Symantec Critical System Protection 5.2.9 vSphere Support Guide

Symantec Critical System Protection 5.2.9 vSphere Support Guide

Documentation version: 5.2.9

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing Symantec Critical System Protection vSphere

This chapter includes the following topics:

About Symantec Critical System Protection vSphere

Symantec Critical System Protection provides intrusion prevention and detection features across a broad range of platforms and applications that include virtualized ecosystems. A virtualized ecosystem consists of many moving parts such as virtual guests, hypervisors, and management systems that span a variety of operating systems. In addition, it requires numerous software components to virtualize, operate, and manage the environment. To protect this diverse environment, Symantec Critical System Protection relies on specific policies and enforcement agents that are appropriate in securing each component.

See "About Symantec Critical System Protection vSphere architecture and components" on page 10.

See "About Symantec Critical System Protection vSphere Protection Policy" on page 35.

About Symantec Critical System Protection vSphere features

The vSphere support feature leverages and extends existing Symantec Critical System Protection prevention and detection capabilities to address specific vSphere applications and platforms. The key features of Symantec Critical System Protection vSphere include:

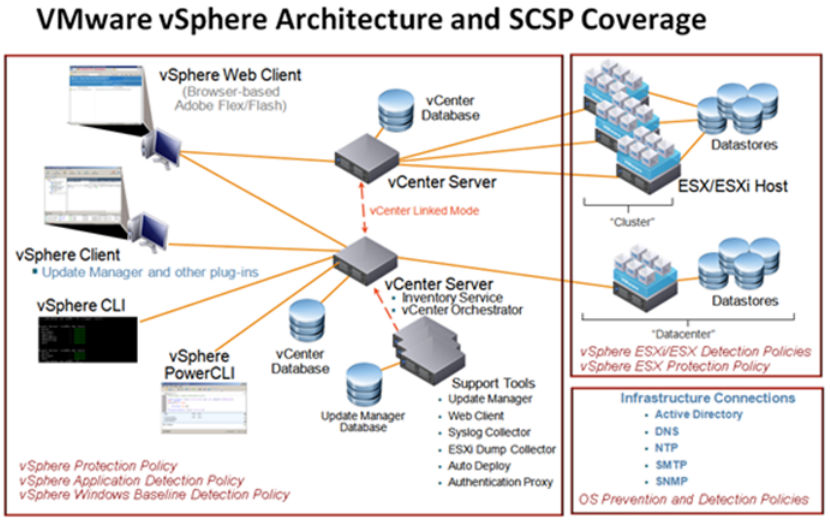
- Hardening and lockdown of vSphere management platforms that are specific to vSphere applications and resources such as files, registry, and network. This feature includes blocking unauthorized access to sensitive files such as SSL keys, tamper protection of binaries, configuration files and registry keys, data and logs, and control over privileged users and processes.
- The File Integrity Monitoring across vSphere components includes vCenter, utilities, clients, ESXi hosts, and VM guest configuration files.
- Log Monitoring directly at the source for ESX, ESXi, and vCenter, which includes login accesses and specific operational events of concern.
- Specific policy features that address VMware 4.1 Hardening Guideline requirements out of the box and ready to deploy, in addition to the standard regulatory compliance standards, such as PCI.
- vSphere-specific reporting for easy summarization and drill-down into events that occur across the virtualized environment.

See "About Symantec Critical System Protection vSphere architecture and components" on page 10.

About Symantec Critical System Protection vSphere architecture and components

Protecting a virtualized ecosystem requires that you address all the layers of the virtualization hierarchy. This includes the virtual guests, hypervisors, and management infrastructure, as well as all the supporting systems such as database, Active Directory , SMTP, SNMP, and so on.

Figure 1-1 A high level overview of the components in a typical VMware infrastructure and the applicable policies.



The key point is to address all the components in a virtualization hierarchy from VM guests to hypervisors to the management infrastructure and support systems such as database, Active Directory, SMTP, SNMP and so on.

Wherever a policy is applied, a Symantec Critical System Protection enforcement agent is in place. The agent turns the abstract rules into appropriate prevention or detection actions, which provides protection, visibility, and insight into security activities in the virtualized world. The ESXi platform provides a challenge to this processing model in that it follows a lightweight appliance model and does not support local agent installation. To address this challenge, an intermediate Symantec Critical System Protection Collector host should be created. This Collector host remotely does the file and log monitoring of the ESXi host by using VMware APIs.

The vSphere support solution supports a wide range of infrastructure components. It also has the ability to lock-down and securely manage the critical infrastructure components in the vSphere suite.

See "Installing a Symantec Critical System Protection Linux agent on the Collector host" on page 17.

See "Installing Symantec Critical System Protection agent in an ESX 4.1 host" on page 14.

Chapter 2

Planning the installation

This chapter includes the following topics:

System requirements

To use the Symantec Critical System Protection vSphere support package is available on the Symantec Critical System Protection 5.2.9 installation CD. The Symantec Critical System Protection vSphere support package supports the vSphere 5.0 infrastructure. The platform support is determined by the underlying systems that are supported by VMware vSphere 5.0 components. The vCenter support is limited to the Windows 2003/2008 (64-bit) operating systems.

As the ESXi 5 environment provides no means to install an agent, Symantec Critical System Protection accesses this platform by using the vSphere vCLI 5.0 APIs installed on an intermediary Symantec Critical System Protection Collector system. SLES 10 and 11 and Red Hat 5.5 are the supported intermediary platforms.

See "Installing a Symantec Critical System Protection Linux agent on the Collector host" on page 17.

See "Installing VMware vCLI package" on page 21.

About vSphere support package installation and configuration

You can install Symantec Critical System Protection components on the same computer or on different computers. All computers must run a supported operating system. Symantec Critical System Protection contains detection and prevention policies that you can use and customize to protect your network.

You can download the Symantec Critical System Protection installation CD from Symantec FileConnect Web site or you can request it from Symantec support.

Installing Symantec Critical System Protection agent in an ESX 4.1 host

The Symantec Critical System Protection installation CD comes with an agent installation binary that can be used to install on an ESX host.

Before you install the Symantec Critical System Protection ESX agent, you should note the following:

- You must install the ESX agents as root. ESX agents require root privileges to run.
- You must use the binary transfer mode when you transfer the ESX agent installation .bin files from a Windows computer to a Linux computer by using FTP or some other file transport method. Otherwise, the transfer corrupts the installation files.
- If you install the ESX agent on a system that supports non-english character sets, the destination directory that you choose for the agent must contain only ASCII characters. If you include any non-ASCII characters in the path, the installation fails.
- The communication ports between an agent and the management server must be available on the agent computer and must match the values that are used

during the management server installation. By default, the port settings are 443 and 2222.

- After you install the agent, you must use the management console to assign a prevention policy and one or more detection policies to the agent.
- Before you install an agent, you must place the SSL certificate on the computer that is targeted for installation. The certificate file `agent-cert.ssl` is located on the management server in the \Symantec\Critical System Protection\Server directory.

To place the certificate on a computer that is targeted for installation, do the following:

- On the management server that is used to manage the agent, locate the `agent-cert.ssl` file in the Symantec\Critical System Protection\Server directory.
- On the computer where the agent is installed, create a directory and then copy the `agent-cert.ssl` file into the directory by using FTP in binary mode or some other protocol. The directory path name cannot contain spaces.

To install the Symantec Critical System Protection agent in an ESX 4.1 host

1. Open a Terminal window and become superuser.
2. Insert the installation CD and if necessary, mount the volume.
3. Type and run the following command:

   ```
   cd /mnt/cdrom
   ```

4. Type and run the following command:

   ```
   ./agent64-esx4.bin
   ```

5. Follow the prompts until the installation completes.
6. Restart the computer if prevention was enabled.

See "About Symantec Critical System Protection Collector System setup" on page 16.

Importing Symantec Critical System Protection vSphere Policies

You can import the following workspace policies from the Symantec Critical System Protection 5.2.9 installation CD and use them in the extended vSphere environment:

- SCSPvSphereDetectionPolicyWorkspacePack-v5.2.9-m5.2.0-<sequence number>.zip
- SCSPvSpherePreventionPolicyWorkspacePack-v5.2.9-m5.2.0-<sequence number>.zip
- SCSPvSpherePreventionPolicyWorkspacePack-v5.2.9-m5.2.9-<sequence number>.zip

To import vSphere policies

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
   - **Prevention** view lets you import only Prevention policies.
   - **Detection** view lets you import only Detection policies.
3. On the **Policies** page, in the Policies tree, navigate to and select the folder and then right-click **Import Policy**.
4. In the **Import** dialog box, browse to the policy pack that you want to import.
5. Click **Import** to import the policy into the policy library.

   In the **Import** dialog box, each successfully imported policy is marked with a green check mark.

See "About vSphere queries and reports" on page 67.

See "About vSphere query and report customization" on page 70.

About Symantec Critical System Protection Collector System setup

In an ESX environment, you can install a native Symantec Critical System Protection agent and apply policies to monitor and protect the local host. However, ESXi does not allow agent installation or local enforcement. Instead, a Symantec Critical System Protection observer system is used to monitor the ESXi host remotely by using VMware-supported APIs and command line tools such as vCLI. This observer system is referred to as the Symantec Critical System Protection Collector host and is similar to the VMware Management Assistant (VMA). VMA is a virtual machine that manages agents that interact with ESXi hosts. VMA is not used because it no longer supports the capture of forwarded ESXi Syslog events and the choice of deployment scenarios is limited.

Symantec recommends that the Symantec Critical System Protection Collector system should be a single-purpose system that is dedicated to monitor a set of ESXi servers. The Symantec Critical System Protection Collector system contains

account and password information for the monitored ESXi servers, copies of ESXi server configuration files and logs, and VM guest configuration files. Therefore, you should limit login access to the Symantec Critical System Protection Collector system in the same way you limit login access to the ESXi servers or vCenter Servers. The ESXi credential store and other ESXi files are protected by operating system ACLs – only the root user has access to them. Symantec recommends you to use Symantec Critical System Protection Prevention and Detection policies for additional protection of the Collector host system, as you would with any other important server in the organization.

