User Guide

NetIQ Change Guardian

March 2013

Legal Notice

Contents

About this Book and the Library

The *User Guide* provides planning, installation, and conceptual information about the Change Guardian Policy Editor, the Change Guardian server, and Change Guardian modules. This book guides you through installation, defines terminology, and explains implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding Change Guardian product concepts, and for individuals installing and using this operational change auditing solution for their enterprise network.

Other Information in the Library

The library provides the following information resources:

Help

Provides context-sensitive information and guidance for frequently- performed-tasks.

Release Notes

Provides additional information about the release, known issues, and resolved issues.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	◆ Window and menu items ◆ Technical terms, when introduced
Italics	◆ Book and CD-ROM titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must type ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value*]	◆ Optional parameters of a command
Braces, such as {*value}*	◆ Required parameters of a command
Logical OR, such as *value1*|*value2*	◆ Exclusive parameters. Choose one parameter.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Introduction

The NetIQ Change Guardian product (Change Guardian) is a change auditing solution that provides organizations with the ability to monitor for changes to critical system and corporate files. Change Guardian events allow you to see file changes, as well as who made the change, the time of the change, and the computer from which the user initiated the change. In many cases, Change Guardian provides the before and after values for the change so organizations have enough information to take needed action.

1.1 What is Change Guardian?

Change Guardian is an enterprise monitoring and reporting solution for UNIX, Linux, Microsoft Windows, and Microsoft Active Directory that provides a powerful, flexible way to monitor and report on changes.

Change Guardian provides the ability to monitor critical system and corporate resources for changes and display information about the changes made, including who made the change, to which file, and where.

1.2 How Change Guardian Works

Change Guardian allows you to create policies, which define the critical enterprise resources and configurations to monitor, and to determine how to classify detected changes. Based on the policies you create, Change Guardian sends event information to the Change Guardian server.

The Change Guardian Policy Editor is a Windows-based console through which you create policies to monitor computers in your enterprise. The Change Guardian server, a Linux-based computer, stores your policies and change events. The Change Guardian Web interface allows you to view events, or you can use syslog to forward events from the Change Guardian server to another computer.

1.2.1 Understanding Managed and Unmanaged Users

Change Guardian allows you to designate specific users to make specific changes. These users are **managed users**. Events generated when managed users make changes appear as managed change events. Users who are not authorized to make changes are **unmanaged users**.

1.2.2 Understanding Change Guardian Agents

Change Guardian communicates with monitored computers through agents you install on those computers. Agents receive policy information from the Policy Repository on the Change Guardian server, and send events back to the Change Guardian server. You can use the Change Guardian Web interface to view events, or use syslog to forward them to other applications.

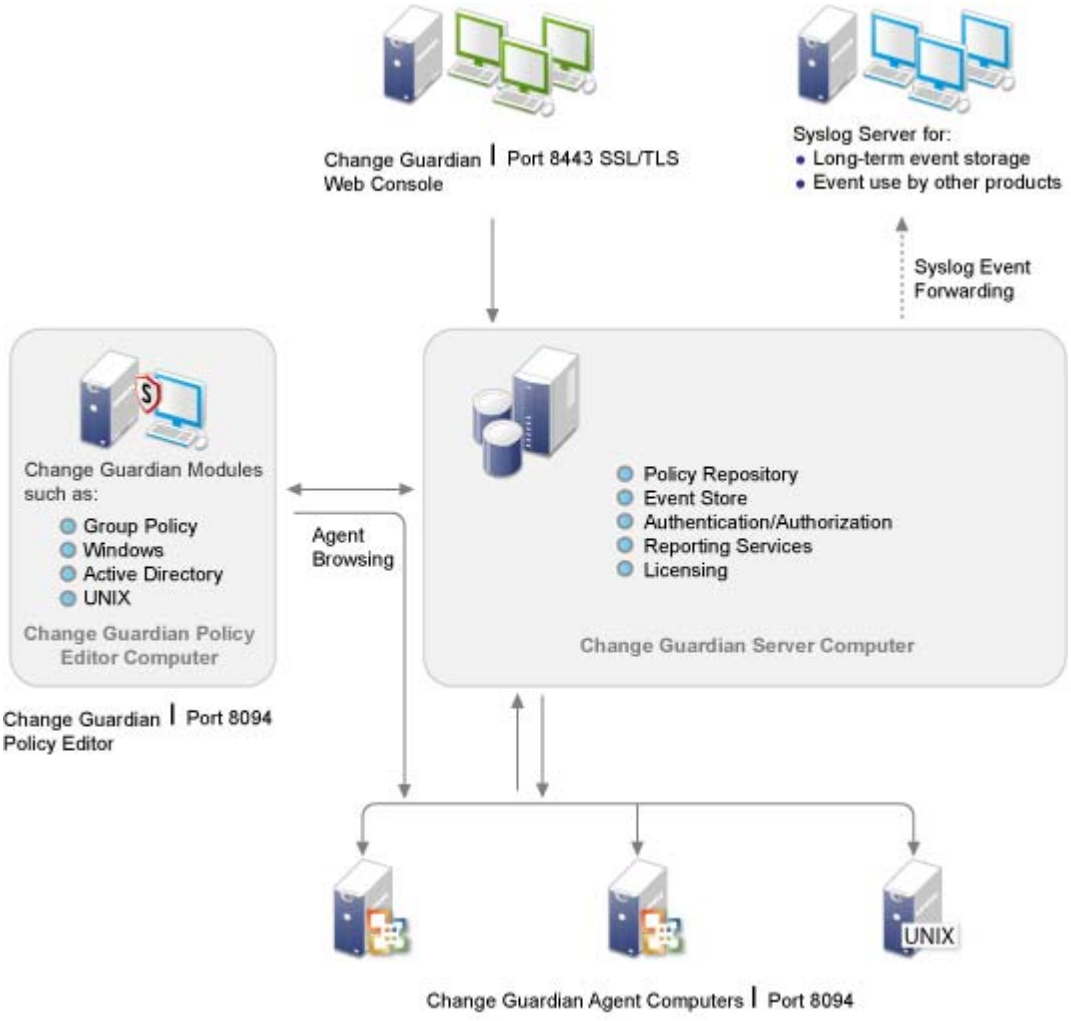
When you install the Policy Editor, you can choose to install an agent locally, on other Windows computers in your enterprise, or both. To install the agent on other Windows computers, Change Guardian creates a silent agent installer that includes the same communication options set during your Policy Editor installation.

You can install the UNIX agent to UNIX and Linux computers using either a silent installation file or by remote deployment using either the UNIX Agent Manager console or the standalone deployment wizard.

UNIX Agent Manager allows you to install and configure all your UNIX agent components across your enterprise instead of interacting with the agents individually. UNIX Agent Manager also allows you to see any UNIX computers that NetIQ Secure Configuration Manager, NetIQ AppManager, and NetIQ Security Manager products monitor. UNIX Agent Manager includes a console and a server that stores information and communicates with the agents. You can install numerous consoles that can connect to a single server. UNIX Agent Manager runs on Windows, Solaris, and Linux computers.

1.3 Understanding Change Guardian Architecture

Change Guardian comprises the Change Guardian Policy Editor, the Change Guardian server, the agents, and the Change Guardian Web interface.



Opening ports on agent computers is not necessary unless you want the ability to browse the computer for files, processes, and users when you create policies.

1.4 Change Guardian Implementation Checklist

Change Guardian installation requires you to perform the following actions:

	Checklist Items
❑	Plan your Change Guardian server installation. For more information, see Chapter 2, “Planning to Install the Change Guardian Server,” on page 15.
❑	Install the Change Guardian server. For more information, see Chapter 3, “Installing the Change Guardian Server,” on page 25.

	Checklist Items
❑	Verify the Change Guardian Web console can connect to the server by specifying the following URL in your Web browser: `https://`*IP_Address_Change_Guardian_server*`:8443`
❑	Install the Change Guardian Policy Editor. For more information, see Chapter 4, “Installing the Change Guardian Policy Editor,” on page 37.
❑	(Conditional) If you are using Change Guardian for UNIX, install UNIX Agent Manager and the UNIX agent. For more information, see Chapter 5, “Installing the UNIX Agent and UNIX Agent Manager,” on page 41.
❑	Synchronize time by using the Network Time Protocol (NTP).
❑	(Conditional) If you install the Change Guardian server appliance, ensure that the ports listed in Section 2.1.8, “Understanding Port Usage by the Change Guardian Server,” on page 20 are opened in the firewall.
❑	(Conditional) If you plan to perform an appliance installation, you must also: ◆ Obtain your license key if you plan to install the licensed version. ◆ Obtain your registration code to register for software updates. For more information, see Section 3.5, “Installing the Change Guardian Server Appliance,” on page 30.

2 Planning to Install the Change Guardian Server

This chapter guides you through planning considerations before installing the Change Guardian server. You must install the Change Guardian server before you install the Change Guardian Policy Editor.

2.1 System Requirements

This section describes the hardware, operating system, browser, and event source compatibility requirements for the Change Guardian server.

2.1.1 Supported Operating Systems and Platforms

You can install the Change Guardian server on a computer (standalone installation), or on a virtual machine (appliance installation) running one of the following operating systems:

- SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 (64-bit)
- Red Hat Enterprise Linux for Servers (RHEL) 6 (64-bit)

NOTE

- Open Enterprise Server installations of SLES do not support the Change Guardian server.
- RHEL and SLES each have specific prerequisites. For more information, see Section 2.2, "Completing Prerequisites for SLES 11 SP 2 and RHEL 6," on page 21.

Category	Requirement
Operating System	The Change Guardian server is supported on the following operating systems: ◆ SUSE Linux Enterprise Server (SLES) 11 SP 2 (64-bit) ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 (64-bit) **NOTE** ◆ Open Enterprise Server installations of SLES do not support the Change Guardian server. ◆ RHEL and SLES each have specific prerequisites. For more information, see Section 2.2, "Completing Prerequisites for SLES 11 SP 2 and RHEL 6," on page 21.

Category	Requirement
Virtual Platform	NetIQ provides appliances that install a SLES 11 SP 2 (64-bit) server and the Change Guardian server on the following virtual platforms: ◆ VMware ESX 4.0 ◆ Xen 4.0
DVD ISO	NetIQ provides an appliance as a DVD ISO file that installs SLES 11 SP 2 (64-bit) and the Change Guardian server on the following: ◆ Hyper-V Server 2008 R2 ◆ Hardware without an operating system installed

Hardware Requirements

The hardware recommendations for the Change Guardian server can vary based on your environment and monitoring needs. Consult NetIQ Professional Services prior to finalizing the Change Guardian implementation.

Use the following hardware requirements for running the Change Guardian server:

Category	100 Events per Second	2500 Events per Second
CPU	One Intel Xeon X5570 2.93-GHz (4 CPU cores)	Two Intel Xeon X5470 3.33-GHz (4 core) CPUs (8 cores total)
Disk Space	150 GB (less can be used for fewer days of storage, no RAID required)	6 x 1 TB, 7.2k RPM drives (hardware RAID with 256 MB cache, RAID 10)
Memory	4 GB	16 GB

NOTE: The Change Guardian server is supported on x86 (64-bit) Intel Xeon and AMD Opteron processors, but is not supported on pure 64-bit processors like Itanium.

2.1.2 Supported Database Platforms

The Change Guardian server includes an embedded file-based storage system and a database.

2.1.3 Supported Browsers

The following browsers are supported for the Change Guardian Web console.

NOTE: To load the Change Guardian Web console properly, you must have the Sun Java plug-in installed on your computer.

Operating System	Browser
Windows 7	◆ Firefox 5 ◆ Firefox 6 ◆ Firefox 7 ◆ Firefox 8 ◆ Firefox 9 ◆ Firefox 10 ◆ Internet Explorer 8 ◆ Internet Explorer 9 For more information, see “Prerequisites for Internet Explorer” on page 17.
SLES 11 SP 2 and RHEL 6	◆ Firefox 5 ◆ Firefox 6 ◆ Firefox 7 ◆ Firefox 8 ◆ Firefox 9 ◆ Firefox 10 For more information, see “Manually Updating the Firefox Version” on page 17.

Prerequisites for Internet Explorer

To view Change Guardian events using Internet Explorer 8, ensure the following:

- Set the security level to Medium-high. If the Internet Security Level is set to High, only a blank page appears after logging in to the Change Guardian Web console. To change your security level, on the Tools menu, click **Internet Options** > **Security** and select **Medium-high**.
- On the Tools menu, ensure **Compatibility View** is not selected.
- Enable the Automatic prompting for file downloads option to ensure the browser does not block the file download. To enable this feature, click **Tools** > **Internet Options** > **Security** > **Custom Level**, scroll down to the Downloads section, and then select the **Enable** check box under Automatic prompting for file downloads.

Manually Updating the Firefox Version

The Change Guardian server supports Firefox version 5, 6, 7, 8, 9, and 10. However, SLES 11 SP 2 is packaged with Firefox 3.6.

To manually update a SLES 11 SP 2 installation to include Firefox 5, 6, 7, 8, 9, or 10:

1. Open YaST.
2. Click **Software** > **Software Repositories** to display the Configured Software Repositories window.
3. Click **Add** to open the Media Type window.
4. Select **Specify URL**, and then click **Next**.

5 Type the address for the Software Repository (http://download.opensuse.org/repositories/mozilla/SLE_11/) **URL** text box, and then click **Next** to download the software repository.

6 Click **OK** to refresh the software repository.

7 Click **Software Management** to open the YaST2 window.

8 Type `Firefox` in the **Search** text box.

9 Select the required packages for Firefox 5, 6, 7, 8, 9, or 10.

NOTE: A warning appears if you select a package that conflicts with the existing version. Select the appropriate option, and then click **OK Try Again**.

10 Click **Accept**.

2.1.4 Estimating Data Storage Requirement

The Change Guardian server stores raw data to comply with legal and other requirements. Change Guardian employs compression to help you make efficient use of local and networked storage space.

To determine the amount of random-access storage space required for the Change Guardian server, first estimate the number of days of data for which you need to regularly perform searches or run reports. You should also have additional hard drive space beyond your minimum requirements to account for data rates that are higher than expected.

Use the following formulas to estimate the amount of space required to store data:

Local event storage (partially compressed):

```
{average byte size per event} x {number of days} x {events per second} x
0.00008 = Total GB storage required
```

Event sizes typically range from 300-1000 bytes.

Networked event storage (fully compressed):

```
{average byte size per event} x {number of days} x {events per second} x
0.00002 = Total GB storage required
```

Raw data storage (fully compressed on both local and networked storage):

```
{average byte size per raw data record} x {number of days} x {events per
second} x 0.000012 = Total GB storage required
```

A typical average raw data size for syslog messages is 200 bytes.

Total local storage size (with networked storage enabled):

```
{Local event storage size for desired number of days} + {Raw data storage size
for one day) = Total GB storage required
```

If you enable networked storage, event data moves to networked storage when local storage fills up. Raw data, however, is located in local storage temporarily before it moves to networked storage. It typically takes less than a day to move the raw data from local storage to networked storage.

