Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark

For Red Hat Enterprise Linux 5

Symantec™ ESM Baseline Policy Manual for CIS Benchmark for Red Hat Enterprise Linux 5

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT 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 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

Symantec™ ESM Baseline Policy Manual for CIS Benchmark for Red Hat Enterprise Linux 5

This chapter includes the following topics:

- Introducing the policy
- Installing the policy

Introducing the policy

The Symantec Enterprise Security Manager (ESM) Baseline Policy for the Center for Internet Security (CIS) Benchmark for Red Hat Enterprise Linux assesses a host’s compliance with the benchmark's recommendations.

This release of the policy was built based on the CIS benchmark version 1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1. This policy can be installed on Symantec ESM 6.5.3 and later managers running Security Update 36 or later on Red Hat Enterprise Linux version 5.

For information on the Center for Internet Security benchmarks, visit the following URL:

http://www.cisecurity.org

Installing the policy

Before you install the policy, you must decide on the Symantec ESM Managers that you want to install the policy. Since policies run on Managers, you do not require to install policies on agents. You must install the policy on Symantec ESM 6.5.3 or later with Security Update 36 or later.

Obtaining and Installing the policy using LiveUpdate

You can install the LiveUpdate feature in the following ways:

- By using the LiveUpdate feature on the Symantec ESM console
- By using files from a Product disc or from the Internet

To install the policy using LiveUpdate

1. Connect the Symantec ESM Enterprise Console to the managers on which you want to install the policy.
2. Click the **LiveUpdate** icon to start the LiveUpdate Wizard.
3. In the wizard, ensure that Symantec LiveUpdate (Internet) is selected, and then click **Next**.
4. In the **Welcome to LiveUpdate** panel, click **Next**.
5. In the **Available Updates** panel, do one of the following:
   - To install all checked products and components, click **Next**.
   - To omit a product from the update, uncheck it, and then click **Next**.
   - To omit a product component, expand the product node, uncheck the component that you want to omit, and then click **Next**.
6. In the **Thank you** panel, click **Finish**.
7. In the list of managers panel, ensure that all the managers that you want to update are checked, and then click **Next**.
8. In the **Updating Managers** panel, click **OK**.
9. In the **Update Complete** panel, click **Finish**.

If you cannot use LiveUpdate to install the policy directly from a Symantec server, you can install the policy manually, using files from a Product disc or the Internet.

Note: To avoid conflicts with updates that are performed by standard LiveUpdate installations, copy or extract the files into the LiveUpdate folder, which is usually Program Files/Symantec/LiveUpdate.

To install the policy from a Product disc or from the Internet

1. Connect the Symantec ESM Enterprise Console to the managers that you want to update.

2. From the Symantec Security Response Web site, download the executable files for Red Hat Enterprise Linux 5.0. You can go to the following link:

   http://securityresponse.symantec.com

3. On a computer running Windows NT/2000/XP/Server 2003 that has network access to the manager, run the executable that you downloaded from the Symantec Security Response Web site.

4. Click **Next** to close the **Welcome** panel.

5. In the **License Agreement** panel, if you agree to the terms of the agreement, click **Yes**.

6. In the **Question** panel, click **Yes** to continue installation of the best practice policy.

7. In the **ESM Manager Information** panel, type the requested manager information, and then click **Next**.

   If the manager's modules have not been upgraded to Security Update 36 or later, the installation program returns an error message and stops the installation. Upgrade the manager to Security Update 36 or later, and then rerun the installation program.

8. Click **Finish**.

Chapter 2

Policy modules

This chapter includes the following topics:

Policy modules

The CIS Benchmark for Red Hat Enterprise Linux 5 policy include the modules that ensure compliance with various technical and administrative aspects. Each module lists the enabled checks with the standards that they address, the associated name lists, and the templates. As specific values are not required everywhere, default values and templates are provided. Although the policy appears as read only, you can copy or rename the policy, depending on the requirements of your corporate security policy.

Account Integrity

The Account Integrity module reports new, changed, and deleted accounts, account name and rights vulnerabilities, and user rights.

Table 2-1 gives a list of the checks and their CIS sections.