Symantec Critical System Protection Collector systems can be either SLES 10 (32-bit and 64-bit), SLES 11 (32-bit and 64-bit), or Red Hat 5.5 (32-bit and 64-bit). The Symantec Critical System Protection Collector system does not require many system resources. So, configuring it as a virtual machine makes the most sense from a manageability standpoint.

The Symantec Critical System Protection Collector system includes the following components:

- Base Linux Platform (SLES, RHEL)
- VMware vCLI
- Symantec Critical System Protection agent

After you install and configure the collector system components, you must apply the ESXi Detection policy to the Symantec Critical System Protection Collector host in addition to other prevention detection or prevention policies that your organization uses to protect the systems.

See "Installing a Symantec Critical System Protection Linux agent on the Collector host" on page 17.

Installing a Symantec Critical System Protection Linux agent on the Collector host

Before you install the Symantec Critical System Protection Linux agent, you should note the following:

- You must install the Linux agents as root. Linux agents require root privileges to run.
- You must use the binary transfer mode when you transfer the Linux agent installation .bin files from a Windows computer to a Linux computer by using FTP or some other file transport method. Otherwise, the transfer corrupts the installation files.

- If you install the Linux agent on a system that supports non-english character sets, the destination directory that you choose for the agent must contain only ASCII characters. If you include any non-ASCII characters in the path, the installation fails.
- The communication ports between an agent and the management server must be available on the agent computer and must match the values that are used during the management server installation. By default, the port settings are 443 and 2222.
- After you install the agent, you must use the management console to assign a prevention policy and one or more detection policies to the agent.
- Before you install an agent, you must place the SSL certificate on the computer that is targeted for installation. The certificate file `agent-cert.ssl` is located on the management server in the \Symantec\Critical System Protection\Server directory.

To place the certificate on a computer that is targeted for installation, do the following:

- On the management server that is used to manage the agent, locate the `agent-cert.ssl` file in the Symantec\Critical System Protection\Server directory.
- On the computer where the agent is installed, create a directory and then copy the `agent-cert.ssl` file into the directory by using FTP in binary mode or some other protocol. The directory path name cannot contain spaces.

To install the Symantec Critical System Protection Linux agent on the Collector host

1. Open a Terminal window and become superuser.
2. Insert the installation CD and if necessary, mount the volume.
3. Type and run the following command:

```
cd /mnt/cdrom
```

4 Type and run one of the following commands:

Red Hat Enterprise Linux ES 5 (32-bit)	`./agent-linux-rhel5.bin`
Red Hat Enterprise Linux ES 5 (64-bit)	`./agent64-linux-rhel5.bin`
SUSE Enterprise Linux 10 (32-bit)	`./agent-linux-sles10.bin`
SUSE Enterprise Linux 10 (64-bit)	`./agent64-linux-sles10.bin`
SUSE Enterprise Linux 11 (32-bit)	`./agent-linux-sles11.bin`
SUSE Enterprise Linux 11 (64-bit)	`./agent64-linux-sles11.bin`

5 Follow the prompts until the installation completes.

6 Restart the computer if prevention was enabled.

See "About Symantec Critical System Protection Collector System setup" on page 16.

About VMware vCLI installation

The Symantec Critical System Protection Collector host monitors the ESXi host by using VMware-supported, publicly available APIs and client access tools. The Symantec Critical System Protection ESXi support utility uses the VMware vCLI client access package to communicate with an ESXi host. Thus, you must install the VMware vCLI client access package before you use the Symantec Critical System Protection ESXi support utility.

The VMware vCLI interface on Linux depends on the Perl modules as well as a number of pre-requisite Linux software packages. The VMware vCLI installation procedure automatically downloads and installs all the required Perl modules. But, it does not automatically installs the required Linux software packages. You must ensure that these packages are installed before you run the VMWare vCLI installation procedure. For more information about installing the VMware vCLI installation, refer VMware documentation. The Symantec Critical System Protection ESXi support utility itself depends on some additional Perl modules. You must install the additional Perl modules on the Symantec Critical System Protection collector system.

For information about installing VMware CLI, refer to the VMware documentation.

You can download the VMware vCLI package from the following Web site:

Table 2-1 lists the Web addresses to download VMware components.

VMware components	Web address
VMware CLI documentation	http://pubs.vmware.com/vsphere-50/index.jsp?topic=/com.vmware.vcli.getstart.doc_50/cli_about.html
VMware CLI tool for Linux	http://www.vmware.com/support/developer/vcli/

The following items are Linux installer prerequisites:

- Perl 5.8.8 or 5.10
- OpenSSL (libssl-dev)
- LibXML2 2.6.26 or higher
- Uuid

The following Perl modules are prerequisites for the Symantec Critical System Protection ESXi support utility. You must ensure that these modules are present before you use the support utility.

- Date::Parse
- File::Copy
- File::Path
- File::Basename
- Sys::Hostname
- Text::CSV

To download a Perl module

- Open a terminal window, and run the following commands:

  ```
  cpan App::cpanminus
  ```

  ```
  cpanm <Module>::<Name>
  ```

  For example, `cpanm Date::Parse`

See "Installing vCLI prerequisite software" on page 20.

Installing vCLI prerequisite software

- Red Hat Enterprise Linux 5.5 (32-bit and 64-bit)

Symantec recommends that you install the prerequisites by using yum (the RHEL package installer) or from the installation DVD. For example,

```
yum install openssl-devel libxml2-dev e2fsprogs-dev
```

- SLES 10 (32-bit) and SLES 10 (64-bit)
  Install the prerequisite packages from the SLES 10/11 SDK DVD. When you insert the DVD, it opens auto-run. Cancel the auto-run dialog box and use the yast package installer to install OpenSSL and other required packages. For example:

  ```
  SLES 10, 64 bit. yast -I openssl-devel libxml2-devel-32bit
  e2fsprogs-devel-32bit
  SLES 10, 32 bit. yast -I openssl-devel libxml2-devel
  e2fsprogs-devel
  ```

  Note: SLES 10 includes libxml2 version 2.6.23. Since the vCLI client requires libxml2 version 2.6.26 or higher, you must upgrade to version 2.6.26 or higher.

- SLES 11 (32-bit) and SLES 11 (64-bit)
  Install the prerequisite packages from the SLES 10/11 SDK DVD. When you insert the DVD, it opens auto-run. Cancel the auto-run dialog box and use the yast package installer to install OpenSSL or other required packages. For example,

  ```
  SLES 11 64 bit. yast -I openssl-devel libuuid-devel
  libuuid-devel-32bit
  SLES 11 32 bit. yast -I openssl-devel libuuid-devel
  ```

  You can also download the required packages from alternative SLES repositories. For example, you can configure the download.opensuse.org repository for downloading packages. For example:
  http://download.opensuse.org/distribution/11.1/repo/oss/
  http://en.opensuse.org/Package_repositories

See "Installing VMware vCLI package" on page 21.

Installing VMware vCLI package

Before you install the vCLI package, you must install all the required software.

Note: A vCLI package installation may fail due to a missing dependency. You must identify the missing dependencies and install them manually.

To install the vCLI package

1. Log in as root.
2. Unzip the vCLI binary that you have downloaded.

   ```
   tar -zxvf VMware-vSphere-CLI-5.X.X-XXXXX.i386.tar.gz
   ```

   This creates a vmware-vsphere-vcli-distrib directory.
3. Optionally, if your server uses a proxy to access the Internet, and if your http:// and ftp:// proxy were not set when you installed the prerequisite software, set them now by using the following commands:

   ```
   export http_proxy=<proxy_server>:port
   ```

   ```
   export ftp_proxy=<proxy_server>:port
   ```
4. Run the installer by using the following command:

   ```
   /sudo vmware-vsphere-cli-distrib/vmware-install.pl
   ```

   For example:

   ```
   Creating a new vSphere CLI installer database using the tar4 format.
   Installing vSphere CLI 5.0.0 build-422456 for Linux.
   ```

5 Type **Yes** and press **Enter** to accept the license terms.

```
Do you accept? (yes/no) yes

Thank you.

Please wait while configuring CPAN ...

Please wait while configuring perl modules using CPAN ...

CPAN is downloading and installing pre-requisite Perl module "Archive::Zip" .

CPAN is downloading and installing pre-requisite Perl module
"Class::MethodMaker" .


This installer has successfully installed both vSphere CLI and the vSphere SDK
for Perl.

The following Perl modules were found on the system but may be too old to work
with vSphere CLI:

Compress::Raw::Zlib 2.017 or newer
ExtUtils::Installed 1.54 or newer
version 0.78 or newer
HTML::Parser 3.60 or newer
LWP::Protocol::https 5.805 or newer
```

6 Specify an installation directory or press **Enter** to accept the default directory.

By default, the installation directory is set to /usr/bin.

If you select the default installation directory, you can find the installed software at the following locations:

vCLI scripts	/usr/bin
vSphere SDK for Perl utility applications	/usr/lib/vmware-vcli/apps
vSphere SDK for Perl sample scripts	/usr/share/doc/vmware-vcli/samples
VMWare Perl modules	/usr/lib/vmware-vcli/VMware/share/VMware /usr/lib/perl5/5.10.0/VMware/

See "About VMware vCLI installation" on page 19.

See "Installing vCLI prerequisite software" on page 20.

About the Symantec Critical System Protection ESXi support utility

Remote File Synchronization (RFS) is a support utility tool that is installed on the Collector host to help the Symantec Critical System Protection agent monitor multiple ESXi hosts. Root users should use a setup script to configure RFS. RFS periodically synchronizes ESXi host configuration files, Virtual Machine Configuration files (VMX files), and selected ESXi log files. The local agent computer with policies applied performs the file integrity and log monitoring activities.

The files that are available for monitoring are specifically exposed by the VMware APIs. Not all the files that are visible when you log into the ESXi host are available for monitoring purposes.