Total local storage size (with networked storage disabled):

```
{Local event storage size for retention time} + {Raw data storage size for
retention time) = Total GB storage required
```

Total networked storage size:

```
{Networked event storage size for retention time} + {Raw data storage size for
retention time} = Total GB storage required
```

NOTE

- The coefficients in each formula represent {(seconds per day) x (GB per byte) x compression ratio}.
- These numbers are only estimates and depend on the size of the event data and the size of compressed data.
- Partially compressed means that the data is compressed, but the index of the data is not compressed. Fully compressed means that both the event data and index data is compressed. Event Data compression rates are typically 10:1. Index compression rates are typically 5:1. The index is used to optimize searching through the data.

You can use the formulas above to determine how much storage space is required for a long-term data storage system.

2.1.5 Estimating Disk I/O Usage

Use the following formulas to estimate the amount of disk usage on the server at various EPS rates.

Data written to disk (kilobytes per second):

```
(average event size in bytes + average raw data size in bytes) x (events per second) x .004 compression coefficient = data written per second to disk
```

For example, at 500 EPS, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, data written to disk is determined as follows:

```
(464 bytes + 300 bytes) x 500 EPS x .004 = 1558 KB
```

Number of I/O requests to the disk (transfers per second):

```
(average event size in bytes + average raw data size in bytes) x (events per second) x .00007 compression coefficient = I/O requests per second to disk
```

For example, at 500 EPS, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, the number of I/O requests per second to the disk is determined as follows:

```
(464 bytes + 300 bytes) x 500 EPS x .00007 = 26 tps
```

Number of blocks written per second to the disk:

```
(average event size in bytes + average raw data size in bytes) x (events per second) x .008 compression coefficient = blocks written per second to disk
```

For example, at 500 EPS, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, the number of blocks written per second to the disk is determined as follows:

```
(464 bytes + 300 bytes) x 500 EPS x .008 = 3056
```

Data read per second from disk when performing a search:

```
(average event size in bytes + average raw data size in bytes) x (number of events matching query in millions) x .13 compression coefficient = kilobytes read per second from disk
```

For example, at three million events matching the search query, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, the number of blocks written per second to the disk is determined as follows:

```
(464 bytes + 300 bytes) x 3 x .13 = 300 KB
```

2.1.6 Estimating Network Bandwidth Usage

Use the following formulas to estimate the network bandwidth utilization on the server at various EPS rates:

```
{average event size in bytes + average raw data size in bytes} x {events per
second x .0003 compression coefficient = network bandwidth in Kbps (kilobits per
second)
```

For example, at 500 EPS for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, the network bandwidth utilization is determined as follows:

```
(464 bytes + 300 bytes} x 500 EPS x .0003 = 115 Kbps
```

2.1.7 Setting Up Your Virtual Environment

Change Guardian is extensively tested and fully supported on a VMware ESX server. When you set up a virtual environment, the virtual machine must have two or more CPUs. To achieve comparable physical computer performance results in a virtual environment, the virtual environment should provide the same memory, number of CPUs, disk space, and I/O as the physical computer recommendations.

For more information, see "Hardware Requirements" on page 16.

2.1.8 Understanding Port Usage by the Change Guardian Server

The Change Guardian server uses a number of local and network ports for internal and external communication.

Local Ports

Change Guardian uses the TCP port 5432 for internal communication with the PostgreSQL database. You do not need to open this port by default.

Network Ports

The Change Guardian server uses various ports for external communication with other components. The appliance installation opens the ports on the firewall by default. However, when performing the standard installation, you must configure the operating system on which you are installing the Change Guardian server to open the ports on the firewall.

Ensure the following ports are open on the firewall.

Ports	Description
TCP 1099 and 2000	Used together by monitoring tools to connect to the Change Guardian server process using Java Management Extensions (JMX).
TCP 8443	Used for HTTPS communication.
TCP 8094	Used by the Change Guardian Policy Repository and for syslog event forwarding.

Change Guardian Server Appliance Ports

In addition to the above ports, the following ports are open when you install the Change Guardian server appliance.

Ports	Description
TCP 22	Used for secure shell access to the Change Guardian appliance.
TCP 54984	Used by the Change Guardian Appliance Management Console (WebYaST). Also used by the Change Guardian appliance for the update service.
TCP 443	Forwarded to 8443 for HTTPS communication.
TCP 1290	Used to connect through the SuSE Firewall.
UDP and TCP 40000 - 41000	Used when configuring data collection servers, such as syslog. Change Guardian does not listen on these ports by default.

2.2 Completing Prerequisites for SLES 11 SP 2 and RHEL 6

You must complete all the prerequisites described in this section to install any of the Change Guardian server components on RHEL 6 or SLES 11.

2.2.1 Prerequisites for RHEL 6

You must perform the following steps before you can install the Change Guardian server to a computer running RHEL 6:

1. Install the common libraries. SLES 11 installs the libraries by default. However, you must select the option to install the common libraries during the installation of RHEL 6.
2. Install prerequisite files for RHEL 6. On the command line, type the following:

   ```
   yum install –y libstdc++.i686 pam.i686 pcre.i686 expat.i686 openldap.i686
   libtool-ltdl.i686 compat-libstdc++-33.i686
   ```
3. Install the Legacy Support Package on computers with the RHEL 6 operating system. To install the Legacy Support package, log in to the computer as root. On the command line, type the following:

   ```
   yum install "Legacy Software Support"
   ```

2.2.2 Prerequisites for SLES 11 SP 2

The Change Guardian server requires the 32-bit Runtime Environment. By default, the standard installation of SLES 11 SP 2 includes this environment. If your installation does not include the 32-bit Runtime Environment, you must perform one of the following procedures to install it.

To install the 32-bit Runtime Environment using YaST:

1. Run YaST.
2. Select **Software Management**.
3. Select **Patterns**.

4 In the Base Technologies category, select **32-Bit Runtime Environment**.

5 Click **Accept**, and follow the prompts.

To install the 32-bit Runtime Environment using the command line:

You can also use the Linux command line to install the 32-bit Runtime Environment. Log in as root, and type the following command:

```
zypper install –t pattern 32bit
```

2.2.3 Verifying the Host Name Returns Properly

For the Change Guardian server installer to work correctly, ensure the Linux system can return the host name. You must add the host name to the line in the `/etc/hosts` file containing the IP address. For example, `127.0.0.1`, and then enter *hostname* `-f` to ensure the hostname displays properly.

You have the option to install the Change Guardian server using an address, rather than a host name. If you install using this option, use the `configure.sh` utility, which is available in the `$INSTALL_ROOT/netiq/cg/scripts directory`, after you install the Change Guardian server.

To use the configuration utility, type `./configure.sh` on the command line.

2.2.4 Changing the Kernel SHMMAX Parameter to Enable PostgreSQL

You must change the kernel SHMMAX parameter to enable the PostgreSQL database to run on the Linux server.

To change the kernel SHMMAX parameter, append the following information to the `/etc/sysctl.conf` file.

```
# for Sentinel Postgresql
kernel.shmmax=1073741824
```

2.2.5 Ensuring Ports Are Open

Depending on the installation you choose, you must open the ports listed in Section 2.1.8, "Understanding Port Usage by the Change Guardian Server," on page 20. If the firewall blocks any of these ports, or if they are not open, the Change Guardian server cannot communicate with the monitored computers or the Change Guardian Policy Editor.

To open a port, enter the following at the command line:

```
iptables -I INPUT -p tcp --dport port_number -j ACCEPT
```

Save the changes in the firewall using the following commands, depending on the operating system that you use:

- On RHEL:

  ```
  service iptables save
  ```

- On SLES:

  ```
  iptables-save
  ```

2.3 Understanding Change Guardian Server Installation Types

You can install the Change Guardian server on a computer running the SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 or the Red Hat Enterprise Linux (RHEL) 6 operating system. You can also use an appliance installation, which installs both the SLES 11 SP 2 64-bit operating system and the Change Guardian server. This section describes the installation types available for the Change Guardian server.

This section describes the installation types available for the Change Guardian server.

2.3.1 Installation to a Server with SLES 11 Service Pack 2 or RHEL 6

Use one of the following methods for installation:

Interactive

The installation proceeds with user input. During installation, you can record the installation options (user input or default values) to a file, which you can later use for silent installation. This installation method allows for either a standard or a custom configuration.

Silent

The installation uses pre-recorded options. The silent installation refers to the file that has the recorded installation input and performs the installation with the values captured in the file. Use the silent installation method when you want to install many instances of the same configuration in your environment. For more information, see Section 3.4, “Performing a Silent Installation,” on page 29.

Standard and Custom Installation

Use one of the following configurations when you install using the interactive method:

Standard

In this configuration, the installation uses default values during the configuration setup, and requires minimal input. For more information, see Section 3.3.1, “Standard Configuration,” on page 26.

Custom

In this configuration, the installation prompts you to specify the values during the configuration setup. You can either select the default values, or specify the necessary values. For more information, see Section 3.3.2, “Custom Configuration,” on page 28.

Standard Configuration	Custom Configuration
Installs with the default 90-day evaluation key.	Installs with the 90-day license key, or with a valid license key.
Installs with the same default password for the admin, dbauser, and appuser.	Allows you to either keep the default password or change the password for the admin, dbauser, and appuser.
Installs the default ports for all the components.	Allows you to specify ports for different components.
Authenticates users with the internal database.	Authenticates users with the internal database, or with LDAP authentication.

Standard Configuration	Custom Configuration
	Allows you to change the installation location.
	Allows you to specify that agents resolve the Change Guardian server by host name or IP address.

2.3.2 Installing the Appliance

This release offers a ready-to-run software appliance built on SUSE Studio. Delivered as a VMware, Xen, or ISO image, and certified to run on all major hypervisors, the software appliance enables a cost-effective, less complex Change Guardian deployment. You can install the software appliance on hardware or in a virtual environment.

The appliance installation type combines a hardened SUSE Linux Enterprise Server (SLES) 11 SP 1 operating system and the Change Guardian server software integrated update service to provide an easy and seamless user experience that allows customers to leverage existing investments. For more information, see Section 3.5, “Installing the Change Guardian Server Appliance,” on page 30.

3 Installing the Change Guardian Server

The Change Guardian server is a Linux-based server containing Change Guardian components, including those required for policy and event storage, as well as communication with monitored computers and computers to which you want to forward events.

This chapter describes the procedure for installing the Change Guardian server on a computer running the SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 or the Red Hat Enterprise Linux (RHEL) 6 operating system.

3.1 Implementation Checklist for the Change Guardian Server

Verify that you have completed the following tasks before you start the installation:

	Checklist Items
❑	Verify that your hardware and software meet the system requirements. For more information, see Section 2.1, “System Requirements,” on page 15.
❑	Use the `hostname -f` command to ensure the operating system returns the host name. For more information, see Section 2.2.3, “Verifying the Host Name Returns Properly,” on page 22. **NOTE:** If you plan to install the Change Guardian server using an IP address, rather than a host name, use the configuration utility after installation to verify the server configuration. For more information, see Section 2.2.3, “Verifying the Host Name Returns Properly,” on page 22.
❑	Obtain your license key if you plan to install the licensed version.
❑	Synchronize time by using the Network Time Protocol (NTP).
❑	***If you install the Change Guardian server appliance***, ensure that the ports listed in Section 2.1.8, “Understanding Port Usage by the Change Guardian Server,” on page 20 are opened in the firewall.
❑	***If you plan to perform an appliance installation***, you must also: ◆ Obtain your license key if you plan to install the licensed version. ◆ Obtain your registration code to register for software updates. For more information, see Section 3.5, “Installing the Change Guardian Server Appliance,” on page 30.

3.2 Understanding Installation Options

On the command line, type `/install-changeguardian.sh --help` to display the following installation options.

Options	Value	Description
`--location`	Directory	Specifies a directory other than the root (/) to install Change Guardian.
`-m, --manifest`	File name	Specifies a product manifest file to use instead of the default manifest file.
`--no-configure`		Specifies to not configure the product after installation.
`-n, --no-start`		Specifies to not start or restart Change Guardian after installation or configuration.
`-r, --recordunattended`	File name	Specifies a file to record the parameters you can use for silent installation.
`-u, --unattended`	File name	Uses the parameters from the specified file for silent installation of the Change Guardian server on unattended computers.
`-h, --help`		Displays the options you can use while installing Change Guardian.
`-l, --log-file`	File name	Records log messages to a file.
`--no-banner`		Suppresses the display of the banner message.
`-q, --quiet`		Displays fewer messages.
`-v, --verbose`		Displays all messages during installation.

3.3 Performing an Interactive Installation

This section describes the interactive method of installing the Change Guardian server using the standard configuration and the custom configuration. Using the interactive method, you can record your installation options (user inputs or default values) to a file, which you can later use for silent installation.

3.3.1 Standard Configuration

The standard configuration option installs the Change Guardian server using default values. The only required input is the password.

To install the Change Guardian server using a standard configuration:

1. Download the Change Guardian server installation file, or insert the Change Guardian server installation CD.
2. Extract the Change Guardian server installation file.
3. On the command line, type the following command to extract the installation file:

   ```
   tar -zxvf install_cgserver-4.0.0-xx.x86_64.tgz
   ```

4 Install the Change Guardian server. Type the following command in the root of the extracted directory to install the Change Guardian server:

```
./install-changeguardian.sh
```

To install the Change Guardian server on more than one system, you can record your installation options in a file. Use this file for a silent Change Guardian server installation on other computers. To record your installation options, specify the following command:

```
./install-changeguardian.sh -r response_filename
```

5 Type the number for the language you want to use for the installation, and then press **Enter**.

6 Press the space bar to read the license agreement.

7 Type `yes` or `y` to accept the license and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt you for the configuration type.

8 When prompted, type `1` to proceed with the standard configuration.

Installation proceeds with the 90-day Sentinel evaluation license key included with the installer. This license key activates the full set of product features for a 90-day evaluation period. At any time during or after the trial period, you can replace the evaluation license with a license key you have purchased.

9 Create a Sentinel admin password.

NOTE: The `admin`, `dbauser`, and `appuser` accounts use this password.

---

10 Confirm the password.

At this point, the Change Guardian portion of the server installation begins.

11 When prompted, type `1` to use the Change Guardian standard configuration, or type `2` to use the Change Guardian custom configuration, which allows you to change default values for the Change Guardian server installation.

12 Create a Change Guardian `cgadmin` user password.

NOTE: The `cgadmin`, `dbauser`, and `appuser` accounts use this password.

---

13 Confirm the password.

14 Set up the default email destination.

NOTE: This step is necessary if you want to email reports and events. You can skip this step, but if you later decide to email reports and events, you must use the Change Guardian server `configure.sh` script.

14a Type `y` to configure email.

14b When prompted, enter values for the following:

- SMTP Host – The full name, including domain name, of the email server from which you want to send email alerts.
- SMTP Port – The remote SMTP port used to connect. The default is 25.
- From – The return email address appearing on each email sent.
- SMTP User Name – The user name to use when connecting to the SMTP server.
- SMTP Password – The password corresponding with the entered SMTP user name.

When the Change Guardian server installation finishes, the server starts. It might take a few minutes for all services to start after installation. Wait until the installation finishes and all services start before you log in to the server.

