C

clear vmwall rules **68**
clear vty **94**
CLI
 backing up configuration **43**
 configuration mode **61**
 help **62**
 interface mode **61**
 logging in **61**
 modes **61**
 privileged mode **61**
 syntax **62**
Cluster Level Rules **48**
command syntax **62**
configuration mode of CLI **61**
configure terminal **66**
connecting to vCenter Server **15**
continuous discovery **58**
copy running-config startup-config **69**
Create User **24**

D

data
 on-demand backups **19**
 restoring a backup **20**
 scheduling backups **20**
Data Center High Precedence Rules **48**
Data Center Low Precedence Rules **48**
database erase **69**
date **16**
date range for VM Flow **52**
debug copy **75**

debug packet capture **76**
debug packet display interface **76**
debug remove **77**
debug service **77**
debug service flow src **78**
debug show files **79**
Default Rules **48**
default web-manager password **93**
deleting a port mapping **55**
deleting a user **25**
disable **66**
discovery **57**
 continuous **58**
 manual **58**
 periodic **59**
 removing a result **60**
 terminating **59**
DNS **16**
downloads
 firewall logs **45**

E

Edit Port Mappings **54**
 add a mapping **54**
 deleting **55**
 Hide Port Mappings **55**
editing a user account **24**
enable **66**
enable password **69**
end **67**
events
 sending as traps to SNMP server **43**
 sending to syslog **43**
 syslog format **28**
 system events **27**
 vShield events **28**
 vShield Manager events **27**
exit **67**
export tech-support scp **91**

F

firewall
 about **47**
 adding L2/L3 rules **49**
 adding L4 rules **48**
 adding rules from VM Flow **53**

- deleting rules **50**
- logs **45**
- planning rule enforcement **48**
- flow analysis date range **52**
- Force Sync **44**

H

- help **13**
 - CLI **62**
- Hide Port Mappings **55**
- hierarchy of VM Wall rules **48**
- history of updates **22**
- hostname **70**
- Hosts & Clusters view **14**
- HTTP Proxy **16**

I

- Install vShield **31**
- installation
 - vShield manually **33, 36**
- installing
 - updates **21**
 - vShield from template **31**
- interface **67**
- interface mode of CLI **61**
- inventory
 - panel **14**
 - VM Inventory **60**
- inventory panel **14**
- ip address **70**
- ip name server **71**
- ip route **71**

L

- L2/L3 rules
 - about **47**
 - adding **49**
- L4 rules
 - about **47**
 - adding **48**
- link-detect **91**
- list **65**
- login
 - CLI **61**
 - vShield Manager **13**
- logs
 - audit **29**
 - firewall **45**

M

- manager key **72**
- Manual Install **33, 36**

N

- Networks view **14**
- NTP **16**
- ntp server **73**

O

- on-demand discovery **58**
- online help **13**

P

- password **24**
- periodic discovery **59**
- ping **91**
- plug-in **17**
- port mappings **54**
 - add **54**
 - deleting **55**
 - hiding **55**
- privileged mode of CLI **61**
- proxy service **16**

Q

- quit **68**

R

- reboot **65**
- removing a discovery result **60**
- reports
 - audit log **29**
 - system events **27**
- reset **95**
- restarting a vShield **44**
- restoring backups **20**
- results of discovery **57**
- roles and rights
 - about **23**
 - assigning to a user **24**
- rules
 - adding L2/L3 rules to VM Wall **49**
 - adding L4 rules to VM Wall **48**
 - deleting VM Wall rules **50**

S

- scheduling backups **20**
- serial number of vShield Manager **17**
- services
 - DNS **16**
 - NTP **16**
 - proxy **16**
- set clock **72**
- setup **73**
- show alerts **79**
- show arp **80**

- show clock **80**
- show debug **80**
- show ethernet **81**
- show filesystem **81**
- show gateway rules **81**
- show hardware **82**
- show interface **82**
- show ip route **83**
- show log **83**
- show log alerts **84**
- show log events **84**
- show log last **84**
- Show Logs **45**
- show manager log **85**
- show manager log last **85**
- show ntp **86**
- Show Report **52**
- show running-config **86**
- show services **86**
- show session-manager counters **87**
- show session-manager sessions **87**
- show slots **88**
- show stacktrace **88**
- show startup-config **88**
- show syslog **89**
- show system memory **89**
- show system uptime **89**
- show tech support **92**
- show version **90**
- show vmwall log **90**
- show vmwall rules **90**
- shutdown **65**
- SNMP traps from a vShield **43**
- ssh **92**
- status
 - of a vShield **44**
 - of update **21**
 - of vShield Manager **17**
- syncing a vShield **44**
- syntax for CLI commands **62**
- syslog **74**
- syslog format **28**
- Syslog Servers **43**
- system events **27**
- System Status **44**
 - Force Sync **44**
 - Restart **44**
 - Show VM Wall Logs **45**
 - traffic stats **44**
- system time **16**

T

- telnet **92**

- terminal length **95**
- terminal no length **95**
- terminating a discovery **59**
- time **16**
- traceroute **93**
- traffic analysis date range **52**
- traffic stats for a vShield **44**
- Trap Destinations **43**

U

- Uninstall vShield **41**
- uninstalling a vShield **41**
- Update History **22**
- Update Status **21**
- Update User **24**
- Updates
 - installing **21**
 - Update History **22**
 - Update Status **21**
- user **93**
- user interface
 - logging in **13**
 - online help **13**

Users

- adding **24**
- admin account **24**
- assigning a role and rights **24**
- changing a password **24**
- deleting **25**
- editing **24**
- roles and rights **23**

V

- vCenter Server connection **15**
- vCenter tab **15**
- views
 - Hosts & Clusters **14**
 - Networks **14**
- VM Discovery
 - continuous **58**
 - manual **58**
 - periodic **59**
 - removing a result **60**
 - results **57**
 - terminating **59**
- VM Flow
 - adding a VM Wall rule **53**
 - date range **52**
 - show report **52**
- VM Inventory **60**
- VM Wall **47**
 - about L4 and L2/L3 rules **47**
 - adding L2/L3 rules **49**

- adding L4 rules **48**
- adding rules from VM Flow **53**
- deleting rules **50**
- hierarchy of rules **48**
- planning rule enforcement **48**

vMotion 97

vShield

- about **11**
- CLI configuration **43**
- discovery **57**
- firewall logs **45**
- forcing sync **44**
- installing from template **31**
- manual installation **33, 36**
- notification based on events **28**
- restarting **44**
- sending events as traps to SNMP **43**
- sending events to syslog **43**
- System Status **44**
- traffic stats **44**
- uninstalling **41**

vShield Manager

- about **11**
- accessing online help **13**
- date and time **16**
- DNS **16**
- inventory panel **14**
- logging in **13**
- Manual Install **17**
- notification based on events **27**
- NTP **16**
- on-demand backups **19**
- proxy service **16**
- restoring a backup **20**
- scheduling a backup **20**
- serial number **17**
- status **17**
- user interface panels **13**
- vSphere Plug-in **17**

vShield Zones

- vShield **11**
- vShield Manager **11**

vSphere Plug-in 17

W

- web-manager **94**
- write **74**
- write erase **75**
- write memory **75**