RFS performs the following functions:

- Remote access to a designated ESXi host by using a VMware-encrypted credential store.
- Discovery and transfer of changed ESXi host configuration files.
- Discovery and transfer of changed ESXi host log files of interest to Symantec Critical System Protection ESXi detection policy.
- Discovery and detection of VMs that are registered or de-registered from the ESXi host.
- Discovery and transfer of changed Virtual Machine VMX configuration files for VMs that are registered with the ESXi host.

RFS is periodically executed based on a scheduled interval that is configured by the administrator. For example, the interval might be 10 minutes, 30 minutes, 2 hours and so on. After an initial one-time file population, only the files that are changed on the ESXi host are copied to the local Collector host.

Note: During the initial one-time file population, you may see a lot of **File Create** events in the console.

The ESXi Syslog log file is handled separately from RFS. Syslog configuration settings at the ESXi host are used to forward its Syslog to the Symantec Critical System Protection Collector node for monitoring purposes.

The Symantec Critical System Protection agent performs file integrity monitoring based on the mirrored files. Monitoring includes checking for changes in last modification date, size, name, and file content. The policy, as configured by the Symantec Critical System Protection console users, determines the event severity, rule name, and other parameters associated with FIM and log monitoring events. Each ESXi host can be viewed as a virtual agent on the 5.2.9 console. All the events generated for a particular ESXi host will be available to be viewed for that virtual agent.

See "Installing and setting up the ESXi support utility" on page 25.

Installing and setting up the ESXi support utility

To install and set up ESXi utility

1. The ESXi Support utility is installed as a part of Symantec Critical System Protection 5.2.9 agent installation on a Linux operating system. If you upgrade from a 5.2.8 agent to 5.2.9 agent, the ESXi support utility is automatically upgraded. The default directory for the ESXi support utility is:

   ```
   /opt/Symantec/scspagent/IDS/bin/esxi_fim
   ```

2. When you install ESXi support utility for the first time, open a terminal window, and run the following command located in the default directory:

   ```
   rfs_config.sh -setup
   ```

3. When prompted for a root directory, type a directory (that you have already created) where you want to store the ESXi host files that are retrieved by the tool. Update the conf/esxi_fim_root with an entry that identifies the directory for the FIM root.

4. When prompted for the synchronization interval, type a valid interval between 3 to 60 minutes. It adds a cron job to the root user's crontab to run the RFS utility based on the specified synchronization interval.

Note: If you want to create a synchronization interval of more than 60 minutes, type 60 when you run the setup, and then manually edit the cron-tab entry `/etc/crontab` fileto change the synchronization interval.

You can also run the setup silently by providing the above information in the following way:

```
rfs_config.sh -setup -fimpath <path for the root directory>
-syncinterval <interval in minutes>
```

5 To upgrade from a 5.2.8 agent to 5.2.9 agent with an ESXi support utility installed on 5.2.8 agent, open a terminal window and run the following command located in the default directory:

```
rfs_config.sh -upgrade
```

Note: Please install Perl module Text::CSV on the system before you run the upgrade. If you do not install this module, file monitoring of the ESXi host stops.

6 On an upgrade from 5.2.8 agent to 5.2.9 agent with no ESXi support utility installed on 5.2.8 agent, follow steps 2 to 4.

Note: The ESXi support utility will not work unless you have performed either steps 2 to 4 on a new install or step 5 on an upgrade.

When you install the ESXi support utility for the first time, you should apply the vSphere ESXi Detection Policy to start monitoring the ESXi Hosts. You can only apply the vSphere ESXi Detection Policy after you have run the setup.

When you upgrade from 5.2.8 agent to a 5.2.9 agent, you must re-apply the vSphere ESXi Detection Policy from the 5.2.9 Detection Policy Pack.

The ESXi support utility can now be configured to add, modify, delete, list ESXi Hosts.

After you provide all the values, the setup script configures the following settings on the local system:

- Updates the `conf/esxi_fim_host.conf` file by setting the ESXi_HOSTS entry to ESXi host name/IP address.
- Creates a credential store under `conf/esxi_fim_hostcred` by using a vCLI command. It also populates the store with an entry for the ESXi host and the user account credentials.
- If the Syslog mode is on:
  - Adds an entry in the `etc/syslog-ng/syslog-ng.conf` file to accept the forwarded syslogs from the ESXi host.
  - Configures the remote ESXi host to forward its events to the local collector by using a vCLI command.

Note: Syslog forwarding is done by UDP on port 514. Please ensure that the ESXi firewall does not block that port.

You can use the following options in place of OPTIONS in the `rfs_config.sh OPTIONS` command:

Table 2-2 List of options for the OPTIONS parameter

OPTIONS	Description
-help	Prints this message.
-version	Prints the RFS Package Version Information.
-setup	Runs interactive setup of the RFS utility (Default mode). Allows you to enter the directory where local copies of ESXi files are stored and the synchronization interval for these files. You can also run the setup via command line using the following options: ■ `-fimpath=<fimrootdir>` Set the directory where local copies of ESXi files are stored. The default directory path is /fim. ■ `-syncinterval=<mins>` Set the synchronization interval in minutes. By default, the synchronization interval is 30 minutes. For example, `rfs_config.sh -setup -fimpath=<fimrootdir> -syncinterval=<mins>` **Note:** The directory specified to store the local copies of the ESXi files are appended with a the path `/scspfim`. Therefore, the local files are stored in the directory `<fimrootdir>/scspfim`. Each ESXi host that is being monitored has its own sub-directory under `<fimrootdir>/scspfim`. When you uninstall, it removes the `/scspfim` folder.

Table 2-2 List of options for the OPTIONS parameter *(continued)*

OPTIONS	Description
-addHost	

Table 2-2 List of options for the OPTIONS parameter *(continued)*

OPTIONS	Description

	Adds a new ESXi Host to monitor.
	`rfs_config.sh -addHost <Mandatory Options> [Optional Options]`
	Following are the supported options:
	■ -server=<IP address or host name>
	Set the ESXi Server Address. This option is mandatory.
	■ -username=<user>
	Set the ESXi Username. This option is mandatory.
	■ -password=<passwd>
	Set the password for the ESXi user. This option is mandatory.
	■ -protocol=<protocol>
	Set the protocol (https or http) for RFS to use to communicate with ESXi server. The default protocol is https. This option is optional.
	■ -port=<port>
	Set the port to use to communicate with the ESXi server. The default port number is 443. Valid port number range from 1 to 65535. This option is optional.
	■ -syslogon
	Enable ESXi Syslog forwarding. This is the default value. This option is optional.
	■ -syslogoff
	Disable ESXi Syslog forwarding. This option is optional.
	For example:
	`rfs_config.sh -addHost -server=<addr> -username=<user> -password=<passwd>`
	`rfs_config.sh -addHost -server=<addr> -username=<user> -password=<passwd> -protocol=<protocol> -port=<port>`
	`rfs_config.sh -addHost -server=<addr> -username=<user> -password=<passwd> -protocol=<protocol> -port=<port> -syslogoff`
	Note: When you add a host, verify if the syslog messages are reported from the ESXi host that contain IP address or host name as the source. Depending on the ESXi host, use either the IP address or the host name.
	Note: The server information that is used here < IP address or

Table 2-2 List of options for the OPTIONS parameter *(continued)*

OPTIONS	Description
	host name> is used to name the Virtual Agent that contains the logs.

-modifyHost	Allows you to modify ESXi Host Information. Specify the ESXi Host that should be modified.
	`rfs_config.sh -modifyHost <Mandatory Options> [Optional Options]`
	Following are the supported options:
	■ -server=<addr>
	Set the ESXi Server Address. This option is mandatory.
	■ -username=<user>
	Set the ESXi Username. This option is optional.
	■ -password=<passwd>
	Set the password for the ESXi user. This option is optional unless you intend to change the username.
	■ -protocol=<protocol>
	Set the protocol (https or http) for RFS to use to communicate with ESXi server. The default protocol is https. This option is optional.
	■ -port=<port>
	Set the port to use to communicate with the ESXi server. The default port number is 443. Valid port number range from 1 to 65535. This option is optional.
	For example:
	`rfs_config.sh -modifyHost -server=<addr> -username=<user> -password=<passwd>`
	`rfs_config.sh -modifyHost -server=<addr> -protocol=<protocol>`

Table 2-2 List of options for the OPTIONS parameter *(continued)*

OPTIONS	Description

-deleteHost	Allows to delete a single ESXi host or all ESXi hosts.
	`rfs_config.sh -deleteHost <Mandatory Options>`
	Following are the supported options:
	■ -server=<addr>|all
	Set the ESXi Server Address. This option is mandatory.
	■ -username=<user>
	Set the ESXi Username. This option is mandatory. If you specify -server=all then you do not require the username.
	For example:
	`rfs_config.sh -deleteHost -server=<addr> -username=<user>`
	`rfs_config.sh -deleteHost -server=all`

-listHost	Allows to view all the ESXi hosts currently monitored. `rfs_config.sh -listHost`
-upgrade	Allows you to upgrade the older ESXi Support Utility to version 5.2.9.
-runrfs	Run the ESXi support utility on demand.

The ESXi Support Utility tool logs error messages during its scheduled execution to a file named RFS.log. You can find the `rfs.log` file in the same directory where the local copies of the ESXi host files are stored. Thesefiles are stored under a folder `SCSPCollectorNode_<Agent name given during the SCSP Agent Installation>`. The ESXi Detection policy provides an option to monitor error events recorded in the RFS.log and to send these events to the console. The error events are available as a different virtual agent of the same name as the folder.

To uninstall the ESXi support utility

The ESXi Support Utility (RFS - Remote File Synchronization Tool) runs at least once to get the ESXi host files and store it locally. However, to detect changes to those files, you must apply vSphere ESXi detection policy.

Note: If you have a vSphere ESXi detection policy already applied to the collector system. The first time you add a new ESXi host to monitor, you observe lot of file creation events on the console.