To access the Change Guardian Web interface, specify the following URL in your Web browser:

`https://IP_Address_Change_Guardian_server:8443`

3.3.2 Custom Configuration

If you are installing the Change Guardian server with a custom configuration, you can specify the license key, change the password for different users, and specify values for different ports that are used to interact with the internal components.

To install the Change Guardian server using a custom configuration:

1. Complete Step 1 through Step 7 of the "Standard Configuration" on page 26.
2. Type `2` to perform a custom configuration of the Change Guardian server.
3. ***If you want to use the default 90-day evaluation license key for the Change Guardian server***, type `1`.
4. ***If you want to enter a purchased license key for the Change Guardian server***, type `2`.
5. Create the Sentinel `admin` user password.
6. Confirm the password.
7. Type the password for the database user `dbauser`, and confirm the password.

   NOTE: The Change Guardian server uses the `dbauser` account identity to interact with the database. Use the `dbauser` password you enter here to perform database maintenance tasks, including resetting the `admin` password if the `admin` password is forgotten or lost.
8. Type the password for the application user `appuser`, and confirm the password.
9. Change the port assignments for the Change Guardian services by entering the number, and then specifying the new port number.
10. Type `7`.
11. ***If you want to authenticate users using only the internal database***, type `1`.
12. ***If you want to authenticate users by using LDAP directory authentication, and you configured an LDAP directory in your domain***, type `2`.
13. Enter the Sentinel `admin` password.

    At this point, the Change Guardian portion of the server installation begins.
14. When prompted, type `1` to use the Change Guardian standard configuration, or type `2` to use the Change Guardian custom configuration, which allows you to change default values for the Change Guardian server installation.
15. Create a Change Guardian `cgadmin` user password.

    NOTE: The `cgadmin`, `dbauser`, and `appuser` accounts use this password.
16. Confirm the password.
17. When prompted to configure email now, type `y` or `yes`.
18. Set up the default email destination.

NOTE: This step is necessary if you want to email reports and events. You can skip this step, but if you later decide to email reports and events, you must use the Change Guardian server `configure.sh` script.

18a Type `y` to configure email.

18b When prompted, enter values for the following:

- SMTP Host – The full name, including domain name, of the email server from which you want to send email alerts.
- SMTP Port – The remote SMTP port used to connect. The default is 25.
- From – The return email address appearing on each email sent.
- SMTP User Name – The user name to use when connecting to the SMTP server.
- SMTP Password – The password corresponding with the entered SMTP user name.

When the Change Guardian server installation finishes, the server starts. It might take a few minutes for all services to start after installation. Wait until the installation finishes and all services start before you log in to the server.

To access the Change Guardian Web interface, specify the following URL in your Web browser:

`https://`*IP_Address_Change_Guardian_server*`:8443`

3.4 Performing a Silent Installation

Use the silent installation of the Change Guardian server when you need to install more than one Change Guardian server in your environment. You can record the installation parameters during the interactive installation, and then run the recorded file on all the other servers. You can record the installation parameters with either the standard configuration or custom configuration.

To install the Change Guardian server using the silent installation method:

1. Ensure that you have recorded the installation parameters to a file. For more information, see Section 3.3.1, "Standard Configuration," on page 26.
2. Download the Change Guardian server installation files, or insert the Change Guardian server installation CD.
3. Log in as `root` to the server where you want to install Change Guardian.
4. On the command line, type the following to extract the install files from the `.tar` file:

   `tar -zxvf install_`*filename*
5. On the command line, type the following to install the Change Guardian server in silent mode:

   `./install-changeguardian.sh -u response_`*file*

When the Change Guardian server installation finishes, the server starts. It might take a few minutes for all services to start after installation. Wait until the installation finishes and all services start before you log in to the server.

To access the Change Guardian Web interface, specify the following URL in your Web browser:

`https://`*IP_Address_Change_Guardian_server*`:8443`

3.5 Installing the Change Guardian Server Appliance

The Change Guardian server appliance is a ready-to-run software appliance built on SUSE Studio. The appliance combines a hardened SUSE Linux Enterprise Server (SLES) 11 SP 2 operating system and the Change Guardian server software integrated update service to provide an easy and seamless user experience that allows customers to leverage existing investments. You can install the software appliance on a virtual environment or on hardware.

3.5.1 Implementation Checklist for the Change Guardian Server Appliance

Ensure that you have completed the following tasks before you start the installation of the appliance.

	Checklist Items
❑	Verify the hardware meets system requirements. For more information, see Section 2.1, “System Requirements,” on page 15.
❑	If you plan to install the licensed version, ensure you have your license key.
❑	Ensure you have your registration code to register for software updates.

3.5.2 Installing the Change Guardian Server Appliance Using VMware

You can install the Change Guardian server on a VMware ESX 4.0 virtual platform.

To install the Change Guardian server appliance image on a VMware ESX server:

1. Download the VMware appliance installation file.

   The correct file for the VMware appliance has `vmx` in the filename.

   For example: `changeguardian_server_4.0.0.0.x86_64-0.`*`build_number`*`.0.vmx.tar.gz`
2. Establish an ESX datastore on which you can install the appliance.
3. Log in as `Administrator` to the server where you want to install the appliance.
4. Specify the following command to extract the compressed appliance image from the computer running VM Converter:

   `tar -xvf` *install_file*
5. To import the VMware image to the ESX server, use the VMware Converter and follow the instructions in the conversion wizard.
6. Log on to the ESX server computer.
7. Select the imported VMware image of the appliance and click **Power On**.
8. Select the language of your choice, and then click **Next**.
9. Select the keyboard layout, and then click **Next**.
10. Read and accept the Novell SUSE Linux Enterprise Server (SLES) 11 SP 2 Software License Agreement.
11. Read and accept the NetIQ Change Guardian End User License Agreement.
12. Specify the hostname and domain name on the Hostname and Domain Name page, and verify that the **Assign Hostname to Loopback IP** option is selected.

NOTE: Only select **Change Hostname via DHCP** if you do not have a DHCP or IP reservation.

13 Click **Next**.

14 To use the current network connection settings, select **Use the following configuration** on the Network Configuration II page.

or

To change the network connection settings, click **Change**, and then make the desired changes.

15 Set the time and date, and then click **Next**.

Use YaST from the appliance command line to change the NTP configuration after installation. For more information, see Section 3.5.6, "Configuring WebYaST," on page 35.

NOTE: You can use WebYast to change the time and date, but not the NTP configuration.

If the time appears out of sync immediately after the installation, run the following command to restart NTP:

```
rcntp restart
```

16 Set the `root` password, then click **Next**.

WARNING: The installation checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation cannot proceed.

If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended.

17 Set the Sentinel server `admin` password, and then click **Next**.

18 Set the Change Guardian server `cgadmin` password, and then click **Next**.

When the Change Guardian server installation finishes, the server starts. It might take a few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes and services start before you log in to the server.

19 Make a note of the appliance IP address shown in the console.

20 Proceed with Section 3.5.5, "Installing VMware Tools," on page 35.

3.5.3 Installing the Change Guardian Server Using a Xen Appliance

You can install the Change Guardian server on a Xen 4.0 virtual platform.

To install the Change Guardian server appliance image on a Xen server:

1 Download the Xen virtual appliance installation file to `/var/lib/xen/images`.

The correct filename for the Xen virtual appliance contains `xen`.

For example, `changeguardian_4.0.0.0.x86_64-0.`*`build_number`*`.xen.tar.gz`.

2 Before you install the Xen appliance, you must modify the `xenconfig` file as follows:

- Comment the line, `vfb = ["type=vnc,vncunused=1,vnclisten=0.0.0.0"]`.
- Add the line, `extra = "console=hvc0 xencons=tty"`

The final `xenconfig` file must be as follows:

```
# -*- mode: python; -*-
name=install_file_name
memory=4096
```

```
disk=["tap:aio:/var/lib/xen/images/install_directory/install_filename]
    vif=[ "bridge=br0" ]
    # vfb = ["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
    extra = "console=hvc0 xencons=tty"
```

3. On the command line, type the following command to unpack the file:

   `tar -zxvf install_file`

4. Change to the new installation directory. This directory has the following files:
   - *file_name*`.raw`
   - *file_name*`.xenconfig`
5. Use a text editor to open the *`file_name`*`.xenconfig` file.
6. Modify the file as follows:
   - Specify the full path to the `.raw` file in the `disk` setting.
   - Specify the `bridge` setting for your network configuration. For example, `bridge=br0` or `bridge=xenbr0`.
   - Specify values for the `name` and `memory` settings.

     For example:

     ```
     # -*- mode: python; -*-
     name="changeguardian_4.0.0.0.x86_64"
     memory=4096
     disk=[ "tap:aio:/var/lib/xen/images/changeguardian_4.0.0.0.x86_64/
     changeguardian_4.0.0.0.x86_64.raw,xvda,w" ]
     vif=[ "bridge=br0" ]
     ```
7. After you modify the *filename*`.xenconfig` file, specify the following command to create the VM:

```
xm create file_name.xenconfig
```

8. ***If you want to verify creation of the VM***, type the following on the command line:

   ```
   xm list
   ```

   The VM appears in the generated list.

   For example, if you configured `name="changeguardian_4.0.0.0.x86_64"` in the `.xenconfig` file, the VM appears with the name `changeguardian_4.0.0.0.x86_64`.
9. On the command line, type the following command to start the installation:

   `xm console` *vm_name*

   For example, using the value returned in Step 8, type the following command:

   ```
   xm console changeguardian_7.0.0.0.x86_64
   ```

WARNING: The installation checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation cannot proceed.

If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. Enter `y` if you want to continue with the installation, or enter `n` if you do not want to proceed.

---

10. Select the language of your choice, then click **Next**.
11. Select the keyboard layout, then click **Next**.
12. Read and accept the Novell SUSE Linux Enterprise Server (SLES) 11 SP 2 Software License Agreement.

13 Read and accept the NetIQ Change Guardian End User License Agreement.

14 Specify the hostname and domain name on the Hostname and Domain Name page, and verify that the **Assign Hostname to Loopback IP** option is selected.

NOTE: Only select **Change Hostname via DHCP** if you do not have a DHCP or IP reservation.

---

15 Click **Next**.

16 To use the current network connection settings, select **Use the following configuration** on the Network Configuration II page.

or

To change the network connection settings, click **Change**, and then make the desired changes.

17 Click **Next**.

18 Set the time and date, and then click **Next**.

Use YaST from the appliance command line to change the NTP configuration after installation. For more information, see Section 3.5.6, "Configuring WebYaST," on page 35.

NOTE: You can use WebYast to change the time and date, but not the NTP configuration.

If the time appears out of sync immediately after the installation, run the following command to restart NTP:

```
rcntp restart
```

19 Set the Novell SUSE Enterprise Server `root` password, then click **Next**.

20 Set the Sentinel `admin` password, then click **Next**.

21 Set the Change Guardian `cgadmin` password, then click **Next**.

When the Change Guardian server installation finishes, the server starts. It might take few minutes for all services to start after installation. Wait until the installation finishes before you log in to the server.

22 Make a note of the appliance IP address shown in the console.

23 Proceed with Section 3.5.5, "Installing VMware Tools," on page 35.

3.5.4 Installing the Change Guardian Server Appliance on Hardware

You can install the Change Guardian server ISO appliance on either a Hyper-V server or on a computer without an operating system installed. Before installing the Change Guardian appliance on the hardware, be sure you download and unpack the appliance ISO disk image, and that it is available on a DVD.

NOTE: Installation on hardware using the ISO disk image (Bare Metal & Hyper-V) requires minimum memory of 4.5 GB for the installation to complete. For more information, see Section 3.1, "Implementation Checklist for the Change Guardian Server," on page 25.

To install the Change Guardian server to hardware:

1 Boot the computer from the DVD drive with the DVD.

2 Follow the instructions of the installation wizard.

3 Run the Live DVD appliance image by selecting the top entry in the boot menu.

WARNING: The installation checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation cannot proceed.

If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. Enter `y` if you want to continue with the installation, or enter `n` if you do not want to proceed.

4. Select the language of your choice, then click **Next**.
5. Select the keyboard layout, then click **Next**.
6. Read and accept the Novell SUSE Enterprise Server Software License Agreement.
7. Read and accept the NetIQ Change Guardian End User License Agreement.
8. Select **Next**.
9. On the Hostname and Domain Name page, specify the host name and domain name, and then select **Assign Hostname to Loopback IP**.
10. Select **Next** to save the host name configurations.
11. ***If you want to use the current network connection settings,*** select **Use the following configuration** on the Network Configuration II page.
12. ***If you want to change the network connection settings,*** click **Change**, and then make the necessary changes.
13. Click **Next**.
14. Set the time and date, and then click **Finish**.

    Use YaST from the appliance command line to change the NTP configuration after installation. For more information, see Section 3.5.6, "Configuring WebYaST," on page 35.

    NOTE: You can use WebYast to change the time and date, but not the NTP configuration.

    If the time appears out of sync immediately after the install, run the following command to restart NTP:

    ```
    rcntp restart
    ```

15. Set the `root` password, then click **Next**.
16. Set the Change Guardian `admin` password, then click **Next**.
17. Enter the user name and password at the console to log in to the appliance.

    The default value for the user name is `root`. Use the password you set in Step 15.
18. Stop the Change Guardian server. On the command line, type the following:

    ```
    service sentinel stop
    ```

19. On the command line, type the following command to reset the user interface for a clear display in YaST:

    ```
    reset
    ```

20. On the command line, type the following to install the appliance on the physical server:

    ```
    /sbin/yast2 live-installer
    ```

    It might take a few minutes for all services to start up after installation because the system performs a one-time initialization. Wait until the installation finishes and services start before you log in to the server.
21. Make a note of the appliance IP address that is shown in the console.
22. Install VMware Tools. For more information, see Section 3.5.5, "Installing VMware Tools," on page 35.

3.5.5 Installing VMware Tools

For the Change Guardian server to work effectively on the VMware server, you need to install VMware Tools. The VMware Tools suite of utilities enhance the performance of operating system on a virtual machine's. The tools also improve management of virtual machines. For more information on installing VMware Tools, see VMware Tools for Linux Guests.

For more information on the VMware documentation, see *Workstation User's Manual*.

3.5.6 Configuring WebYaST

The Change Guardian server appliance user interface includes WebYaST, which is a Web-based remote console for controlling appliances based on SUSE Linux Enterprise. You can access, configure, and monitor the Change Guardian server appliances with WebYaST. The following procedure briefly describes the steps to configure WebYaST. For more information on detailed configuration, see the *WebYaST User Guide* at http://www.novell.com/documentation/webyast/.

To configure WebYaST:

1. Log in to the Change Guardian appliance.
2. Click **Appliance**.
3. Configure the Change Guardian server to receive updates.
4. Click **Next** to finish the initial setup.

3.5.7 Configuring the Appliance with the Subscription Management Tool

In secured environments where the appliance must run without direct Internet access, you can configure the appliance with the Subscription Management Tool (SMT). This tool enables you to upgrade the appliance to the latest versions of Change Guardian. SMT is a package proxy system that is integrated with Novell Customer Center and provides key Novell Customer Center capabilities.

For information on configuring the appliance with SMT, see "Configuring Clients to Use SMT" in the SMT documentation.