Table 2-1 Checks and CIS sections

Check	CIS section
Duplicate IDs	11.2.1, 11.2.2, 11.2.3, 11.2.4

File Attributes

The File Attributes module reports changes to file creation and modification times, file sizes, and CRC/MD5 checksum signatures. It also reports violations of the file permissions that are specified in the template files.

Table 2-2 gives a list of the checks and their CIS sections.

Table 2-2 Checks and CIS sections

Check	CIS section
Group Ownership	4.14, 4.4, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 9.1, 9.11, 9.3, 9.9, 9.10, 10.1, 10.2, 11.1.1, 11.1.4, 11.3.1, 11.4.2
Permissions	2.3, 3.2, 3.6, 4.14, 4.3, 4.4, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 9.1, 9.10, 9.11, 9.3, 9.6, 9.9, 10.1, 10.2, 11.1.3, 11.1.6, 11.3.3, 11.4.4, 11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.6.1
Template List	4.15, 4.16, 4.17, 4.18, 4.19, 4.20
User Ownership	4.4, 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 9.1, 9.11, 9.3, 9.9, 9.10, 10.1, 10.2, 11.1.2, 11.1.5, 11.3.2, 11.4.3

File Find

The File Find module reports weaknesses in the file permissions and the configuration files.

Table 2-3 gives a list of the checks and their CIS sections.

Table 2-3 Checks and CIS sections

Check	CIS section
File Content Search	2.3, 3.2, 4.14, 4.3, 4.4, 5.1, 5.2, 6.2, 7.1, 7.2, 7.9, 8.1, 8.2, 8.4, 8.6, 8.8, 8.10, 9.1, 9.10, 9.11, 9.4, 10.2, 10.3, 11.1.11, 11.1.12, 11.1.13, 11.1.14, 11.1.15, 11.4.1
Setgid executable files	7.7
Setuid executable files	7.7
Unowned Directories/Files	7.8
World writable directories with sticky bit	7.5
World writable files	7.6

Login Parameters

The Login Parameters module reports accounts, resources, and settings that are not complaint with the policies.

Table 2-4 gives a list of the checks and their CIS sections.

Table 2-4 Checks and CIS sections

Check	CIS section
Inactive accounts	9.3
Locked Accounts	9.1
Warning Banners	10.1

Network Integrity

The Network Integrity module reports the system configuration settings that pertain to authentication and remote access.

Table 2-5 gives a list of the checks and their CIS sections.

Table 2-5 Checks and CIS sections

Check	CIS section
FTP Denied Users	8.2
FTP debug logging disabled	6.2
Forbidden listening TCP ports	8.3
NFS exported directory non-secure	8.9

OS Patches

The OS Patches module reports the patches that are defined in the UNIX patch template files for RHEL but are not installed on the agent.

Table 2-6 gives a list of the checks and their CIS sections.

Table 2-6 Checks and CIS sections

Check	CIS section
Patch Template	2.1

Password Strength

The Password Strength module examines the system parameters that control a password's construction, change, age, expiration, and storage.

Table 2-7 gives a list of the checks and their CIS sections.

Table 2-7 Checks and CIS sections

Check	CIS section
Accounts without password	9.2
Maximum password age	9.3
Minimum password age	9.3
Password age warning	9.3
Password length restrictions	9.3

Startup Files

The Startup Files module examines the system parameters that control processes and the services that are executed at system startup time.

Table 2-8 gives a list of the checks and their CIS sections.

Table 2-8 Checks and CIS sections

Check	CIS section
Grub Password	8.7
Installed Services	3.1, 3.3, 3.4, 3.5, 3.6, 4.1, 4.10, 4.11, 4.12, 4.13, 4.14, 4.2, 4.3, 4.5, 4.6, 4.7, 4.8, 4.9, 4.21, 4.22, 11.1.7, 11.1.8, 11.1.9, 11.1.10
Syslog	6.1, 6.4

User Files

The User Files module reports issues with ownership and permissions on the files that are contained in the user home directories.

Table 2-9 gives a list of the checks and their CIS sections.

Table 2-9 Checks and CIS sections

Check	CIS section
Startup file protection	9.9
umask (parsing startup scripts)	9.9
Umask	4.1
World writable directories in PATH	9.5
World writable files	9.7, 9.8