The ESXi support utility automatically gets uninstalled when you uninstall the Symantec Critical System Protection agent. As part of uninstall, it deletes all the files that were retrieved from the ESXi hosts. It also updates the syslog/syslog-ng files on the collector node to stop receiving forwarded events from the ESXi host and updates the syslog forwarding entries on the ESXi hosts. It removes all the credentials that are stored on the Symantec Critical System Protection collector system.

See "About the Symantec Critical System Protection ESXi support utility" on page 23.

Chapter 3

About Symantec Critical System Protection vSphere policies

This chapter includes the following topics:

About vSphere 5.0 vCenter, utilities, and clients

While the Symantec Critical System Protection agent provides the actual prevention and detection features for any endpoint, it is the out-of-the-box policy content and management framework that quickly addresses the compliance and security requirements of an organization. When an operating environment becomes more complex as is the case in a virtualized ecosystem, the need for security policy content to address the complexity becomes more acute. The Symantec Critical System Protection vSphere policy content is designed to address the key management, hypervisors, and client platforms operating in the environment.

To protect and secure VMware vCenter servers is critical to an enterprise, as these systems have complete access to all of the host systems, such as ESX or ESXi, and all virtual machines that it manages, which may number in the thousands.

VMware's own hardening guideline points out the critical nature of these central aggregation points and the need to protect and monitor the platform to the greatest extent possible.

VMware vCenter production systems run on Windows 64-bit server operating systems and thus are susceptible to many of the Windows vulnerabilities and threats. To address this need, specific protection and detection policies have been developed to harden these VMware management platforms and the software components that make up the vCenter software suite.

The Symantec Critical System Protection policy content addresses the vSphere 5.0 application management stack, which encompasses a number of components.

- vCenter Server, which includes the following components:
  - vCenter Orchestrator
  - Inventory Service
  - Profile Driven Storage
  - Tomcat
  - Jetty
  - Java Runtime Environment
- vCenter support tools, which include the following components:
  - VMware vSphere Authentication Proxy
  - VMware ESXi Dump Collector
  - VMware Syslog Collector
  - VMware Auto Deploy
- vSphere Service Utilities, which include the following components:
  - VMware vSphere Update Manager
  - VMware vSphere Web Client and Server
- vSphere Clients, which include the following components:
  - vSphere Client
  - vCenter Orchestrator Client
  - vSphere Update Manager Utility
  - vSphere PowerCLI
  - vSphere CLI (Windows)

The vSphere policies understand the applications location (binaries, configuration files, and registry locations) and the resources required, such as network access. However, it goes beyond basic tamper protection to control access to highly sensitive data such as certificates and to limit access by privileged users and programs. Users with appropriate administrative privileges can control and configure the vSphere policies based on simple lists. Users can also take advantage of the more advanced policy capabilities for more precise control.

About Symantec Critical System Protection vSphere Protection Policy

The vSphere Protection Policy is based on the out-of-the-box Symantec Critical System Protection Windows Strict Prevention Policy. However, its enhancements protect and control the vSphere applications by using two sandboxed process sets. One set protects vSphere services, the other, vSphere interactive client tools and utilities.

To address ease of policy configuration and management in large environments, specific task-focused vSphere lists are defined. These lists allow the administrator to quickly adjust the behavior controls as required. For example, network IP address lists are predefined to control communications over multiple vSphere ports to critical components. By configuring a few lists, the policy tightly controls the access between linked vCenter servers and access to its backend database, or between vCenter and the managed ESX and ESXi hosts. Even highly privileged system processes are not allowed to communicate to the critical resources unless they are specifically granted access in the policy.

The lists control which programs and users can access the vCenter master certificates and keys. In addition, the lists lock down the modification of vCenter binaries and configuration files. Users and programs must have specific access rights to change the vCenter binaries and configuration files. The policy is designed in such a manner that it can be immediately deployed on a vCenter platform with minimal tuning required. Symantec recommends that you deploy the policy in non-blocking mode initially until you test and approve it in your environment.

Following are the key features of vSphere Protection Policy:

- vSphere Tamper Protection (no unauthorized modification of files and registry)
  - vSphere binaries tamper protection
  - vSphere configuration files tamper protection
  - vSphere data, log, and SSL certificate tamper protection

    - Policy allows only vSphere programs (or trusted users, programs) to modify contents
- vSphere SSL certificate protection (no unauthorized access)
    - Policy globally denies access to all programs and users
    - Policy only allows access to vCenter programs and trusted users
    - Identified as a specific requirement in the VMware hardening guide
- Network Firewall
    - Reduces network attack surface area so that non-vSphere applications have very limited network access
    - Controls vSphere applications, network access so that inbound or outbound port usage is channeled to specifically intended remote systems. For example, the database ports communicate only with database hosts.
- Policy framework for easy customer modification
    - Policy is ready to be applied to vCenter servers (predefined programs and resources)
    - Re-use components for off-box utilities and client usage
    - Readily configurable

The following vSphere Hardening Requirements are either directly addressed or are compensated for by the control in Symantec Critical System Protection:

- VSH01 – Maintain supported operating system, database, and hardware for vCenter
  The vSphere Protection Policy provides system and application hardening even for the software that is not supported.
- VSH02 – Keep VMware center system properly patched
  The vSphere Protection Policy provides system and application hardening even for the software that is not properly patched.
- VSH03 – Provide Windows system protection on VMware vCenter server host
  The vSphere protection policy provides operating system level protection so that vulnerabilities can be mitigated and malware contained.
- VSH04 – Avoid user login to VMware vCenter server system
  The vSphere Protection Policy can restrict logins to authorized users that perform legitimate tasks and also limit their actions and privileged activity.
- VSH06 – Restrict usage of vSphere administrator privilege

The vSphere Protection Policy can limit privileged user activity so that vCenter privileges are given to specifically identified local accounts while also de-escalating normal administrator account privileges.

- VSH10 – Clean up log files after failed installations of VMware vCenter server
  The vSphere Protection Policy can act as a compensating control by locking down the install logs that contain sensitive data in plain text.
- VSC03 – Restrict access to SSL certificates
- VSC05 – Restrict network access to VMware vCenter server system
  The vSphere Protection Policy restricts access to only those components that are required to communicate with VMware vCenter.
- VSC06 – Block access to ports not being used by VMware vCenter
  The vSphere Protection Policy firewall rules implement this requirement explicitly.
- VUM02 – Keep Update Manager system properly patched
  The vSphere Protection Policy provides system and application hardening even for the software that is not supported.
- VUM03 – Provide Windows system protection on Update Manager system
  The vSphere Protection Policy provides operating system level protection so that vulnerabilities can be mitigated and malware contained.
- VUM04 – Avoid user login to Update Manager system
  The vSphere Protection Policy can restrict login to only those users that perform legitimate tasks and can limit their actions and privileged activity.

See "About configuring and using vSphere Protection Policy" on page 37.

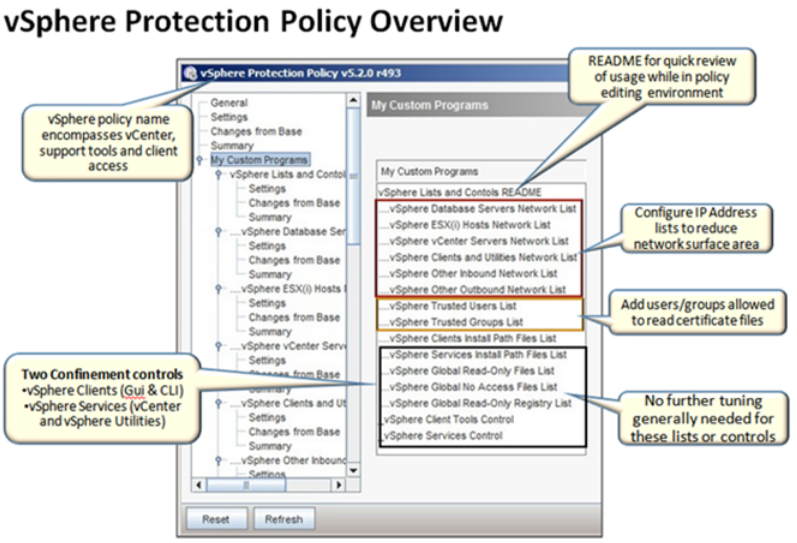
See "About Symantec Critical System Protection vSphere Detection Policies" on page 40.

About configuring and using vSphere Protection Policy

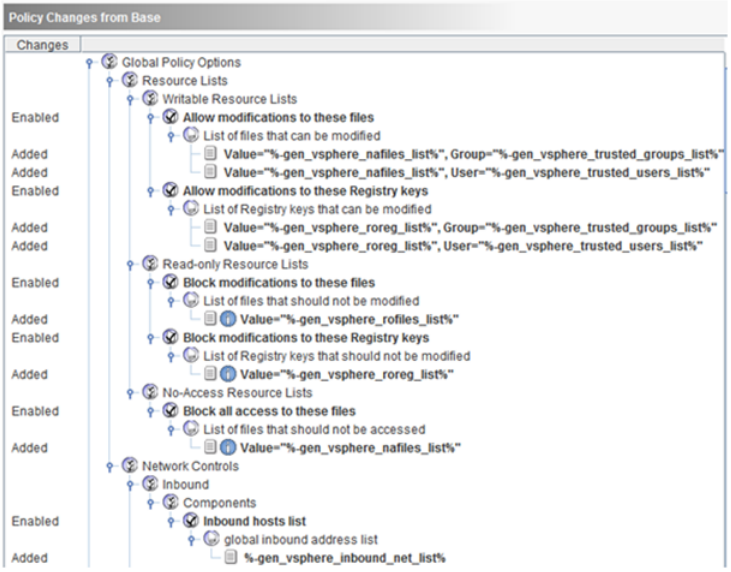
The combination of the stock primary policy components and vSphere-specific lists and settings immediately hardens a vSphere management system. You can also easily customize the policy's default settings. When you deploy the vSphere Protection Policy you should tighten down the default network IP address ranges. You should also identify the trusted users and groups that need access to the sensitive data, such as keys and certificates.