4 Installing the Change Guardian Policy Editor

The topics in this chapter guide you through the planning considerations before installing the Change Guardian Policy Editor. If you want to install a custom configuration not identified in the sections that follow, or if you have any questions, contact NetIQ Technical Support.

4.1 Policy Editor Computer Requirements

You must install the Policy Editor on a computer running one of the following operating systems:

- Windows XP (32- and 64-bit version)
- Windows Server 2003 (32- and 64-bit version)
- Windows Server 2008 (32- and 64-bit version)
- Windows Server 2008 R2
- Windows 7 (32- and 64-bit version)
- Windows Vista (32- and 64-bit version)

NOTE: If you install the Policy Editor on a computer running Microsoft Windows XP (64-bit) or Windows 2003 (64-bit), you must install Microsoft Windows Hotfix 942589. For more information, see support.microsoft.com/kb/942589.

In addition, the Policy Editor computer must include Microsoft .NET Framework 3.5 Service Pack 2 or later.

4.2 Implementation Checklist for the Policy Editor

Complete the following steps before you install the Policy Editor and its components.

	Checklist Items
❑	Install the Change Guardian server. For more information, see Chapter 3, “Installing the Change Guardian Server,” on page 25.
❑	Install a version of Microsoft .NET Framework 3.5 SP 1 or later. For more information, see Section 4.1, “Policy Editor Computer Requirements,” on page 37.
❑	If you are installing the Policy Editor on a computer running Microsoft Windows XP (64-bit) or Microsoft Windows 2003 (64-bit), you must install Microsoft Windows Hotfix 942589. For more information, see support.microsoft.com/kb/942589.

4.3 Installing Change Guardian

This section explains how to install the Policy Editor and the Change Guardian agents. Follow the procedures to install the Policy Editor, Change Guardian agents, and to connect to the Change Guardian Policy Repository. For more information, see Section 4.1, "Policy Editor Computer Requirements," on page 37.

4.3.1 Selecting Components to Install

The setup program allows you to perform the following tasks:

Install Change Guardian Policy Editor

The Policy Editor interface lets you install Change Guardian modules, configure monitoring policies, and assign monitoring policies to monitored computers.

Install Change Guardian Agent

Change Guardian agents allow the modules to monitor computers for change. You can choose from the following agent installation options:

- Install the agent only.
- Create the silent installer only.
- Install the agent locally and create the silent agent installer, which allows you to install the agent on the computers you want to monitor.

NOTE: The default location for the silent agent installer is your desktop.

For more information, see Section 1.2.2, "Understanding Change Guardian Agents," on page 12.

Uninstall Old Change Guardian Modules

This option allows customers upgrading from previous versions of Change Guardian for Windows or Change Guardian for Group Policy to remove agents for those products before installing the current agent.

4.3.2 Running the Change Guardian Installation Program

This section describes how to install Change Guardian components.

To install the Policy Editor:

1. Log on to the computer with an administrator account.
2. Close all open applications.
3. Run the installation program (`setup.exe`) from the Change Guardian installation kit and follow the instructions.

4 When prompted, enter the following information:

Communication Settings	Enter the port number to use to communicate with the agent computers. The default port is 8094.
Policy Repository Information	Enter the following information to communicate with the Change Guardian server: ◆ **Repository Computer**: Enter the fully-qualified host name or the IP address of the Change Guardian server. ◆ **Communication Port**: Enter the port used to communicate with the Policy Repository. NetIQ recommends using port 8094. ◆ **Password:** Enter the `cgadmin` password you created when you installed the Change Guardian server. **NOTE:** This option appears when you choose to install the agent.

5 On the Summary window, review your installation options. Click **Back** to change your options, or click **Install** to install Change Guardian.

6 When the installation completes, click **Finish**.

4.4 Performing a Silent Agent Installation

When you install the Policy Editor, you can choose the **Change Guardian Agent** option, which installs the agent on the local computer. Selecting the option also instructs the setup program to save the communication settings you choose during installation to an agent silent installer file, and then save the file to the Policy Editor computer when installation completes.

To silently install the agent to a computer you want to monitor, copy the `NetIQ Change Guardian.msi` file from your Policy Editor computer to each computer you want to monitor. Run the file either from the command line, or by using a third-party product. For more information about using the Microsoft Windows Installer from the command line, see "Msiexec (command-line options)" in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/cc759262(v=ws.10)). You can also copy the file to a network file share, and use a script to distribute the file and execute it on computers you want to monitor.

NOTE: If you want to enable browsing for items like files, processes, and users on the monitored computer, you must open port 8094 on the computer's firewall.

To remove the agents from a computer, use the Control Panel utility for adding and removing programs. For more information, see Section 1.2.2, "Understanding Change Guardian Agents," on page 12.

4.5 Using the Change Guardian Module Manager

The Change Guardian Module Manager provides you with information about licensed modules, allows you to import module licenses to the Policy Editor, and allows you to remove module licenses from the Policy Editor. To use the Module Manager, start the Policy Editor, click **NetIQ Change Guardian**, and then select **Module Manager** in the navigation pane.

When you install Change Guardian, you install all available modules. You must import the license key for each module you want to use. To import license keys, click **Import License Key**, and then select the license key for the modules you want to use. After you import the license keys, you can use the module to create and assign policies.

You can use the Module Manager to remove one or more module licenses. To remove a license key, select the license you want to remove, and then click **Delete License Key**.

5 Installing the UNIX Agent and UNIX Agent Manager

This chapter provides information about installing the UNIX agent on computers you want to monitor and using UNIX Agent Manager. This chapter also provides an overview of how to manage users using UNIX Agent Manager.

To install UNIX agent, complete the following checklist:

❑	Ensure you have the necessary environment. For more information, see Section 5.1, “System Requirements,” on page 42.
❑	Install UNIX Agent Manager. See Section 5.2, “Installing UNIX Agent Manager,” on page 43.
❑	Install the agent on the computer you want to manage. ◆ For information about how to install on a local computer, see Section 5.3, “Installing the Agent on the Local Computer,” on page 44. ◆ For information about how to install using an answer file, see Section 5.4.2, “Silently Installing on the Agent Computer,” on page 45. ◆ For information about how to install, or deploy, to one or more computers from the console, see Section 5.4.1, “Deploying the UNIX Agent Using UNIX Agent Manager,” on page 44.
❑	Ensure auditing is configured on your operating system. For more information about configuring auditing, see Appendix C, “Configuring Operating System Auditing,” on page 85.
❑	Install any agent hotfixes applicable to your environment. For information about how to install patches to the console and the UNIX agent, see Section 5.5, “Applying Patches to the UNIX Agent and UNIX Agent Manager,” on page 47.
❑	Set up UNIX agent users in UNIX Agent Manager. For information about how to define users, see Section 5.7, “Using UNIX Agent Manager to Configure Access to the UNIX Agent,” on page 48.

5.1 System Requirements

For the latest information about specific supported software versions and the availability of updates, visit the Change Guardian for UNIX Supported Products page.

The UNIX agent, when used with Change Guardian, has the following system requirements.

Item	Requirement
Operating system on agent computers	One of the following: ◆ CentOS ◆ HP-UX ◆ IMB AIX ◆ Oracle Linux ◆ Oracle Solaris ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server
Operating system on UNIX Agent Manager computers	One of the following: ◆ Oracle Solaris ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server ◆ Windows 7 (32-bit and 64-bit) ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit)
Memory on UNIX agent computers	UNIX agents require the following: ◆ 128 MB RAM ◆ 512 MB swap file (virtual memory)
Memory on UNIX Agent Manager computers	512 MB
Hard disk space on UNIX agent computers	350 MB plus 400 Bytes per inode used by local file systems
Hard disk space on UNIX Agent Manager computers	1.2 GB
Default port assignments	UNIX agents use the following default ports: ◆ 2620: Communication with UNIX Agent Manager. ◆ 8094: Communication with the Change Guardian Policy Repository.
Accounts	The UNIX Deployment wizard uses the su command to access the root account on the computer on which you want to install UNIX agents. The root password is used by the wizard only at installation and is not stored.

5.2 Installing UNIX Agent Manager

NetIQ UNIX Agent Manager is a console that you can use to manage all your UNIX agent components across your enterprise. UNIX Agent Manager runs on Windows, Solaris, and Linux. You can use UNIX Agent Manager to install to several computers at the same time. UNIX Agent Manager also allows you to see any UNIX computers that other NetIQ products monitor.

UNIX Agent Manager includes a server component and a console. This section guides you through installing UNIX Agent Manager components on Windows, UNIX, or Linux computers.

5.2.1 Installing UNIX Agent Manager on a Microsoft Windows Computer

Complete the following steps to install either the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Windows computer.

To install UNIX Agent Manager on a Windows computer:

1. Log on to the Windows computer using a local administrator account.
2. Run `UAMInstaller.MSI` in the root folder of the installation kit, and begin responding to the questions in the wizard.
3. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms. This option is not yet viable for the Change Guardian environment. If you select that option, UNIX Agent Manager cannot manage agents that work with Change Guardian.
4. Complete the automatic installer wizard. The wizard guides you through installing the UNIX Agent Manager to the folder that you specify.
5. Start the UNIX Agent Manager server.
6. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.

5.2.2 Installing UNIX Agent Manager on a UNIX or Linux Computer

Complete the following steps to install either the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Solaris, Red Hat, or SUSE computer.

To install the UNIX Agent Manager on a UNIX or Linux computer:

1. Change directories to where you copied the installation package for UNIX Agent Manager. In the installation package, change directories to where the installation files are located.
2. Uncompress the appropriate `.tar.gz` file for your platform.
3. Start the UNIX Agent Manager server by running the `runserver.sh` script.
4. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.
5. Start the UNIX Agent Manager console by running the `run.sh` script.

5.3 Installing the Agent on the Local Computer

The following procedure guides you through logging on to an agent computer and locally installing to that computer.

To install an agent on the local computer:

1. Log on to an agent computer using the root account.
2. Change directories to the product installation package, and then enter the following command to start the install script:

   ```
   /bin/sh ./install.sh
   ```

3. Proceed through the prompts.
4. When you are given the option to configure the agent for use with other products, select the option only if you run NetIQ Secure Configuration Manager, NetIQ AppManager, or NetIQ Security Manager to monitor the computer. If you will not use those products, type n instead of accepting the default response of y for those questions.
5. When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 5.8, "Restart Methods for the UNIX Agent," on page 48.

When you finish the installation process, the UNIX agent starts the daemons.

5.4 Installing the UNIX Agent

You can install the agent locally on the computer you will monitor, by deploying from UNIX Agent Manager, or without user interaction by using an answer file.

5.4.1 Deploying the UNIX Agent Using UNIX Agent Manager

Remote deployment provides a convenient and uniform method for installing one or more UNIX agents. You can use the Deployment wizard provided in the UNIX Agent Manager for remote deployment, unless one of the following conditions exists:

- Your site standards prohibit your access to root passwords.
- Your site standards require a specific software distribution mechanism.
- Your site standards prohibit software distribution mechanisms.

For information about installing UNIX Agent Manager, see Section 5.2, "Installing UNIX Agent Manager," on page 43.

To remotely deploy UNIX agent components:

1. In the **File** menu of UNIX Agent Manager, select **Remote Deployment**.
2. Click the **Add Host** button and fill in the fields as prompted.
3. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms. This option is not yet viable for the Change Guardian environment. If you select that option, UNIX Agent Manager cannot manage agents that work with Change Guardian.

4 When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 5.8, "Restart Methods for the UNIX Agent," on page 48.

5 Proceed through the wizard to complete installation.

5.4.2 Silently Installing on the Agent Computer

Performing a silent installation allows you to install the UNIX agent without interactively running the installation script. Instead, silent installation uses an installation file that records the information required for completing the installation. Each line in the file is a *name=value* pair that provides the required information, for example, `HOME=/usr/netiq`.

If you use the deployment wizard to perform a local installation on one computer, the wizard offers you an opportunity to create a silent installation file based on your choices. A sample installation file, `SampleSilentInstallation.cfg`, is located on your UNIX agent download package. The following parameters are available for silent installation for the NetIQ UNIX Agent working with Change Guardian.

Parameter	Description
`FRESH_INSTALL`	Specifies whether you want the install program to install the agent only as defined in the silent install file, or if you want to use the installation to add product support to an existing agent. Valid entries are `1`, to install the agent normally and `0`, to add an additional product to an existing agent installation. The default is `1`.
`CREATE_TARGET_DIR`	Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are `y` and `n`. The default is `y`.
`CONTINUE_WITHOUT_PATCHES`	Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are `y` and `n`. The default is `n`.
`IQCONNECT_PORT`	Specifies the port that the UNIX agent uses to communicate with UNIX Agent Manager. The default is `2620`.
`IQ_STARTUP`	Specifies restart method for the uagent process. This process is used by the UNIX agent for the Change Guardian, AppManager, Security Manager, and Secure Configuration Manager products. For information about the options, see Section 5.8, "Restart Methods for the UNIX Agent," on page 48. Valid entries are `rclink` and `inittab`. The default is `rclink`.

Parameter	Description
USE_FIPS_COMMON	Specifies whether the UNIX agent communicates with UNIX Agent Manager using only Federal Information Processing Standard (FIPS) encrypted algorithms. Ensure this is set to 0. This option is not yet viable for the Change Guardian environment. If you select that option, UNIX Agent Manager cannot manage agents that work with Change Guardian.
INSTALL_CGU	Specifies whether the UNIX agent works with Change Guardian. Valid entries are y and n.
IQRM_ADDR	Specifies the IP address of the computer where you installed the Change Guardian Policy Repository.
IQRM_PORT	Specifies the port that the UNIX agent will use to communicate with the Change Guardian Policy Repository. The default is 8094.
IQRM_USER	Specifies the account that the UNIX agent uses when accessing the Change Guardian Policy Repository.
IQRM_PASS	Specifies the password for the account that the UNIX agent uses when accessing the Change Guardian Policy Repository.
IQCONFIG_RECONNECT	Specifies how often, in minutes, the UNIX agent checks for new information in the Change Guardian Policy Repository. For example, 2.
CGU_STARTUP	Specifies restart method for the detectd process. For information about the options, see Section 5.8, "Restart Methods for the UNIX Agent," on page 48. Valid entries are rclink and inittab. The default is rclink.
MANAGE_AUDIT_LOGS	Specifies whether the UNIX agent reduces the size and removed old audit logs. Valid entries are y and n.
AUDIT_LOG_SIZE	Specifies the maximum size, in bytes, that the UNIX agent allows an audit log to reach before starting a new log.
AUDIT_LOG_RETENTION	Specifies the number of audit logs that the UNIX agent keeps. Once this number of audit logs exists, the agent will delete old logs when making new ones.
KEEP_OLD_AGENT_DIR	Specifies whether to keep the previous installation directory when you are upgrading from version 7.1 of the UNIX agent. Valid entries are y and n.
OLD_INSTALL_DIR_MOVED	Specifies the directory where you want the installation program to move the previous installation directory.

Once you have created the installation file, you can run the silent installation from the command line. For example:

```
./install.sh <Target_Directory> -s <SilentConfigurationFile>.cfg
```

Where <Target_Directory> is the directory you want to install to and <SilentConfigurationFile> is the file name you used to specify the installation options. You can also use the default configuration file, `SampleSilentInstallation.cfg`.