Note: Symantec recommends that you disable prevention until you have tested the policy in your environment.

Figure 3-1 vSphere Protection Policy custom programs and lists options



These lists are referenced in the main policy to protect vSphere resources. The following image displays the policy changes from baseline:



The vSphere Protection Policy tuning process includes the following steps:

Tuning 1: Network Surface Area

By default there are no predefined inbound or outbound network IP address range restrictions. To control the range of systems that can interact with the vSphere infrastructure, you should further restrict network lists for key components such as databases, vCenter servers, ESX/ESXi hosts, and vSphere client access systems.

Refine each of these network lists as required:

- ESX/ESXi hosts
- vCenter servers
- vSphere clients (GUI or CLI) and utilities (Update Manager, Syslog Collector, and so on)
- Other inbound and outbound systems such as AD, DNS, DHCP, NTP, SMTP, SNMP, and so on

Tuning 2: Trusted Access to SSL certificates

This policy blocks global access to vSphere SSL certificates except for vSphere services, safe or full privileged users, and groups or programs. In the rare instance where a user, group, or program without privileges needs to access this sensitive data, you can use the vSphere Trusted Users List or vSphere Trusted Groups List to make an exception. Additional custom list settings, such as installation paths and global data access file lists are static and do not need further tuning in the policy unless required.

Tuning 3: Base Windows Policy Tuning for your environment

Finally, you should apply the same basic tuning that you use for other Windows systems, such as the following steps:

- Define trusted programs and administrators for system updates
- Override users and groups
- Base platform networking

While the vSphere Protection Policy is designed to be all inclusive and integrated with the main policy controls, you can also re-use some or all of the custom components. For example, you can copy the Custom Programs and Lists into your own Windows Strict Policy and then reference the lists either the same or differently than the behavior in the vSphere default policy.

See "About Symantec Critical System Protection vSphere Protection Policy" on page 35.

About Symantec Critical System Protection vSphere Detection Policies

The vSphere Detection Policies can be quickly deployed on your virtualization infrastructure setup to provide file integrity monitoring and log monitoring.

Symantec Critical System Protection includes the following two vSphere Detection Policies:

- **vSphere Windows Baseline Detection Policy**
  This policy is based on the default Windows Baseline Detection Policy but with the default settings tightened down. The two policies provide the same functionality, including Windows operating system File and Registry Integrity Monitoring and Windows Event Log Monitoring. For the vSphere management platform, the vSphere Windows Detection Policy detects failed login attempts, creation or modification of local user accounts or groups, changes to audit subsystem and some other events detected on these key systems. If your organization already uses a well-defined Windows Baseline Detection Policy, you may decide to use or modify your own policy to maintain consistency across the Windows servers.
- **vSphere Application Detection Policy**
  This policy is based on the Windows Template Policy and thus uses the custom rules to add specific FIM and log monitoring for vSphere application and log files. It also helps to address specific regulatory requirements and VMware hardening requirements.

Table 3-1 lists the vSphere ESXi Detection Policy features.

Table 3-1 Symantec Critical System Protection vSphere Detection Policy features

vSphere Detection Policy	Features
Windows operating system RT-FIM, Registry, Audit, Event, and Log Monitoring	■ Preconfigured settings that are suitable for the vCenter platform ■ Option to customize further or use your own Baseline policy that is already in use on other platforms
vSphere Real-Time File and Registry Integrity Monitoring	■ vSphere binaries (more than traditional executables) ■ vSphere configuration and files ■ Reports detailed file changes, including the user and program that makes the change

Table 3-1 Symantec Critical System Protection vSphere Detection Policy features *(continued)*

vSphere Detection Policy	Features
VMware unique hardening requirements	■ vCenter SSL Certificate Files Usage monitoring (VSC02) ■ vCenter Using Built-in Windows account (VSH05)
vSphere General Log Monitoring	Monitoring of vCenter vpxd log (main vCenter interaction log)
Framework for easy customer modification	■ Little tuning required Ready to be applied to vCenter servers with programs, resource, and exceptions predefined. ■ Readily configurable and easy to integrate with any existing policies

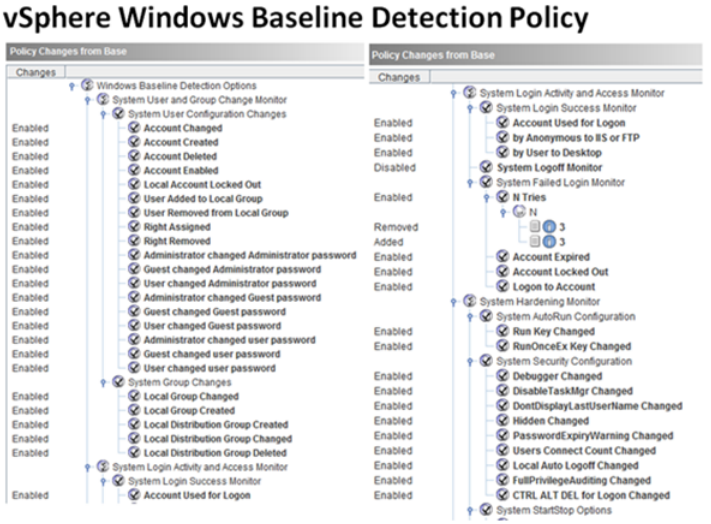
See "About configuring and using vSphere Detection Policies" on page 41.

See "About Symantec Critical System Protection vSphere Protection Policy" on page 35.

About configuring and using vSphere Detection Policies

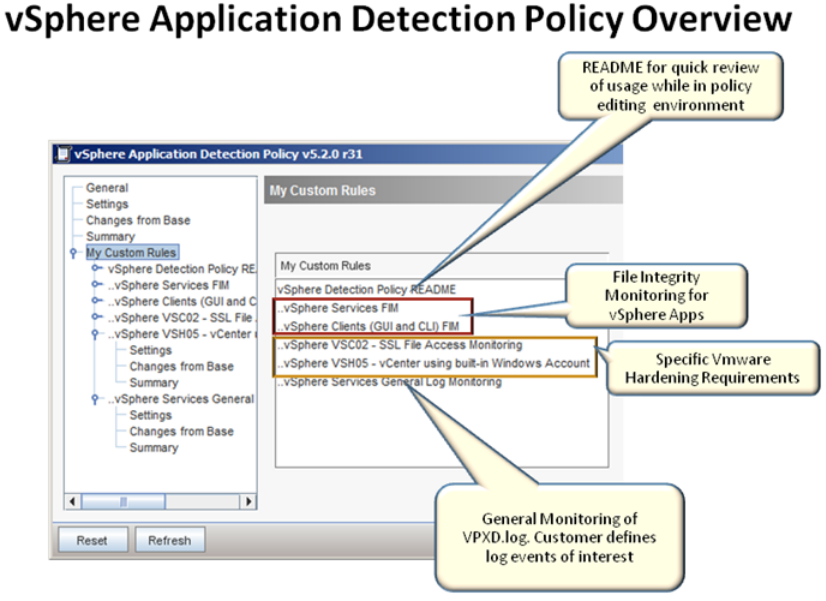
The following illustration shows changes from Baseline for the vSphere Windows Baseline Detection Policy.

Figure 3-2 Baseline changes in the vSphere Windows Baseline Detection policy



The following illustration shows the custom rules that are defined in the vSphere Application Detection Policy.

Figure 3-3 Custom rules defined in the vSphere Application Detection policy



The custom detection rules are designed to work with a Windows Baseline Detection Policy to monitor a vSphere application infrastructure. You can also easily customize its default settings.

The custom detection rules are designed to provide the following functionality:

- Perform File Integrity Monitoring of vSphere binaries and configuration files
- Monitor access to SSL certificates and keys (VSC02)
- Monitor access to vCenter by using built-in Windows account (VSH05)
- Monitor vSphere logs as required

Tuning 1: FIM Exceptions

You can tune out exceptions in the default FIM rules by using the Files to ignore or ignore patterns for text logs. In most cases, you want to ignore the vSphere programs (or your own trusted programs) that access their own files and thus record FIM events generated from non-trusted processes.

Tuning 2: Add additional vpxd log monitoring

To monitor the vCenter main log file, enable the rule and add matching event patterns. You can use VSH05 to monitor the vpxd log for specific security events that are mentioned in the VMware hardening guide. You can add the additional textlog or Windows Event log rules to the policy to monitor other related vSphere logs.

On the virtualization platforms, there is typically no downside to the deployment of these policies since they do not block any activity.

See "About Symantec Critical System Protection vSphere Detection Policies" on page 40.

Chapter 4

About Symantec Critical System Protection ESXi policies

This chapter includes the following topics:

About vSphere ESXi support

As with monitoring the VMware vCenter servers, it is important to understand the state and the login accesses made into the ESXi environment to ensure the integrity of the environment and its guests. The VMware hardening guide has explicit guidance to perform file integrity monitoring on the configuration and log files it exposes by the vSphere API. It also advises that certain VM configuration files are a cause for concern in terms of weakening security or exposing information in unwanted ways. In both instances, the vSphere ESXi Detection Policy addresses the requirements in the hardening guide. The ESXi Support Utility (RFS - Remote File Synchronization Tool) runs at least once to get the ESXi host files and store it locally. However, to detect changes to those files, you must apply vSphere ESXi detection policy.

Note: If you have a vSphere ESXi detection policy already applied to the collector system, you observe lot of file creation events on the console when you add a new ESXi host to monitor for the first time.

See "About the vSphere ESXi Detection Policy" on page 46.