The script will then extract information from the installation file and install the agent according to the values you have specified.

NOTE: The installation filename must be specified as an absolute path. By default, `SampleSilentInstallation.cfg` is located in the UNIX agent install directory.

5.5 Applying Patches to the UNIX Agent and UNIX Agent Manager

NetIQ provides patches in a zipped file known as a **p-ball** for agent components and in a zipped file with the extension `.um` for UNIX Agent Manager.

Patches to UNIX Agent Manager are applied to the UNIX Agent Manager server, which automatically applies any required changes to the consoles using that server. To install patches to UNIX Agent Manager, right-click on the UNIX Agent Manager server icon in the task bar at the bottom of the screen.

To upgrade the agent computer using the UNIX Agent Manager:

1. Click **Patch > Patch Manager**.
2. Click **Load Patch** to add the patch you want to apply to the list of available patches.
3. Select the computers where you want to apply the patch.
4. Select the patch or patches that you want to apply.
5. Click **Start Install**. The time necessary to update your agents depends on the number of agents to update, distance from the UNIX Agent Manager server, network connectivity, and bandwidth, among other factors. This process can take up to 20 minutes per agent.
6. Click **Back** to close the Patch Manager.

5.6 Uninstalling UNIX Agents and UNIX Agent Manager

You can uninstall the UNIX agent components manually or using UNIX Agent Manager.

5.6.1 Uninstalling the UNIX Agent

You can use UNIX Agent Manager to uninstall agents from remote computers, or you can uninstall them locally. When you uninstall the agent, all agent components, including AppManager, Change Guardian, Security Manager, and Secure Configuration Manager, are uninstalled.

NOTE: You do not need to uninstall agents with a lower version number before upgrading agents. Use this procedure only if you want to completely remove agents from remote computers. For more information about upgrading agents, see Section 5.9, “Saving UNIX Agent Information to a File,” on page 49.

To uninstall the agent locally, change to the installation directory, then run the following command:

```
./uninstall.sh
```

You can also uninstall using the console. This option allows you to uninstall from many computers at once. To uninstall an agent in UNIX Agent Manager, select the computers where you want to uninstall the agent, click **Manage Hosts > Uninstall Agent**.

5.6.2 Uninstalling UNIX Agent Manager

To uninstall the UNIX Agent Manager on Windows computers, use the **Add/Remove Programs** Control Panel to remove the **UNIX Agent Manager** program.

To uninstall the UNIX Agent Manager on a Linux computer, change directories to the UNIX Agent Manager installation directory, and then enter `rm -rf UAM`.

5.7 Using UNIX Agent Manager to Configure Access to the UNIX Agent

UNIX Agent Manager allows administrators to control user access to features and computers. To log into any UNIX Agent Manager server, an administrator on that server must create the user account in the UNIX Agent Manager Administrator Console, which is part of the UNIX Agent Manager console.

You can grant different permissions to each user account that allows access to only the features required by that user's role. Permission sets allow you to simplify this process. Permission sets define product, computer, and feature access. Once you create a permission set, you can assign it to multiple user accounts with the same role.

For example, you can create a permission set that grants access to all Change Guardian functionality separate from AppManager functionality. You can then assign this permission set to all computers running Change Guardian. When you grant a new Change Guardian user access to a console, simply assign the user to the Change Guardian permission set to grant them access to the applicable features and computers.

To assign permissions, log into a UNIX Agent Manager console as an administrator and click **Access Control** > **Admin Console**. From there, add the users that need access to that UNIX Agent Manager server, then assign the appropriate permissions.

5.8 Restart Methods for the UNIX Agent

NetIQ recommends that you accept the default, rclink. However, the following start methods are available.

Option	Description
`rclink`	Starts the agent daemons immediately after the deployment process and adds a startup script to the `/etc/rc.d` directory. This startup script starts the agent daemons after each reboot when the master rc script runs. This is the default method, and should be used in nearly all environments.

Option	Description
`inittab`	Starts the agent daemons immediately after the deployment process and adds an entry to the `/etc/inittab` file. This inittab file entry starts the agent daemons at the default run level after each reboot.
`inetd`	Configures the (x)inetd daemon to start the agent daemons when needed and then stop and unload the agent daemons.

5.9 Saving UNIX Agent Information to a File

The UNIX Agent Manager server stores the information about the UNIX agents you monitor. However, storing the information to a separate file can be useful for backups or for copying the server to another computer. You can store your UNIX agent list and configuration information in a file outside the UNIX Agent Manager server by clicking **Manage Hosts > Export/Import Host Lists** in UNIX Agent Manager.

6 Setting Up Your Environment for Monitoring

This chapter guides you through using the Change Guardian Policy Editor, including assigning policies, creating policy sets, setting group membership, and creating reports.

6.1 Logging into Change Guardian

When you start the Policy Editor, you must log into the Policy Repository running on a Change Guardian server, which allows you to submit and assign policies and policy sets to the computers and asset groups in your enterprise. You can omit this step by choosing to automatically log in to the Policy Editor. If your Change Guardian installation includes more than one Policy Repository, you can select **Settings > Connection** to select a different default Policy Repository computer.

6.2 Creating Policies and Policy Sets

Change Guardian **policies** allow you to define how Change Guardian monitors assets in your environment. Change Guardian modules each include several policy types for the respective platforms they support. Policy sets allow you to group policies together to organize and to assign monitoring.

6.2.1 Understanding Policies

A policy includes one or more constraints to define a specific change event you want to monitor in your enterprise.

Policies allow you to identify the monitoring target, and then add any combination of the following constraints:

- Add filters to more precisely narrow the monitoring target and results
- Define managed users for the activity
- Assign event contexts to categorize policies

Designating Managed Users

The **Events are considered managed for** pane allows you to specify one or more users as managed users authorized to perform the action on the asset the policy monitors. For more information, see Section 1.2.1, “Understanding Managed and Unmanaged Users,” on page 11.

You can also specify user groups as managed users. As group membership changes, Change Guardian synchronizes policies with the new group members. For more information, see Section 6.3, “Understanding Resource Expansion,” on page 54.

Understanding Event Context

You can use **event context** to categorize a policy and specify the purpose of the policy to other members of your enterprise. When you create a policy, you can select one or more options to describe the policy by such contexts as risk, vulnerability, and regulation compliance. Events generated by these policies include the event contexts. You can select from a list of default event context options or create additional contexts.

Risk Domain

Categorize the risk domain of the event as follows:

- operational continuity
- financial viability
- reputation and good will
- civil
- criminal
- environmental
- intangible

Risk

Categorize events associated with operational continuity, financial viability, corporate reputation, civil, criminal, environmental, Intangible, Information security, Information integrity

Sensitivity

Categorize event sensitivity level as Public, Internal, Restricted, Confidential, or Secret.

Regulation/Policy

You can classify monitoring policies as compliant with regulatory compliance such as Sarbanes-Oxley, PCI-DSS, FDA Part 11, GLBA, FISMA, HIPAA, COBIT, NIST, AS 3806, APRA, and C-SOX.

Control/Classification

User-defined String

Response Window

User-defined String

Submitting a Policy

When you use a Change Guardian module to create and modify a policy, you can save your changes in one of the following three states:

Policy revision saved

Policy saved as a new revision to the Policy Editor computer. Only the policy author can access the policy. You can retain multiple revisions of each policy.

Submitted

Policy saved as a new revision to the Policy Repository. Other users can access submitted policies, but you cannot assign a policy to computers or computer groups until you enable it.

Enabled

Policy saved as a new revision to the Policy Repository. Other users can access the policy. This option also enables the policy revision, which makes the saved revision of the policy available for assignment. If you modified a policy revision already assigned to computers, this option updates that policy to all computers with the policy assigned.

You cannot enable or assign policies, or make policies available to others, until you submit policies to the Policy Repository.

Enabling a Policy Revision

When you submit a policy to the Policy Repository, you must enable the policy before you can assign it to monitor computers or asset groups. You can choose whether to enable the policy immediately, or choose to submit the policy without enabling it. Later, you can enable the policy from the selected module window.

To enable a policy revision from a Change Guardian module window:

1. In the left pane, select the policy.
2. Select the **History** tab.
3. Select the version of the policy you want to enable.
4. Click **Enable**.

Loading a Policy Revision

When you make changes to a policy and then submit that policy, Change Guardian creates a new revision of that policy in the Policy Repository. You can view all revisions of a policy stored in the Policy Repository. Policy revisions allow you to keep and share works in progress, and you can choose to load a previous revision of the policy to edit or enable. The **History** tab displays the version number of the currently loaded policy, and the version number of the currently enabled policy.

The Properties pane contains information about the loaded policy, including the version number. Change Guardian indicates the enabled policy version by displaying a check mark in the **Enabled** column of the lower table.

Exporting and Importing a Policy Revision

Change Guardian allows you to export a policy to an `.xml` file. You can import the `.xml` file for future use as a new policy. You can modify an imported policy to easily create a new policy with a similar definition.

Cloning a Policy

Cloning a policy allows you to quickly create a new policy based on a selected existing policy, and then make needed changes. Change Guardian uses the enabled version of the selected policy. If no enabled version of the policy exists, Change Guardian clones the last submitted version of the selected policy.

6.2.2 Understanding Policy Sets

The Policy Set Manager allows you to combine multiple policies from one or more Change Guardian modules to form policy sets. Policy sets allow you to organize and manage monitoring needs for a specific use case. Also, reusing policies in multiple policy sets cuts down o the total number of policies needed in the system.

To view policy sets, click **NetIQ Change Guardian**, and then select **Policy Set Manager** in the left pane.

Adding and Editing a Policy Set

The Policy Set Manager allows you to add any submitted policy from any Change Guardian module to a policy set.

Click **My Policy Sets** to view policy sets you created and to add new policy sets. Select a specific policy set to delete, clone, or edit its details. After you create a policy set, you can assign the set as you would assign a policy. For more information, see Section 6.5, “Assigning Policies and Policy Sets,” on page 57.

Cloning a Policy Set

Cloning a policy set allows you to quickly create a new policy set based on a selected existing policy set, and then make needed changes.

6.2.3 Using Policy Templates

Change Guardian policy templates provide examples of policies you can create. When using a Change Guardian module, select a policy template, and then copy it to the policies for that module. When a copy of the template appears in the list of policies for the module, you can edit the constraints to specify your monitored computers and files.

6.3 Understanding Resource Expansion

Change Guardian uses resource expansion to process each user group or computer group specified in a policy as a list of the group members. For example, if a policy specifies a user group to monitor, Change Guardian uses the resource expansion configuration to monitor for activity performed by the individual users in the group. If the policy returns an event, the name of the user performing the change appears in the event report.

NOTE: You must configure resource expansion for every grouped resource. If you do not configure resource expansion for a grouped resource, and you specify that grouped resource in a policy, the policies using that grouped resource either produces an event for an unmanaged user, or does not filter the event.

To access resource expansion, click **Settings > Resource Expansion**.

The Resource Expansion Configuration window lists the **scope**, or domain name, for each expanded resource. From this window, you can choose to expand a new resource or edit an existing expanded resource.

Creating or editing an expanded resource requires you to define the **resource type**, which includes the domain, type of resource, and the credentials to allow access to group information.

6.4 Understanding and Managing Asset Groups

You can place computers in **asset groups** to categorize them, or assign the same policies to many computers with one policy assignment. Asset Membership displays your asset groups and the monitored computers each asset group contains. You can centralize administration of your monitored computers by creating asset groups, and applying policies or policy sets to monitor multiple computers that require the same level of monitoring. Rather than assign policies separately to multiple computers, you can place those computers in an asset group, and then assign policies only once to the asset group.

Click **NetIQ Change Guardian**, and then select Asset Groups to perform the following functions:

- Add and remove asset groups
- Add and remove computers to and from asset groups
- Edit computers in asset groups
- View computers in your enterprise, and the asset groups to which a selected computer belongs
- View computer attributes, such as computer name and operating system
- View asset groups, and the computers each group contains

Select **Computers** to see a list of computers with Change Guardian agents installed. Select **Asset Groups** to see a list of asset groups created and the computers they contain.

6.4.1 Filtering Computers and Asset Groups

If Change Guardian lists a large number of computers and asset groups, you can use **Filter Values** to expand the pane, and then use any of the following conditions to narrow the view of computers or asset groups:

Contains

Enter a string of characters that appears anywhere within the names of computers or asset groups you wish to view into the **Set value** text box.

Does not contain

Enter a string of characters that does not appear within the names of computers or asset groups you wish to view into the **Set value** text box.

Starts with

Enter the first characters of the computer or asset group names you wish to view into the **Set value** text box.

Ends with

Enter the last characters of the computer or asset group names you wish to view into the **Set value** text box.

Equals

Enter the name of the computer or asset group to which you want to apply a policy or policy set into the **Set value** text box.

Does not equal

Exclude a computer or asset group from the list by entering the computer or asset group name into the **Set value** text box.

Matches

Enter a name, or a partial name and wildcard, of the computer or asset group to which you want to apply a policy or policy set into the **Set value** text box.

After you select a condition and enter a value for the filter, click **Apply** to display a list of computers or asset groups matching the filter you created. Filter values are cumulative, so you can further narrow the list of computers or asset groups by adding conditions and values to your filters.

6.4.2 Adding and Removing Asset Groups

Select **Asset Groups** from the menu to view all available asset groups and the computers within them. From this screen, you can add and remove asset groups and select an asset group to edit its membership.

To add an asset group:

1. Select **Asset Groups**.
2. Click **Add**.
3. Enter the name of the new asset group.
4. Select the computers you want to add to the group.

   TIP: If you have a long list of monitored computers, use **Filter Values** to display the computers matching a specified naming pattern. For more information about filtering, see Section 6.4.1, "Filtering Computers and Asset Groups," on page 55.
5. Click **OK**.

To remove an asset group:

1. Select **Asset Groups**.
2. Select the asset group you want to remove.
3. Click **Remove**.

6.4.3 Editing Computers in Your Asset Groups

To view a list of computers in an asset group, select an asset group, and then select the Membership tab. From the Membership tab, you can click **Edit Computers** to add computers to the asset group, or to remove computers from it.

6.4.4 Viewing Computers in Your Enterprise

The Asset Groups node can display information about the monitored computers in your enterprise. Select **Computer** to view monitored computers.

From the **Attributes** tab you can view information about a selected computer.

From the **Membership** tab, you can view the groups to which the selected computer belongs, add the computer to other groups, and remove the computer from asset groups.

TIP: If you have a long list of monitored computers, use the **Filter Values** feature to display only those computers matching a specified naming pattern.

6.5 Assigning Policies and Policy Sets

After you create a policy, you can store it in the Change Guardian Policy Repository, which makes the policy available to other Change Guardian users in your enterprise, and enables the policy for assignment to computers and asset groups.

The Policy Assignment screen allows you to assign policies and policy sets to the computers or asset groups in your enterprise, or the asset groups you created. Selecting a computer or asset group allows you to see the policies and policy sets assigned to it, and allows you assign additional policies and policy sets.

6.6 Creating Monitoring Schedules

You can create and configure monitoring schedules that are available as part of assigning policies or policy sets. By default, Change Guardian policies monitor computers and asset groups continuously. Scheduled monitoring allows you to specify that an assigned policy or policy set monitors computers and asset groups during specific time frames. For example, you can suspend monitoring during maintenance windows for computers or asset groups, which eliminates events generated as a result of the Change Guardian server losing contact with an agent.

Scheduled monitoring supports days of the week and inclusive intervals during a day.

Examples of valid time restrictions include the following:

- Mondays, Tuesdays, and Wednesdays from 3-5 PM
- Mondays from 3-5 PM and Tuesdays from 4-6 PM
- Mondays from Midnight-7 AM, 9 AM-2 PM, and 6 PM-Midnight

To create a monitoring schedule:

1. Log in to the Change Guardian Policy Editor.
2. Click **Settings > Schedule Monitoring Time**.
3. Click **Add**.
4. In the **Schedule Name** field, type a name for the schedule.
5. In the **Schedule Monitoring Time** window, select the time and day you want Change Guardian to stop monitoring, and then select **Don't Monitor**.

   TIP: You can drag your cursor to select a range of times and days for scheduled monitoring.
6. Click **OK**.

To edit an existing monitoring schedule:

1. Log in to the Change Guardian Policy Editor.
2. Click **Settings > Schedule Monitoring Time**.
3. Select an existing schedule name.
4. Click **Edit**.
5. Make the desired changes to the monitoring schedule.
6. Click **OK**.

6.7 Understanding Change Guardian Email Alerts

You can configure Change Guardian to send email notifications for events to specified administrators and operators by creating and configuring one or more **email integrators**. Configuring an email integrator creates a connection to an SMTP server, and allows you to create **notification groups** that can be accessed by the Change Guardian Web console to send an email alert to a specified group of email addresses.

Event Routing in the Change Guardian Web console uses the information supplied in the email integrators to assign email alerts to specified events. For more information, see Section 7.2.2, "Assigning Email Alerts to Events," on page 63.

6.7.1 Creating and Configuring Email Integrators

To enable email alerts, you must create an email integrator and store it on an event destination computer. If your Change Guardian environment includes more than one event destination computer, you must create an email integrator on each event destination from which you want to send email alerts.

To create and configure an email integrator:

1. **Select Settings > Email Configuration**.
2. Enter the Sentinel login information for the default event destination computer.
3. Under the Email Servers pane, click **Add**.
4. Type the name of the email server to which you want to connect.
5. Type a description for the email server.
6. Enter values for the following fields:
   - SMTP Host – The full name, including domain name, of the email server from which you want to send email alerts.
   - SMTP Port – The remote SMTP port to which the integrator connects.
   - Secure – Specifies if the connection to the SMTP computer must be a secure connection.
   - From – The return email address appearing on each email alert for this email integrator.
   - Authentication Required – Specifies if the email server requires SMPT authentication to send email.
   - User Name – The user name to use when connecting to the SMTP server.
   - Password – The password corresponding with the entered SMTP user name.

6.7.2 Creating and Configuring Notification Groups

As part of creating an email integrator, you must create one or more notification groups, which specify the recipients of the email alerts and contains change event information. When you assign email alerts to events in the Change Guardian Web console, you can choose from all notification groups available for that event destination. For more information, see Section 7.2.2, "Assigning Email Alerts to Events," on page 63.

NOTE: If you want only one person to receive an email alert, you must create a notification group containing only the desired email address.

To create and configure a notification group:

1. **Select Settings > Email Destination**.
2. Enter the Sentinel login information for the default event destination computer.
3. Under the Notification Groups pane, click **Add**.
4. Type the name of the notification group you want to create.
5. Type a description for the notification group.
6. Enter values for the following fields:
   - From – The return email address appearing on each email alert for this email integrator.
   - To – A list of email addresses, separated by commas, that receive email alerts.
   - CC – A list of email addresses, separated by commas, that receive copies of email alerts.
   - BCC – A list of email addresses, separated by commas, that receive blind copies of email alerts.
   - Subject – The subject appearing on the alert email.
   - Max Events per Email – Specifies the number of events displayed in the email alert. The email includes the events received up to the maximum number set in this field.
   - Include Change Details – Specifies whether the body of the email contains the details of the change detected by Change Guardian.
   - Email Format – Specifies the format of the email as either text or HTML.

6.8 Using Change Guardian Administrative Reports

Change Guardian allows you to create customized reports detailing the Change Guardian configuration for your enterprise. Administrative reports can contain information such as the computers in each asset group, a list of the current policy assignments by asset group, and licensing information. You can use this information for auditing or administration purposes.

You can save the generated report as either a Change Guardian report or as a PDF file. You can also use the Policy Editor to print reports, or send reports to others as an email attachment.

Change Guardian generates the following reports:

Assigned Policies by Asset

This report returns a list of assigned policies for each asset or asset group specified in the report conditions. If you choose to show details, the report includes a subsection with the definition of each assigned policy. This report includes the following report conditions:

- Show policies assigned to specified assets
- Show policies assigned to assets in specified asset groups
- Show policies assigned to specified asset groups
- Show or hide policy assignment details
- Show monitoring schedules assigned to policies assigned to specified assets

Assets Assigned to Policy

This report returns a list of assets assigned for the policies or policy sets specified in the report conditions. This report includes the following report conditions:

- Show assets assigned to specified policies
- Show assets assigned to policies in specified policy sets

Policies Not Assigned

This report returns the list of policies defined, but not assigned to an asset.

Managed Assets

This report returns a list of registered assets, sorted either by asset name or by asset registration.

Schedule Monitoring Time

This report returns a list of monitoring schedules and their monitoring times.

Event Trends

This report lists the occurrence of an event over time. This report includes the following report conditions:

- Show the occurrence of an event over time, grouped by policy
- Show the occurrence of an event over time, grouped by user
- Show the occurrence of an event over time, grouped by asset

7 Viewing Change Guardian Events

This chapter describes using the Change Guardian Web console to view events. Change Guardian displays events—results from assigned policies and policy sets—through event reports displayed in the Change Guardian Web console. To access the Web console, specify the following Web address, as determined by your Policy Repository computer installation:

`https://Change_Guardian_Server_IP_Address:8443`

When prompted, enter your Change Guardian user name and password.

7.1 Supported Web Browsers and Settings

You can view Change Guardian event reports from a Windows or Linux computer with one of the following Web browsers installed:

- Microsoft Internet Explorer 8
- Mozilla Firefox 5

7.1.1 Microsoft Internet Explorer 8 Settings

To view event reports in Internet Explorer 8, ensure the following:

- Set the security level to Medium-high. If you set the security level to High, the Web console displays a blank page. On the **Tools** menu, select **Internet Options > Security**, and then set the security level to Medium-high.
- Ensure you do not select the **Compatibility View** option on the **Tools** menu.
- Enable automatic prompting for file downloads to ensure a pop-up blocker does not prevent the file download. On the **Tools** menu, select **Internet Options > Security > Custom Level**, scroll down to **Downloads**, and then select **Enable** as the **Automatic prompting for file downloads** option.

7.1.2 Updating Mozilla Firefox 5 - SLES 11

SLES 11 SP 2 includes Mozilla Firefox 3.6. You must upgrade to Firefox 5, or you cannot view event reports. This section describes using YaST in SLES to upgrade Firefox.

To upgrade to Firefox 5:

1. Open YaST.
2. Select **Software > Software Repositories** to display the Configured Software Repositories window.
3. Click **Add** to open the Media Type window.
4. Select the **Specify URL** option, then click **Next**.

5 In the **URL** text box, enter `http://download.opensuse.org/repositories/mozilla/SLE_11`, then click **Next**.

6 Click **OK**.

7 Click **Software Management**.

8 Type `Firefox` in the **Search** text box.

9 Select the required packages for Firefox 5.

NOTE: If you select a package that conflicts with the existing version, a warning appears. Select the appropriate option, then click **OK Try Again**.

10 Click **Accept**.

7.2 Understanding Event Information

The Change Guardian Web console, by default, filters events with a severity of 3 to a severity of 5. Using the default filter, you can view the following information for each event:

- The specific alert severity
- The name of the file changed or accessed
- The computer on which that file resides
- Delta information (detected difference in the monitored file)
- Differential (diff) information (the actual changes made to the monitored file)

NOTE: Events reflecting changes to binary files include only delta information. The events do not include diff information.

7.2.1 Viewing Detailed Event Information

The Change Guardian Web console allows you to configure reports and see additional detail for each event. This section describes the configuration options for customizing the information you see for each event.

To see detailed event information, click the shield icon.

Reports

The Change Guardian Web console includes a report for policy events. When you run the report, you can choose to use default options or to customize any of the following options:

- The frequency you want to run the report
- A saved name for the report
- A date range for events
- A specific event type
- A specific policy
- View all events, managed events only or unmanaged events only
- View all change events, only successful change attempts, or only failed change attempts
- View events of a specified severity range
- Choose to send the report to a specified email address

People

You can use Change Guardian with Novell Identity Manager, which allows you to view the user identity details of events. You must have the View People Browser permission to view the identity details.

To view the user identity details of an event:

1. Perform a search, and refine the search results as needed.
2. In the search results, select the events for which you want to view the identity details.
3. Click ***Event operations > Show identity details***.
4. Select whether you want to view the identity of the Initiator user, the Target user, or both.

If you do not have Identity Manager or a similar product installed, this option is not available. For more information about integrating identity information with Change Guardian events, see Integrating Identity Information with Sentinel Events in the *NetIQ Sentinel User Guide*.

Tags

Tags are user-defined values you can use to logically group data collection objects such as event sources, event source servers, report templates, and report results. Tags help you to filter object lists for the data collection objects and also to augment incoming data. You can search for events, report templates, and report definitions that are tagged with a particular tag.

For more information about tags, see Configuring Tags in the *NetIQ Sentinel User Guide*.

Filters

Filters allow you to customize event searches and prevent data overload. The Filter Builder helps you build search queries ranging from simple to complex. You can save a search query as a filter and reuse it as required to quickly perform a search by selecting the filter rather than specifying the query manually every time.

For more information about filters, see Configuring Filters in the *NetIQ Sentinel User Guide*.

7.2.2 Assigning Email Alerts to Events

To send email messages from within the Change Guardian Web console, you must create an event routing rule, and you must have an email integrator configured for the Web console computer. If you do not have an email integrator configured, no notification groups appear as available actions for the event routing rule. For more information on configuring email integrators, see Section 6.7, “Understanding Change Guardian Email Alerts,” on page 58.

To assign email alerts to an event:

1. Start the Change Guardian Web console.
2. Click **Routing**.
3. Click **Create**.
4. Enter the following event routing information:
   - Name – The name for the event routing rule.
   - Filter – A filter to match the Change Guardian event, severity, or both for which you want to send email alerts.

- Tag – An optional field to help categorize events.
- Action – Available notification groups.

5. Click **OK**.

NOTE: You can assign more than one email alert to a specific event by assigning more than one action to the event routing rule

---

7.2.3 Forwarding Events for Long-Term Retention

Change Guardian retains event data for 30 days. If you want to retain event data longer than 30 days, you can configure syslog event forwarding to another server.

Syslog event forwarding requires you create an XML schema and XML file in the Change Guardian server installation folder. The default location of the folder is `/opt/NetIQ/CG/4.0`. The schema must have the following elements and attributes defined:

`<forwarding>`

The schema root element.

`<syslog>`

The element used to define syslog communication and destination. The syslog event forwarding file can contain multiple instances of the `<syslog>` element.

`hostname`

An attribute of the `<syslog>` element that specifies the destination syslog server name or IP address.

`port`

A required attribute of the `<syslog>` element that specifies the syslog server port to use for communication.

`type`

A non-required attribute of the `<syslog>` element that specifies the transport protocol as either TCP (default) or UDP.

`charset`

A non-required attribute of the `<syslog>` element that specifies character encoding. The default is UTF-8.

`<filter>`

Child element of `<syslog>` that specifies the Lucene filter events that must match to be forwarded to the defined syslog server. The default value for all events is `sev:[0 TO 5]`. This element is not required.

The following example configures event forwarding for all Change Guardian events over TCP to a specified IP address and port:

```
<forwarding>

    <syslog hostname="192.168.1.2" port="8888">

       <filter>pn: "NetIQ Change Guardian"</filter>

   </syslog>
```

```
</forwarding>
```

A Configuring Group Policy Auditing

Change Guardian requires you to configure the security event log, Active Directory auditing, and the security access control list (SACL) to enable the generation of Active Directory events related to Group Policy changes.

If you installed both Change Guardian for Group Policy and Change Guardian for Active Directory on the same computer you only need to configure the auditing requirements for Change Guardian for Active Directory.

The auditing requirements for Change Guardian for Active Directory require fewer changes than those for Change Guardian for Group Policy, but allow for monitoring all Active Directory. The auditing requirements for Change Guardian for Group Policy are more specific to reduce the monitoring scope to the minimum necessary.

A.1 Configuring the Security Event Log

You must configure the security event log to ensure Change Guardian for Group Policy does not discard Active Directory events before being processed.

To verify this configuration and ensure Active Directory events are not discarded before processing:

1. Open a command prompt as an administrator.
2. At the command line, type `eventvwr` and press **Enter** to start the Event Viewer.
3. In Windows logs, right-click **Security**, and then click **Properties**.
4. Verify the settings reflect a maximum log size of no less than 10240 KB (10 MB), and a selection of **Overwrite events as needed**.

To manually configure the security event log:

1. Log on to the agent computer.
2. Open a command prompt.
3. On the command line, type `GPMC.msc` to start the Group Policy Management Console.
4. In the forest, click **Domains**, and then select the domain to configure.
5. Click **Group Policy Objects**, and then right-click **Default Domain Controllers Policy**.
6. Click **Edit**.
7. In Computer configuration click **Policies**.
8. Click **Windows Settings**.
9. Click **Security Settings**.
10. Select **Event Log**.
11. Configure **Maximum security log size** to a size of no less than 10240 KB (10 MB).

12 Configure **Retention method for security log** to **Overwrite events as needed**.

13 Return to the command prompt, and then type `gpUpdate`.

NOTE: A Group Policy Organization (GPO) linked to the domain controller's (DC) organizational unit (OU) with a higher link order overrides this configuration when you start the computer, or run `gpUpdate`.

A.2 Configuring Active Directory Auditing

This configuration enables auditing of Active Directory events. The events are logged into the security event log.

The Default Domain Controllers Policy GPO should be configured with Audit Directory Service Access set to monitor both Success and Failure events.

To verify or set this configuration manually in Windows Server 2008 R2:

1 Open a command prompt as an administrator.

2 At the command line, type `gpmc.msc` and press **Enter** to start the Group Policy Management Console.

3 In the forest, click **Domains**, and then select the domain to configure.

4 In the domain to configure, click **Group Policy Objects**.

5 Right-click **Default Domain Controllers Policy**, and then click **Edit**.

6 Expand **Computer configuration > Policies > Windows Settings and Security Settings**.

7 In **Security Settings**, expand **Advanced Audit Policy Configuration**.

8 Click **DS Access**.

9 Click **Audit Directory Service Access**.

10 Verify the following selections:

- Configure the following audit events
- Success
- Failure

11 Click **OK** to return to the command prompt.

12 Type `gpUpdate` to apply changes.

Instead of configuring Audit Directory Service Access, you can configure the subcategories Audit Directory Service Changes, and Audit Directory Service Replication. However the Windows server detects events related to Audit Directory Service Access before it detects events for the other subcategories.