About the vSphere ESXi Detection Policy

The vSphere ESXi Detection Policy provides the following features and capabilities:

- Provides File Integrity Events for ESXi Host configuration files (HMT03)
  - Files monitored are those available by standard vSphere API access
  - Customizable rules (11) for key configuration files (esx.conf, certs)
  - General FIM rule for all host configuration files
  - FIM events contain file change events such as name, size, date, time, and the contents of what has changed (file difference).
- Provides File Integrity Events for Virtual Machine configuration files (VMXnn)
  - FIM for guest VM configuration files (VMX) registered to an ESXi host
  - Customizable rules (9) for monitoring VMX configuration settings that are specifically defined in the VMware hardening guide
    It focuses on the specific content changes within a VMX file that may weaken security.
  - General FIM rule to generically monitor VMX files for changes.
  - Events contain the file change events and the contents of what has changed.
- Monitors ESXi Logs for specific events and provides a framework for general customer-specific monitoring. Logs monitored include the following:
  - Forwarded ESXi Syslog
    - Hostd - Host management service logs, including virtual machine and host task and events, communication with the vSphere Client and vCenter server vpxa agent, and SDK connections
    - Vpxa - vCenter Server vpxa agent logs, including communication with the vCenter Server and the Host Management hostd agent
  - auth.log
    ESXi Shell authentication success and failure
  - shell.log
    ESXi Shell usage logs, including shell enable, disable and other commands
  - vobd.log
    VMkernel observation events, including host boot up, enable or disable of SSH and Shell access, maintenance mode, and so on.

- Monitors ESXi Login, Logoff, and Failed Access attempts
  - Failed logins
    - Individual login failures
    - Threshold-based login failures
  - Successful logins
    - Logins by root or non-root accounts
    - Logins by type
    - Direct Console User Interface (DCUI)
    - SSH (user name and password)
    - SSH public key
    - After hour logins
  - Logoffs
- Monitors these ESXi Observation events
  - Boot-up
  - Shell enabled or disabled
  - SSH enabled or disabled
  - Maintenance mode enter or exit
- Monitors ESXi Interactive User Shell History Log
  - Session Start
  - Commands of interest (pre-populated with su, adduser, addgroup, and so on) and easily configurable
- Monitors ESXi Syslog Error events

The vSphere ESXi Detection Policy addresses a number of VMware hardening guide requirements, which includes the following requirements:

- **HMT03 – Establish and maintain ESXi configuration file integrity**
  The accessible and relevant files are found by browsing to http://hostname/host and should not include log files or those that change often due to system activity.
- **HMT15 – the "messages" kernel log file should be monitored for specific warning messages whenever an unsigned module is loaded into memory. [also addresses requirement HLG01 – configure remote syslog] vmkwarning.log**

A summary of Warning and Alert log messages excerpted from the VMkernel logs.

- **VMXnn – nine VM Configuration file content changes**
  The following image displays the VM configuration file content changes that are identified in the VMware hardening guide:

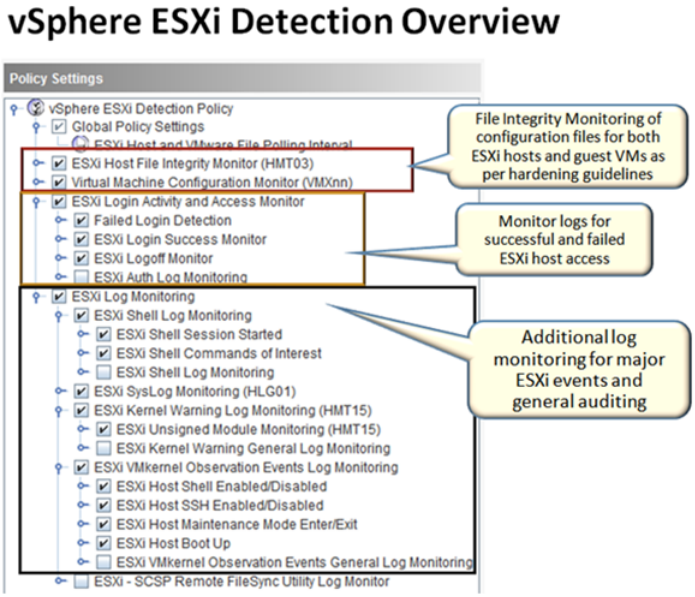
See "About vSphere ESXi support" on page 45.

See "About configuring and using vSphere ESXi Detection Policy" on page 48.

About configuring and using vSphere ESXi Detection Policy

The vSphere ESXi Detection Policy is similar to the existing ESX Security Hardening detection policy with fine grained rules and rich events.

Figure 4-1 vSphere ESXi Detection Policy



The default enabled rules in the vSphere ESXi Detection Policy do not require much tuning. The focus areas include Shell monitoring by adjusting the list of required commands, and specific operational events that may be found in the Syslog or other log files that are available for monitoring.

Note: ESXi monitoring is done Real Time taking advantage of Real Time File Monitoring feature (RTFIM) released in Symantec Critical System Protection 5.2.9. ESXi Host and VMWare File Monitoring Interval is only used if you have disabled RTFIM.

Unlike the vSphere ESX Detection Policy, the vSphere ESXi Detection Policy cannot be applied directly to an ESXi host since no Symantec Critical System Protection agent can be installed on the ESXi host. However, you can apply the vSphere ESXi Detection Policy to one or more Symantec Critical System Protection Collector hosts, which monitor a companion ESXi host.

The Symantec Critical System Protection Collector Agent now monitors multiple ESXi hosts. The events that are generated by monitoring each ESXi host is grouped together for a Virtual Agent. The Virtual Agent is named as the server address information used when adding an ESXi host to monitor (Refer rfs_config.sh -addHost page). If the syslog events are forwarded from the ESXi host using a different ESXi host name or IP address, it creates a new Virtual Agent on the

console. Monitoring RFS tool synchronizes errors: These errors are reported for a collector node under a Virtual Agent - `SCSPCollectorNode_<Agent Name used during SCSP Agent Installation>`. This allows the user to distinguish between multiple collector nodes, if they are set up. You may want to deploy both default prevention and detection policies on the Collector host to harden and monitor its own environment. You must also add specific rules to prevent unauthorized access to the file location that contains local copies of the ESXi host files.

See "About the vSphere ESXi Detection Policy" on page 46.

Chapter 5

About Symantec Critical System Protection ESX policies

This chapter includes the following topics:

About VMware ESX Protection Policy features

Symantec Critical System Protection provides an ESX Protection Policy to handle standard ESX service console components, such as core operating system daemons. The new policy limits the networking of non-ESX programs and blocks write access to ESX configuration and data files. The IPS policy complements the new ESX IDS Server Security Hardening policy.

The ESX Protection Policy features let you do the following on ESX systems:

- Harden the operating system environment
- Control privileged users
- Lock down configurations
- Secure data and other system resources
- Implement a Host firewall
- Control the behavior of applications

VMware ESX Protection Policy

Symantec Critical System Protection provides a new IPS ESX Protection Policy to handle standard ESX service console components, such as core operating system daemons. The new policy limits the networking of non-ESX programs and blocks write access to ESX configuration and data files. The IPS policy complements the new ESX IDS Server Security Hardening policy.

The ESX Protection Policy features let you do the following on ESX systems:

- Harden the operating system environment
- Control privileged users
- Lock down configurations
- Secure data and other system resources
- Implement a Host firewall
- Control the behavior of applications

See "ESX IPS policy custom programs and reference lists" on page 53.

See "Example deployment scenarios" on page 55.

ESX IPS policy custom programs and reference lists

Table 5-1 describes the reference lists that you can customize when you create a custom ESX IPS policy.

Table 5-1 Custom programs and reference lists

Name	Description
ESX Daemon List	A customizable list of file paths for the standard ESX daemons or third-party tools that need write access to critical VMware files and the network. Examples of such files include vmware-watchdog, vmware-authd, vmware-hostd, and webAccess and any child processes.
ESX Client Tools List	A customizable list of the file paths of interactive ESX command line tools and utilities or other third-party tools that need write access to critical VMware files. For example, configuration files and the VMware file system. Tools that it controls include esxcfg-*, esxupdate, and vcb* (used for backup and restore).
ESX Application Blacklist	A customizable list of ESX applications or OS applications that you want to block from execution. A security best practice is to disable the services and applications that are not required. For example, you might want to either remove the ESX webAccess service or block it. You can use the application blacklist to define and customize the applications that should be blocked from starting. For convenience, this list is referenced in both the Daemon and the Interactive Do Not start lists. The list is populated with an example entry for the webAccess daemon, but the option is disabled by default.
ESX Critical File List	A customizable list of ESX file paths for writable data and configuration files, such as /etc/vmware/*, /root/.bash_history, and /var/log/vmware/*. This list can be referenced globally to deny unrelated system and user processes write access to these files.

Table 5-1 Custom programs and reference lists *(continued)*

Name	Description
ESX Inbound Host List	A customizable list of valid inbound host IP addresses. By default, the list includes “Any” (0.0.0.0/0) to provide maximum operational compatibility upon first deployment. Enter the specific IP addresses or local subnet ranges in Classless Inter-Domain Routing (CIDR) notation to tighten the ESX network access restrictions. CIDR addresses include an IPv4 32-bit or IPv6 128-bit IP address as well as information on how many bits are used for the network prefix. For those bits not used, the corresponding bits in the IP address must be zero. **Note:** The IPv6 short notation '::' that is used to compress successive zeros is not supported. Use the full representation of the IP address instead. Typically, this list should include the following systems: ■ vSphere servers, such as license servers, update servers, backup servers, and other ESX/ESXi hosts ■ SNMP management protocol servers ■ Client access points, such as the VI client, Web access, remotecli, ssh, and so on
ESX Outbound Host List	A customizable list of valid outbound host IP addresses or CIDR address ranges. Some typical items that you might want to include in the list are as follows: ■ DNS servers ■ Network file servers ■ SNMP servers ■ Active Directory or LDAP servers ■ vSphere or vCenter servers ■ License servers By default, the list includes an address for Any” (0.0.0.0/0) to providemaximumoperational compatibility for the initial deployment. You can customize the list by entering the specific IP addresses or local subnet ranges in CIDR notation to tighten the ESX network access restrictions.