A GPO linked to the DC's OU with a higher link order overrides this configuration when you start the computer, or run `gpUpdate`.

To verify or set this configuration manually in Windows Server 2003 and Windows Server 2008:

1 Open a command prompt as an administrator.

2 At the command line, type `gpmc.msc` to start the Group Policy Management Console.

3 In the forest, click **Domains**, and then select the domain to configure.

4 In the domain to configure, click **Group Policy Objects**.

5 Right-click **Default Domain Controllers Policy**, and then click **Edit**.

6 Expand **Computer configuration > Policies > Windows Settings and Security Settings**.

7 In **Security Settings**, expand **Local Policies**, and then select **Audit Policy**.

8 Click **Audit Directory Service Access**.

9 Verify the following selections:

- Define these policy settings
- Success
- Failure

NOTE: A GPO linked to the DC's OU with a higher link order overrides this configuration when you start the computer, or run `gpUpdate`.

To log on to the agent computer as an administrator to verify or set this configuration manually in Windows Server 2008 and 2008 R2:

1 Open a command prompt as an administrator.

2 On the command line, `type auditpol /get /subcategory:{0cce923b-69ae-11d9-bed3-505054503030}`.

NOTE: Any GPO configuration will override the `auditpol` configuration when you start the computer, or when you run gpUpdate.

A.3 Configuring Active Directory Security Access Control List (SACLs)

The Security Access Control List (SACL) describes, in detail, the objects and operations to monitor. You must perform this configuration to generate events for operations that can result in, or are related to, changes in GPO data stored in Active Directory.

You must configure the following three Active Directory nodes:

- The domain node
- The GPO container
- The sites container

A.3.1 Configuring the Main Domain Node

You must first configure the following main domain node objects:

- On the object, configure Write gPOptions and Write gPLink.
- On any organizational unit inside the object, configure Write gPOptions, Write gPLink.
- On the object and child objects, configure Create organizational unit objects, Delete organizational unit objects.

You can use the `adsiedit.msc` tool to manually configure the domain main node for the following monitoring actions:

- Monitor changes in links between GPOs and the domain

- Monitor OU deletions
- Monitor descendant OU creations
- Monitor changes in links between GPOs and OUs
- Monitor OU creations inside descendent OUs

The procedures in this section utilize the adsiedit.msc tool to configure the main domain node.

NOTE: If you use Windows Server 2003, you must install the Windows Support Tools to use `adsiedit.msc`. To download Windows Support tools, see http://technet.microsoft.com/en-us/library/cc755948%28WS.10%29.aspx.

Configuring Auditing to Monitor Changes between GPOs and the Domain

This procedure creates auditing entries for gPLink and gPOptions.

To configure auditing to monitor changes between GPOs and the domain:

1. Open a command prompt as an administrator.
2. At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.
3. In the left panel, right-click **ADSI Edit > Connect to**.
4. In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well-known Naming Context**.
6. Select **Default naming context**.
7. In **Computer**, select **Default (Domain or server that you logged in to)**.
8. Click **OK**.
9. Click the new connection point **Default naming context**.
10. Select the node inside **Default naming context**. This node should be the domain node, and its name must start with `DC=`.
11. Right-click the domain node, and then click **Properties**.
12. Click the Security tab.
13. Click **Advanced**.
14. Click the Auditing tab.
15. Click **Add**.
16. Configure auditing to monitor every user.
    - *If you are using Windows Server 2012,*
        1. Click **Select a principal**.
        2. Click **OK**.
        3. Type `everyone`.
        4. Click **OK**.
    - *For all other versions of Windows,*
        1. Type `everyone`.
        2. Click **OK**.
17. Click the Properties tab.

18 In **Apply onto**, select **This object only**.

19 In the Access list, select the **Successful** and **Failed** check boxes for **Write gPLink** and **Write gPOptions**.

20 Click **OK**.

Configuring Auditing to Monitor OU Deletions

This procedure creates an auditing entry for monitoring OU creations and deletions.

To configure auditing to monitor OU creations and deletions:

1 Open a command prompt as an administrator.

2 At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.

3 In the left panel, right-click **ADSI Edit > Connect to**.

4 In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.

5 In **Connection Point**, select **Select a well-known Naming Context**.

6 Select **Default naming context**.

7 In **Computer**, select **Default (Domain or server that you logged in to)**.

8 Click **OK**.

9 Click the new connection point **Default naming context**.

10 Select the node inside **Default naming context**. This node should be the domain node, and its name must start with `DC=`.

11 Right-click the domain node, and then click **Properties**.

12 Click the Security tab.

13 Click **Advanced**.

14 Click the Auditing tab.

15 Click **Add**.

16 Configure auditing to monitor every user.

- *If you are using Windows Server 2012,*
  1. Click **Select a principal**.
  2. Click **OK**.
  3. Type `everyone`.
  4. Click **OK**.
- *For all other versions of Windows,*
  1. Type `everyone`.
  2. Click **OK**.

17 Click the Properties tab.

18 In **Apply onto**, select **This object only**.

19 In the Access list, select the **Successful** and **Failed** check boxes for **Delete**.

20 Deselect **Apply these auditing entries to objects and/or containers within this container only**.

21 Click **OK**.

Configuring Auditing to Monitor Descendant OU Creations

This procedure creates an auditing entry to monitor OU creation.

Configuring auditing to monitor descendant OU creations:

1. Open a command prompt as an administrator.
2. At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.
3. In the left panel, right-click **ADSI Edit > Connect to**.
4. In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well-known Naming Context**.
6. Select **Default naming context**.
7. In **Computer**, select **Default (Domain or server that you logged in to)**.
8. Click **OK**.
9. Click the new connection point **Default naming context**.
10. Select the node inside **Default naming context**. This node should be the domain node, and its name must start with `DC=`.
11. Right-click the domain node, and then click **Properties**.
12. Click the Security tab.
13. Click **Advanced**.
14. Click the Auditing tab.
15. Click **Add**.
16. Configure auditing to monitor every user.
    - *If you are using Windows Server 2012,*
        1. Click **Select a principal**.
        2. Click **OK**.
        3. Type `everyone`.
        4. Click **OK**.
    - *For all other versions of Windows,*
        1. Type `everyone`.
        2. Click **OK**.
17. Click the Properties tab.
18. In **Apply onto**, select **This object only**.
19. In the Access list, select the **Successful** and **Failed** check boxes for **Create Organizational Unit objects**.
20. Click **OK**.

Configuring Auditing to Monitor Changes in Links between GPOs and OUs

This procedure creates two auditing entries for gPLink and for gPOptions.

To configure auditing to monitor changes in links between GPOs and OUs:

1. Open a command prompt as an administrator.
2. At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.
3. In the left panel, right-click **ADSI Edit > Connect to**.
4. In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well-known Naming Context**.
6. Select **Default naming context**.
7. In **Computer**, select **Default (Domain or server that you logged in to)**.
8. Click **OK**.
9. Click the new connection point **Default naming context**.
10. Select the node inside **Default naming context**. This node should be the domain node, and its name must start with `DC=`.
11. Right-click the domain node, and then click **Properties**.
12. Click the Security tab.
13. Click **Advanced**.
14. Click the Auditing tab.
15. Click **Add**.
16. Configure auditing to monitor every user.
    - *If you are using Windows Server 2012,*
        1. Click **Select a principal**.
        2. Click **OK**.
        3. Type `everyone`.
        4. Click **OK**.
    - *For all other versions of Windows,*
        1. Type `everyone`.
        2. Click **OK**.
17. Click the Properties tab.
18. In **Apply onto**, select **Descendant Organizational Unit objects**.
19. In the Access list, select the **Successful** and **Failed** check boxes for **Write gPLink** and for **Write gPOptions**.
20. Deselect **Apply these auditing entries to objects and/or containers within this container only**.
21. Click **OK**.

Configuring Auditing to Monitor OU Creations within Descendant OUs

This procedure creates an auditing entry to monitor the creation of OUs within descendant OUs.

To configure auditing to monitor OUs creation within descendant OUs:

1. Open a command prompt as an administrator.

2. At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.
3. In the left panel, right-click **ADSI Edit > Connect to**.
4. In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well-known Naming Context**.
6. Select **Default naming context**.
7. In **Computer**, select **Default (Domain or server that you logged in to)**.
8. Click **OK**.
9. Click the new connection point **Default naming context**.
10. Select the node inside **Default naming context**. This node should be the domain node, and its name must start with `DC=`.
11. Right-click the domain node, and then click **Properties**.
12. Click the Security tab.
13. Click **Advanced**.
14. Click the Auditing tab.
15. Click **Add**.
16. Configure auditing to monitor every user.
    - *If you are using Windows Server 2012,*
        1. Click **Select a principal**.
        2. Click **OK**.
        3. Type `everyone`.
        4. Click **OK**.
    - *For all other versions of Windows,*
        1. Type `everyone`.
        2. Click **OK**.
17. Click the Object tab.
18. In **Apply onto**, select **Descendant Organizational Unit objects**.
19. In the Access list, select the **Successful** and **Failed** check boxes for **Create Organizational Unit objects**.
20. Deselect **Apply these auditing entries to objects and/or containers within this container only**.
21. Click **OK**.
22. Click **OK**.
23. Click **OK**.

A.3.2 Configuring the GPO Container

You must configure auditing of the following operations on the object and child objects in the GPO container:

- Write All Properties
- Delete
- Modify Permissions

- Modify Owner
- Create All Child Objects
- Delete All Child Objects

This procedure creates an auditing entry to monitor operations related to changes in GPO data.

To configure auditing to monitor changes in GPO data inside the GPO container:

1. Open a command prompt as an administrator.
2. At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.
3. In the left panel, right-click **ADSI Edit > Connect to**.
4. In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well-known Naming Context**.
6. Select **Default naming context**.
7. In **Computer**, select **Default (Domain or server that you logged in to)**.
8. Click **OK**.
9. Click the new connection point **Default naming context**.
10. Select the node inside **Default naming context**. This node should be the domain node, and its name must start with `DC=`.
11. Right-click the domain node, and then click **Properties**.
12. Click the Security tab.
13. Click **Advanced**.
14. Click the Auditing tab.
15. In the list of child nodes of the domain node, click **CN=System > CN=Policies**.

    NOTE: CN=Policies is the container of Group Policy objects.

16. Right-click **CN=Policies**, and then select **Properties**.
17. Click the Security tab.
18. Click **Advanced**.
19. Click the Auditing tab.
20. Click **Add**.
21. Configure auditing to monitor every user.
    - *If you are using Windows Server 2012,*
      1. Click **Select a principal**.
      2. Click **OK**.
      3. Type `everyone`.
      4. Click **OK**.
    - *For all other versions of Windows,*
      1. Type `everyone`.
      2. Click **OK**.
22. Make sure you are in the Object tab.
23. In **Apply onto**, select **This object and all descendant objects**.

24 In the Access list, select the **Successful** and **Failed** check boxes for **Write All Properties**, **Delete**, **Modify Permissions**, **Modify Owner**, **Create All Child Objects**, and **Delete All Child Objects**.

NOTE: When you check **Create All Child Objects** and **Delete All Child Objects** the other nodes related to child objects are selected automatically.

---

25 Deselect **Apply these auditing entries to objects and/or containers within this container only**.

26 Click **OK**.

27 Click **OK**.

28 Click **OK**.

A.3.3 Configuring Site Containers

You must configure auditing for the following site container objects to monitor links between GPOs and sites:

- On the object and child objects: Create site objects, Delete site objects
- On any Site inside the object: Write gPOptions, Write gPLink.

Configuring Auditing to Monitor Site Deletions

This procedure creates an auditing entry to monitor site deletions.

Configuring auditing to monitor Sites deletions:

1 Open a command prompt as an administrator.

2 At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.

3 In the left panel, right-click **ADSI Edit > Connect to**.

4 In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.

5 In **Connection Point**, select **Select a well-known Naming Context**.

6 Select **Configuration**.

7 In **Computer**, select **Default (Domain or server that you logged in to)**.

8 Click **OK**.

9 Click the new connection point **Configuration**. You may need to collapse other connection nodes to see **Configuration**.

10 Click **CN=Configuration > CN=Sites**.

11 Right-click **CN=Sites**, and then click **Properties**.

12 Click the Security tab.

13 Click **Advanced**.

14 Click the Auditing tab.

15 Click **Add**.

16 Configure auditing to monitor every user.

- ***If you are using Windows Server 2012,***
  1. Click **Select a principal**.
  2. Click **OK**.

3. Type `everyone`.
4. Click **OK**.

- ***For all other versions of Windows,***
  1. Type `everyone`.
  2. Click **OK**.

17 Click the Properties tab.

18 In **Apply onto**, select **Descendant Organizational Unit objects**.

19 In the Access list, select the **Successful** and **Failed** check boxes for **Delete**.

20 Deselect **Apply these auditing entries to objects and/or containers within this container only**.

21 Click **OK**.

Configuring Auditing to Monitor Site Creations

This procedure creates an auditing entry to monitor site creations.

To configure auditing to monitor site creations:

1 Open a command prompt as an administrator.

2 At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.

3 In the left panel, right-click **ADSI Edit > Connect to**.

4 In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.

5 In **Connection Point**, select **Select a well-known Naming Context**.

6 Select **Configuration**.

7 In **Computer**, select **Default (Domain or server that you logged in to)**.

8 Click **OK**.

9 Click the new connection point **Configuration**. You may need to collapse other connection nodes to see **Configuration**.

10 Click **CN=Configuration > CN=Sites**.

11 Right-click **CN=Sites**, and then click **Properties**.

12 Click the Security tab.

13 Click **Advanced**.

14 Click the Auditing tab.

15 Click **Add**.

16 Configure auditing to monitor every user.

- ***If you are using Windows Server 2012,***
  1. Click **Select a principal**.
  2. Click **OK**.
  3. Type `everyone`.
  4. Click **OK**.

- *For all other versions of Windows,*
    1. Type `everyone`.
    2. Click **OK**.

17 Click the Object tab.

18 In **Apply onto**, select **This object and all descendant objects**.

19 In the Access list, select the **Successful** and **Failed** check boxes for **Create Site objects**.

20 Select **Apply these auditing entries to objects and/or containers within this container only**.

21 Click **OK**.

Configuring Auditing to Monitor Changes in Links between Sites and GPOs:

This procedure creates auditing entries for gPLink and for gPOptions.

To configure auditing to monitor changes in links between sites and GPOs:

1 Open a command prompt as an administrator.

2 At the command line, type `adsiedit.msc` to start the tool for configuring Active Directory objects.

3 In the left panel, right-click **ADSI Edit > Connect to**.

4 In the connection window, ensure **Name** is **Default naming context** and **Path** points to the domain to configure.

5 In **Connection Point**, select **Select a well-known Naming Context**.

6 Select **Configuration**.

7 In **Computer**, select **Default (Domain or server that you logged in to)**.

8 Click **OK**.

9 Click the new connection point **Configuration**. You may need to collapse other connection nodes to see **Configuration**.