Table 5-1 Custom programs and reference lists *(continued)*

Name	Description
ESX Daemon Control	A Custom Program component that you can use to control the behavior of the ESX daemons. Such daemons include vmware-hostd, vmware-authd, vmware-watchdog, webAccess, and any child processes. Unlike the ESX Daemon List, this component allows the VMware-specific daemons to access such entities as the following: ■ ESX configuration files ■ VMware file systems ■ Devices ■ SysCall options ■ The network
ESX CLI Tools	A Custom Program component. Used to control the ESX interactive command line interface (CLI) tools and the utilities that console users or scripts can run. Tools that it controls include esxcfg-*, esxupdate, and vcb* (used for backup and restore). Unlike the default interactive process control, this component lets the VMware-specific CLI tools access ESX configuration files, VMware file systems, and devices. Use of the network is very limited.

See "VMware ESX Protection Policy" on page 52.

See "Example deployment scenarios" on page 55.

Example deployment scenarios

Suggestions for the initial deployment phase:

- Disable Global Prevention Mode and run only in IDS mode.
- Deploy and observe the events that normal ESX operations generate. In a typical ESX environment, you should expect to see few or no events.

Suggestions for the first policy refinement phase:

- Adjust critical file paths for non-default locations.
- Add application paths to ESX Daemon and CLI Tools list for any third-party tools that need write access to ESX critical files or networking.
- Open network ports for permitted activities, such as SSH outbound access from an ESX host.
- If the events that you see uncover additional resource usage, use the Event Wizard to adjust the policy. Re-examine the events to determine how best to

make adjustments. You may want to adjust the ESX reference lists, or you may want to use general program control change instead.

Suggestions for the policy hardening phase:

Table 5-2 Policy hardening

Task	Description
Network customization	■ Tighten the Inbound/Outbound Address list. Adjust the Any setting (0.0.0.0/0) to reduce the scope of remote system interaction to only valid inbound and outbound addresses or subnet ranges. ■ Customize the Network rules by closing unused service ports. Remove the ports and the protocols that are not used in your environment, for example, update manager, backup manager, and Active Directory. Change logging as desired for specific rules. Refine the ports and the protocols that are used for specific ESX processes as desired.
Blacklist customization	Add program paths for the items that you don't want to execute. For example, you may want to add webAccess.
Other customization	■ You may want to give users other than root the ability to override policies. ■ You may want to give users other than root the ability to run Symantec Critical System Protection configuration tools. ■ You may want to adjust the granularity of event logging. For example, you may want to record actions of interest such as updates to specific configuration files or the execution of specific ESX tools.

See "VMware ESX Protection Policy" on page 52.

About VMware ESX policy

The new VMware ESX policy provides ESX-specific monitoring functionality to secure the ESX host environment. It provides extensive control over rule content, logic, and behavior from the console and increased granularity of rule logic control for advanced tuning capabilities.

It contains the following improvements:

- Rule content can now be tuned more quickly and easily.
- Rule criteria is now dynamic and fully viewable in the console.

- Parameter values are pre-populated with default values and shown as parameter values under the rule option, which provides the standard on or off choice.
- You can now configure the parameter values. You can also set up select logic and ignore logic per rule, new event IDs, new registry paths, and so on from within the console. Changes in user-defined criteria are reflected in the console.
- You can now mouse over each option that is set to see detailed descriptions of the set and its function.

The vSphere ESX Detection policy includes the following top-level options.

Table 5-3 Top-level options in the VMware ESX Server Security Hardening policy

Top-level option	Description
Global Settings	Provides the easy setup of universal variables. It also contains a new choice group addition for file diff polling intervals. See "Global policy settings" on page 60.
Virtual Machine Configuration Monitor	Provides the configuration of hardening options. The configurable variables can each be hidden, if desired. It also includes a new choice group addition for rule severity. Users can select a level rather than having to type in a numerical value. See "Virtual Machine Configuration Monitor settings" on page 61.
ESX Host and VMware File Monitor	Provides the monitoring of critical files and directories. Users can base rules on the incoming flow and outgoing flow of specific data. Users can also enable and disable specific virtual machine (VM) configurations. See "ESX Host and VMware File Monitor settings" on page 62.
ESX Host Command Line Interface (CLI) Monitor	Provides the following features: ■ Privileged user access and command monitoring. ■ Threshold monitoring with higher severity options for customers to choose for multiple failed logon events. ■ Customer logon detection by configuring time and date restrictions. ■ Monitoring of privileged commands, by monitoring the use of superuser (SUDO) daemon and the root bash_history file. See "ESX Host Command Line Interface (CLI) Monitor settings" on page 63.

Table 5-3 Top-level options in the VMware ESX Server Security Hardening policy *(continued)*

Top-level option	Description
ESX Host Firewall Monitor	Real-time monitoring of the ESX host firewall log, esx-firewall. Events are generated for possible malicious activity. Commands to allow all incoming as well as all outgoing traffic are monitored. Nonstandard port and protocol enablement is monitored and events are generated for malicious activity and internal policy violation. See "ESX Host Firewall Monitor settings" on page 63.
ESX Host Administrator Web Access Monitor	Provides detailed Web access monitoring. You can monitor for a preset flood of invalid HTTP requests and can choose to log individual invalid requests. See "ESX Host Administrator Web Access Monitor settings" on page 64.
ESX Host Attack Detection	Monitors several means of possible attack conditions. You can monitor for HTTP/HTTPS vulnerability scanning activity and system vulnerability scanning activity. See "ESX Host Attack Detection settings" on page 64.

VMware ESX Host IDS policy pack

Symantec Critical System Protection now includes support for VMware ESX 4.1. The Symantec Critical System Protection Detection Policy Pack includes the vSphere ESX Detection policy (formerly named in previous releases as ESX_Server_Security_Hardening_Policy), which supports ESX 4.1. There is also an ESX Prevention Policy Workspace Pack that includes an ESX Protection Workspace policy for IPS support.

Note: vSphere Prevention Workspace Policy Pack contains ESX Prevention Policy Workspace Pack. vSphere Prevention Workspace Policy Pack is available in two versions, namely 5.2.0 and 5.2.9. For more details on the difference between the two versions, see *Symantec Critical System Protection Prevention Policy Reference Guide*.

You configure the new vSphere ESX Detection Policy for IDS. The ESX Protection Workspace policy uses custom programs to allow write access to ESX configuration and data files and VMware Virtual Infrastructure networking. It uses custom

reference lists to make it quicker and easier for you to customize the default ESX policy settings.

You use the standard UNIX IPS policy to handle the standard ESX service console components, such as the core operating system daemons. The standard policy was also modified to limit networking of non-ESX programs and to block write access to ESX configuration and data files.

Together, the new policy pack and the modifications to the existing UNIX IPS policy provide the following benefits:

- Provides centralized policy management.
- Provides centralized enforcement.
- Provides log aggregation of virtual and physical servers.
- Monitors and reports on guest and host intrusions in real time.
- Protects the ESX console operating system and guest operating systems and applications with layered controls. Examples include firewall, device control, configuration, system lockdown , administrator access control, and file system protection.
- Provides out-of-the-box policies as a guide to hardening VMware.
- Facilitates PCI compliance, including file integrity monitoring.

IDS ESX Security Hardening policy configuration settings

If you plan to use the IDS ESX Security Hardening policy on VMWare ESX 3.5, you should be sure that you tune the policy carefully. If Symantec Critical System Protection has to watch too many files or uses too many levels of recursion, it can cause a system crash. Sometimes, files are larger than the default limit of 100kb. This causes filewatch warnings. Tune the policy accordingly to monitor on the files that you are interested in.

Symantec Critical System Protection suggests that you take one or both of the following approaches:

- To avoid watching too many files, set the Virtual Machine Volume Path option under **Global Policy Settings > ESX Host Server Log** and **VMXFile Path Settings**, directly to your VMstore volume instead of the default setting (/vmfs/volumes/*.vmx).
  Alternately, you can add multiple paths, each of which points directly to one virtual machine.

- Decrease the **SearchDepth** option to 2. This option is located on the **Detection View** tab, on the **Configs** page, on the **Parameters** tab of the **DefaultDetection Parameters** dialog box.

Global policy settings

Table 5-4 Global Policy settings

Settings	Options
ESX Host Server Log and VMXFile Path Settings	■ **Virtual Machine Volume Path** Paths that contain the vmx configuration files. By default, this path is set to /vmfs/volumes/*.vmx so that all changes in this default location are logged without typing individual virtual machine paths separately. This location is the default location for most VMware ESX host installations. ■ **ESX Host Daemon Log Location** The path that contains the VMware ESX host agent log to monitor for suspicious activity. ■ **Root Bash History Log Path** The path that contains the Root Bash History Log to monitor for root commands at the command line interface prompt. ■ **ESX Host Firewall Log Path** The path that contains the ESX Host Firewall log to monitor for suspicious activity.
ESX Host Server File MonitoringPollingInterval	■ **Virtual Machine (VM) Configuration File Content Polling Interval** The polling interval for reporting configuration files content changes. ■ **ESX Host and VMware File Content Polling Interval** The polling interval for reporting host file and VMware file content changes.

See "About VMware ESX policy" on page 56.

Virtual Machine Configuration Monitor settings

Table 5-5 Virtual Machine Configuration Monitor settings

Settings	Options
VM Remote VNC Display Console Enabled	Detects the addition of a VNC remote display to the VM. Use of the VNC remote display to view active VMs is not advised as it provides access to the VM guest OS by any user.
VM Logging Disabled	Detects when VM users disable all forms of logging.
VM Copy and Paste Between Guest VMX03	Detects the enablement of cut and paste operations to the VM configuration file, and changes to the suggested *.vmx configuration file settings that are used to disable such operations. By default, users can cut and paste between the guest OS and the computer where the remote console is running. Unauthorized users and processes may be able to access the clipboard for the VM console.
VMSetInfo Messages Enabled	Detects the removal or modification of the setting to disable the sending of informational messages to the ESX or ESXi host using VMware tools.
VMSetInfo Memory Size ChangeVMX21	Detects the removal or addition of the setting to change the size of informational messages that can be sent to the ESX or ESXi host using VMware tools. Unrestricted data flow can let a denial-of-service attack use SetInfo messages to flood a host with packets and consume resources.
VMMonitorforAllChanges toVMXFiles	The output of this rule contains the changed content of changes to all .vmx configuration files.
VM Disk Shrinking Enabled -VMX01	Detects adding or removal of the settings in the VM configuration file to allow non-root users, root users, and processes to shrink a virtual disk.
VM Limit Console Connections - VMX02	Detects if VM Configuration file is modified to allow multiple users to connect remote console sessions.
VM Unrestricted Communication Enabled - VMX12	Detects if VM-to-VM Communication (VMCI) is enabled or disabled.

Table 5-5 Virtual Machine Configuration Monitor settings *(continued)*

Settings	Options
VM Remote Operations in Guests Enabled - VMX30	Detects whether VM configuration files are enabled to automate virtual machine operations via scripts.
VM Control VMSafe CPU/Memory API Usage - VMX52	Detects whether virtual machines are configured to explicity accept access by VMWare VMSafe CPU/memory APIs.
VM Control VMSafe Network API Usage - VMX55	Detects whether virtual machines are configured to explicity accept access by VMWare VMSafe Network APIs.

See "About VMware ESX policy" on page 56.

ESX Host and VMware File Monitor settings

Table 5-6 ESX Host and VMware File Monitor settings

Settings	Options
ESX Configuration Files - ESX.conf	Detects the modifications to the file. All modifications include the text content that was added to or removed from the file.
ESXConfigurationStateFiles-License Files	Detects the modifications to the files. All modifications include the text content that was added to or removed from the files.
ESX Configuration Files - Proxy.XML	Detects the modifications to the file. All modifications include the text content that was added to or removed from the file.
ESX Configuration Files - SSL Key and Cert Files	Detects the modifications to the files. All modifications include the text content that was added to or removed from the files.
ESX Configuration Files - Syslog.conf	Detects the modifications to the file. All modifications include the text content that was added to or removed from the file.
ESX Configuration Files - Vmware_config	Detects the modifications to the files. All modifications include the text content that was added to or removed from the file.

Table 5-6 ESX Host and VMware File Monitor settings *(continued)*

Settings	Options
ESX Configuration Files - Vpxa.cfg	Detects the modifications to the files. All modifications include the text content that was added to or removed from the file.
ESX Configuration State Directory - /etc/vmware/	Detects the modifications to the files in this critical directory. All modifications include the text content that was added to or removed from the files.

See "About VMware ESX policy" on page 56.

ESX Host Command Line Interface (CLI) Monitor settings

Table 5-7 ESX Host Command Line Interface (CLI) Monitor settings

Settings	Options
CLI Login Detection	Provides the customization for monitoring the critical files that are associated with the operation of the ESX Host and VMware in general. It monitors failed logon attempts by root and users, and detection based on time of day or week.
CLI Command Monitoring	Provides the customization for monitoring the command activity that is associated with the ESX Host CLI. Monitors SUDO commands and all root commands.

See "About VMware ESX policy" on page 56.

ESX Host Firewall Monitor settings

Table 5-8 ESX Host Firewall Monitor settings

Settings	Options
HostESXFirewallAllowAllIncoming Ports	Monitors the host ESX firewall for the "all incoming TCP/IP traffic is allowed" event.

Table 5-8 ESX Host Firewall Monitor settings *(continued)*

Settings	Options
HostESXFirewallAllowAllOutgoing Ports	Monitors the host ESX firewall for the "all outgoing TCP/IP traffic is allowed" event.
Host ESX Firewall Non-Standard Port/Protocol Modification	Monitors the host ESX firewall for the addition of a nonstandard port to either incoming rules or outgoing rules.

See "About VMware ESX policy" on page 56.

ESX Host Administrator Web Access Monitor settings

Table 5-9 ESX Host Administrator Web Access Monitor settings

Settings	Options
ESXHostAdminWebAccess Failed Login Detection	Detects the failed logon attempts.
ESX Host Admin Web Access Invalid Request Detection	Detects the invalid HTTP requests that may indicateWebvulnerability scanner or other abuse.

See "About VMware ESX policy" on page 56.

ESX Host Attack Detection settings

Table 5-10 ESX Host Attack Detection settings

Settings	Options
Attack Detection Date and Time Restrictions	Lets you customize specific time and date values during which the ESX Host attack detection rules are disabled (whitelisted). Use this setting with specific date and time values for scheduled vulnerability assessment scans in the environment. These restrictions are used to avoid false positives from otherwise known and scheduled vulnerability scanning activity.

Table 5-10 ESX Host Attack Detection settings *(continued)*

Settings	Options
HTTP/HTTPSVulnerability Scanning Activity Detected	Detects HTTP/HTTPS vulnerability scanning activity.
ESX System Vulnerability Scanning Activity Detected	Detects ESX System vulnerability scanning activity.
NMAPNSE Scanning Activity Detected	Detects NMAP NSE vulnerability scanning activity.

See "About VMware ESX policy" on page 56.

Chapter 6

About vSphere reports, configuration, and usage

This chapter includes the following topics:

About vSphere queries and reports

The vSphere report pack adds a new folder and subfolders in the queries and reports hierarchy. It also adds over 55 predefined query and report objects that can be directly executed or can be used as a template to modify filter criteria, sort, or display result. Unlike the general default queries and reports, each of the vSphere objects is focused on slicing the event, agent, and policy data across specific virtualization aspects.

Key features of the vSphere queries and reports include:

- Filters on events and agents that are specifically related to vSphere infrastructure systems.
- Organize and filter data along specific dimensions, including:
  - By virtualization tier – Virtual Machine events, Hypervisor (Host) events, and vSphere Management System events.
  - By resource type – Network events, file integrity events, sensitive data access events, and so on.
  - By Object – User, Hosts, Applications, and Resources.
  - By Hardening requirement or category – VSHnn, VMXnn, HMTnn, and other VMware identified hardening actions.

- Target a specific display purpose – Top n charts, Summary level counts, and detailed activity logs.

The newly added Query tree hierarchy includes a vSphere folder and subfolders that organize the content by VMware Infrastructure tiers (virtual machines, hosts, and management platforms). The subfolder names and their contents are:

- **All Systems and Events**
  Contains queries that display information about all the systems and event activity that occur across the VMware infrastructure where vSphere policies have been deployed. Queries in this folder include:
  - Event trend charts.
  - Top 10 pie charts showing event activity for the top systems, resources, processes, detection rule names, and prevention actions.
  - Details for agents that have vSphere policies applied.
  - Details for events across the infrastructure.
  - Summarized Policy digest showing the entire potential set of rules and hardening requirements addressable across all vSphere policies if every rule was enabled. It also displays event counts for each rule and the number of unique systems where the event activity occurred.
  - Hardening event counts is a subset of the above Policy digest that displays just those explicit VMware hardening rules that had any event activity.
- **Hosts (ESXi)**
  Contains queries that display information about ESXi hypervisor hosts and their event activity for those hosts that are monitored by a Symantec Critical System Protection Collector node. Queries in this folder include:
  - Event trend charts for Hosts.
  - Top 10 pie charts showing event activity for the top hosts and top shell commands issued during direct login to hosts.
  - Summary event counts for hosts, rule names, file integrity and log monitoring.
  - Details for events across all Host activities as well as granular detail displays only for file integrity, direct login activity, shell usage, and general log monitoring.
  - Summarized Policy digest showing the entire potential set of rules and hardening requirements applicable to Hosts. It also shows event counts for each rule and the number of unique systems where the event activity occurred.

- **Virtual Machine Changes**
  Contains queries that display information about Virtual Machine configuration file changes (VMX files). These files are monitored for configuration changes to specific settings that the VMware Hardening document suggests not to be set. In addition, VMX files are monitored for creation and deletion as a way to determine when virtual machines are registered or with or leave an ESXi host. Queries in this folder include:
  - Top 10 pie charts showing event activity for the top hosts and top virtual machine VMX files.
  - Summary event counts for Hosts and Virtual Machine configuration events.
  - Details for VMX change events across all Hosts and Virtual Machines.
  - Details on current VMX location and whether they have been moved from one ESXi host to another.
  - Summarized Policy digest showing the entire potential set of rules and hardening requirements applicable to VMX configuration file changes. It also shows event counts for each rule and the number of unique systems where the event activity occurred.
- **vSphere Systems**
  Contains queries that display information about vSphere Windows-based management systems including vCenter, vCenter support tools, and vSphere clients. The queries report on event activity from the systems that has deployed a vSphere detection or prevention policy. Queries in this folder include:
  - Top 10 pie charts showing event activity for the top systems, resources, processes, and top VMware processes that are involved in event actions.
  - Summary event counts for login failures and processes.
  - Details for events across the management tier as well as granular queries for file integrity, registry integrity, network, login accesses, resources, and access or changes to sensitive SSL keys.
  - Summarized Policy digest showing the entire potential set of rules and hardening requirements addressable across the management tier when every rule was enabled. It also shows event counts for each rule and the number of unique systems where the event activity occurred.
  - Hardening event counts is a subset of the above Policy digest showing just those explicit VMware hardening rules that had any event activity

In addition to the Queries, a **VMware Infrastructure Summary** report is also provided to the Reports hierarchy. This is a multi-page report that combines multiple Top N and trend charts for a dashboard summary display without having to execute each such query individually. The report is simply an example and is

intended as a launch point for users to craft their own reports based on the provided query content or their own customized queries.

See "Importing Symantec Critical System Protection vSphere Policies" on page 15.

About vSphere query and report customization

Use the vSphere queries and report for the following purposes:

- To help tune vSphere policies
- To identify security-related events of interest or spot trends
- To identify key resources, users, programs, and so on in which you may want to establish alerts or real-time monitor displays
- To extend queries and reports as required by your organization
- To re-use query SQL in external reporting programs

See "Importing Symantec Critical System Protection vSphere Policies" on page 15.