10 Click **CN=Configuration > CN=Sites**.

11 Right-click **CN=Sites**, and then click **Properties**.

12 Click the Security tab.

13 Click **Advanced**.

14 Click the Auditing tab.

15 Click **Add**.

16 Configure auditing to monitor every user.

- *If you are using Windows Server 2012,*
    1. Click **Select a principal**.
    2. Click **OK**.
    3. Type `everyone`.
    4. Click **OK**.
- *For all other versions of Windows,*
    1. Type `everyone`.
    2. Click **OK**.

17 Select the Properties tab.

18 In **Apply onto**, select **Descendant Site objects**.

19 In the Access list, select the **Successful** and **Failed** check boxes for **Write gPLink** and **Write gPOptions**.

20 Select **Apply these auditing entries to objects and/or containers within this container only**.

21 Click **OK**.

NOTE: When modifying the Default Domain Controllers Policy, you can avoid modifying the default GPO by creating another GPO and linking it to the domain controllers you want to monitor. That GPO should contain only the configurations required by Change Guardian, and its GPO link must be moved above others to make sure they do not override it.

B Configuring Active Directory Auditing

Change Guardian requires you to configure the security event log, Active Directory auditing, and the security access control list (SACL) to enable the generation of Active Directory events related to Active Directory changes.

B.1 Configuring the Security Event Log

You must configure the security event log to ensure Active Directory events are not discarded before Change Guardian for Group Policy processes them.

Set the maximum size of the Security Event Log to no less than 10 MB, and set the retention method to **Overwrite events as needed**.

To verify this configuration and ensure Active Directory events are not discarded before processing:

1. Open a command prompt as an administrator.
2. At the command line, type `eventvwr` to start the Event Viewer.
3. In Windows logs, right-click **Security**.
4. Verify the settings reflect a maximum log size of no less than 10240 KB (10 MB), and the selection to **Overwrite events as needed**.
5. Select **Overwrite events**.

To manually configure the security event log:

1. Log on to the agent computer.
2. Open a command prompt.
3. On the command line, type `GPMC.msc` and press **Enter** to start the Group Policy Management Console.
4. In the forest, click **Domains**, and then select the domain to configure.
5. Click **Group Policy Objects**, and then right-click **Default Domain Controllers Policy**.
6. Click **Edit**.
7. In Computer configuration click **Policies**.
8. Click **Windows Settings**.
9. Click **Security Settings**.
10. Configure **Maximum security log size** to a size of no less than 10240 KB (10 MB).
11. Configure **Retention method for security log** to **Overwrite events as needed**.
12. Return to the command prompt, and then type `gpUpdate` and press **Enter**.

NOTE: A Group Policy Organization (GPO) linked to the domain controller's (DC) organizational unit (OU) with a higher link order overrides this configuration, when you start the computer, or run `gpUpdate`.

B.2 Configuring Active Directory Auditing

This configuration enables auditing of Active Directory events, and logs the events into the security event log.

You should configure the Default Domain Controllers Policy GPO with Audit Directory Service Access set to monitor both success and failure events.

To verify or set this configuration manually in Windows Server 2008 R2:

1. Log on to the agent computer.
2. Click **Start > All Programs > Accessories**.
3. Right-click **Command Prompt**, and then select **Run as administrator**.
4. At the command line, type `gpmc.msc` and press **Enter** to start the Group Policy Management Console.
5. Expand Forest to select Domains.
6. In the forest, click **Domains**, and then click **Group Policy Objects**.
7. Right-click **Default Domain Controllers Policy**, and then click **Edit**.
8. Expand **Computer configuration > Policies > Windows Settings and Security Settings**.
9. In **Security Settings**, expand **Advanced Audit Policy Configuration**.
10. Click **DS Access**.
11. For each subcategory verify the following selections:
    - Configure the following audit events
    - Success
    - Failure
12. Define the same configuration for all subcategories of **Account management** and **Policy Change**.
13. Click **OK** to return to the command prompt.
14. Type `gpUpdate` and press **Enter** to apply changes.

To verify or set this configuration manually in Windows Server 2003 and Windows Server 2008:

1. Log on to the agent computer.
2. Click **Start > All Programs > Accessories**.
3. Right-click **Command Prompt**, and then select **Run as administrator**.
4. On the command line, type `GPMC.msc` and press **Enter** to start the Group Policy Management Console.
5. In the forest, click **Domains**, and then select the domain to configure.
6. Click **Group Policy Objects**, and then right-click **Default Domain Controllers Policy**.
7. Click **Edit**.
8. Expand **Computer configuration > Policies > Windows Settings and Security Settings**.

9. In **Security Settings**, expand **Local Policies**, and then select **Audit Policy**.
10. Click on **Audit directory service access**.
11. Verify the following selections:
    - Define these policy settings
    - Success
    - Failure
12. Click **OK** to return to the command prompt.
13. Type `gpUpdate` and press **Enter** to apply changes.

NOTE: For all versions of Windows, a Group Policy Organization (GPO) linked to the domain controller's (DC) organizational unit (OU) with a higher link order overrides this configuration, when you start the computer, or run `gpUpdate`.

NOTE: When modifying the Default Domain Controllers Policy, you can avoid modifying the default GPO by creating another GPO and linking it to the domain controllers you want to monitor. That GPO should contain only the configurations required by Change Guardian, and its GPO link must be moved above others to make sure they do not override it.

B.3 Configuring Active Directory Security Access Control Lists (SACLs)

The Security Access Control List (SACL) describes, in detail, the objects and operations to monitor. You must perform this configuration to generate events for operations that can result in, or are related to, changes in GPO data stored in Active Directory.

To monitor all changes of current and future objects inside Active Directory you must configure the domain node.

To verify or set this configuration manually using `adsiedit.msc`:

NOTE: To use `adsiedit.msc` in Windows Server 2003, you must install the Windows Support Tools. For more information about installing Windows Support Tools, see http://technet.microsoft.com/en-us/library/cc755948%28WS.10%29.aspx.

---

1. Log on to the agent computer.
2. Click **Start > All Programs > Accessories**.
3. Right-click **Command Prompt**, and then select **Run as administrator**.
4. On the command line, type `adsiedit.msc` and press **Enter** to start the Active Directory configuration tool.
5. Right-click **ADSI Edit**, and then select **Connect to**.
6. In the connection window ensure Name **Default naming context**, and **Path** points to the domain to configure.
7. In **Connection Point** select **Select a well-known Naming Context**.
8. Select **Default naming context**.
9. In **Computer**, select **Default (Domain or server that you logged in to)**.
10. Click **OK**.

11. Click the new connection point **Default naming context**.
12. Select the node within **Default naming context**. This should be the domain node, and the domain name must start with `DC=`.
13. Right-click the domain node, and then select **Properties**.
14. Select the Security tab.
15. Click **Advanced**.
16. Click **Auditing**.
17. Click **Add**.
18. Configure auditing to monitor every user.
    - ***If you are using Windows Server 2012,***
        1. Click **Select a principal**.
        2. Click **OK**.
        3. Type `everyone`.
        4. Click **OK**.
    - ***For all other versions of Windows,***
        1. Type `everyone`.
        2. Click **OK**.
19. Click **OK**.
20. Select the Properties tab.
21. In the **Apply onto** pane, select **This object and all descendant objects**.
22. In the Access list, select **Successful** and **Failed** for the following:
    - Write All Properties
    - Delete
    - Modify Permissions
    - Modify Owner
    - Create All Child Objects

      The other nodes related to child objects are selected automatically.
    - Delete All Child Objects

      The other nodes related to child objects are selected automatically.
23. Deselect the **Apply these auditing entries to objects and/or containers within this container only** check box.
24. Click **OK**.
25. Click **OK**.

C Configuring Operating System Auditing

Change Guardian requires you to enable the auditing system of your operating system. If you have already enabled auditing and Change Guardian is working as expected, then your operating system is properly configured. However, if you are not receiving events, use the information in this section to properly configure auditing for your operating system.

C.1 Configuring the AIX Audit Subsystem

The auditing subsystem on AIX computers stores files in the `/etc/security/audit` folder. You must have audit streaming enabled. However, streaming all events might consume too much space or processor time.

The following steps describe the minimum auditing activity Change Guardian requires.

1. Add the following line to the `/etc/security/audit/config` and `/etc/security/audit/streamcmds` files:

   ```
   /usr/sbin/auditstream | /usr/sbin/auditpr -t 0 -r -v -helRtcrpPTh >> /audit/stream.out&
   ```

2. Ensure the `/etc/security/audit/config` file includes the following stanzas:

   ```
   start
        binmode = off
        streammode = on
   bin:
        trail = /audit/trail
        bin1 = /audit/bin1
        bin2 = /audit/bin2
        binsize = 10240
     cmds = /etc/security/audit/bincmds
   stream:
     cmds = /etc/security/audit/bincmds
   ```

3. Add the following events to all Change Guardian users:
   - FS_Mount
   - FILE_Unlinkat
   - CRON_Finish
   - FILE_Linkat

- CRON_JobRemove
- PROC_Kill
- PROC_Execute
- FILE_Unlink
- FILE_Rename
- FILE_Fchown
- FILE_Owner
- FILE_Close
- USER_Chpass
- FILE_Symlinkat
- USER_Change
- FILE_Symlink
- PROC_LPExecute
- FILE_Open
- FILE_Mknodat
- FILE_Dupfd
- FILE_Chmod
- FILE_Renameat
- USER_Create
- GROUP_Create
- FS_Chdir
- FS_Umount
- FILE_Chown
- FILE_Fchownat
- GROUP_Change
- PROC_Create
- USER_Remove
- FILE_Fchmod
- PROC_Adjtime
- CRON_JobAdd
- FILE_Utimes
- PROC_Delete
- FILE_Openxat
- GROUP_Remove
- FILE_Fchmodat
- FILE_Mode
- PROC_Settimer
- FILE_Mknod
- CRON_Start
- FILE_Link

If you have unsuccessfully attempted to set up auditing on your AIX computer, ensure you remove all files in the `/etc/security/audit` folder except the `trail`, `stream.out` , and `bin` files.

C.2 Configuring the HP-UX Audit Subsystem

The auditing subsystem on HP computers stores files in the `/etc/rc.config.d` folder. You must process audit trail events. Ensure the `/etc/rc.config.d/auditing` file matches the following lines:

```
AUDITING=0

PRI_AUDFILE=/.secure/etc/audfile1

PRI_SWITCH=1000

SEC_AUDFILE=/.secure/etc/audfile2

SEC_SWITCH=1000

AUDEVENT_ARGS1=" -P -F   -e admin -s exit -s kill -s vfsmount -s rename -s unlink -
s close -s creat -s symlink -s fchown -s execv -s stime -s link -s settimeofday -s
mount -s clock_settime -s fchmod -s lchown -s umount2 -s chmod -s execve -s chown -
s open -s umount -s fork -s mknod -s vfork -s chdir -s adjtime "

AUDEVENT_ARGS2=” "

AUDEVENT_ARGS3=" "

AUDEVENT_ARGS4=" "

AUDOMON_ARGS=" -p 20 -t 1 -w 90"
```

C.3 Configuring the Solaris Auditing Subsystem

Versions 9 and 10 of the Solaris operating system have different auditing subsystems than Solaris version 11.

On computers running Solaris 9 or 10, perform the following steps:

1. Ensure the Basic Security Module will restart after reboot by running `./bsmconv` from the `/etc/security` folder.
2. Ensure the `/etc/security/audit_control` file contains the following lines:

   ```
   flags: ua,fm,cl,pc,fw,fr,ad,as,fc,ps,fd,nf

   naflags: fm,cl,pc,fw,fr,as,ad,fc,ps,fd,nf

   minfree:20

   dir:/var/audit
   ```

For Solaris 11, set the auditing flags by running the following commands:

```
auditconfig -setflags ps,as,cl,fd,fc,fm,fw

auditconfig -setnaflags ps,as,cl,fd,fc,fm,fw
```

C.4 Configuring a Linux Auditing Subsystem

Auditing subsystems on SUSE, Red Hat, and Red Hat variants are very similar. There are some differences in configuration based on operating system and on architecture. For Red Hat 4 and SUSE 10, configure the audit daemon in the `/etc/auditd.conf` and `/etc/auditd.rules` files. For Red Hat 5, Red Hat 6, and SUSE 11, configure the audit daemon in the `/etc/audit/auditd.conf` and `/etc/audit/auditd.rules` files.

Perform the following steps to configure auditing on a Linux computer:

1. (Conditional) For Red Hat and variants of Red Hat, ensure that the auditd service is enable by running the `chkconfig auditd on` command.
2. (Conditional) For SUSE, ensure that the auditd service is enable by running the `auditctl -e 1` command.
3. (Conditional) For computers that use a 32-bit architecture, add the following lines to the `audit.rules` file:

```
-a exit,always -F arch=b32 -S futimesat
-a exit,always -F arch=b32 -S unlinkat
-a exit,always -F arch=b32 -S fchownat
-a exit,always -F arch=b32 -S openat
-a exit,always -F arch=b32 -S exit
-a exit,always -F arch=b32 -S dup2
-a exit,always -F arch=b32 -S kill
-a exit,always -F arch=b32 -S rename
-a exit,always -F arch=b32 -S unlink
-a exit,always -F arch=b32 -S symlinkat
-a exit,always -F arch=b32 -S mount
-a exit,always -F arch=b32 -S fchmod
-a exit,always -F arch=b32 -S mknodat
-a exit,always -F arch=b32 -S execve
-a exit,always -F arch=b32 -S chown
-a exit,always -F arch=b32 -S open
-a exit,always -F arch=b32 -S exit_group
-a exit,always -F arch=b32 -S utime
-a exit,always -F arch=b32 -S adjtimex
-a exit,always -F arch=b32 -S chown32
-a exit,always -F arch=b32 -S renameat
-a exit,always -F arch=b32 -S close
-a exit,always -F arch=b32 -S creat
-a exit,always -F arch=b32 -S symlink
-a exit,always -F arch=b32 -S fchown
```

```
-a exit,always -F arch=b32 -S utimes
-a exit,always -F arch=b32 -S fchown32
-a exit,always -F arch=b32 -S link
-a exit,always -F arch=b32 -S settimeofday
-a exit,always -F arch=b32 -S fchmodat
-a exit,always -F arch=b32 -S lchown32
-a exit,always -F arch=b32 -S lchown
-a exit,always -F arch=b32 -S umount2
-a exit,always -F arch=b32 -S chmod
-a exit,always -F arch=b32 -S linkat
-a exit,always -F arch=b32 -S umount
-a exit,always -F arch=b32 -S fork
-a exit,always -F arch=b32 -S dup
-a exit,always -F arch=b32 -S mknod
-a exit,always -F arch=b32 -S vfork
```

4 (Conditional) For computers that use a 64-bit architecture, add the following lines to the `audit.rules` file:

```
-a exit,always -F arch=b64 -S futimesat
-a exit,always -F arch=b64 -S unlinkat
-a exit,always -F arch=b64 -S fchownat
-a exit,always -F arch=b64 -S openat
-a exit,always -F arch=b64 -S exit
-a exit,always -F arch=b64 -S dup2
-a exit,always -F arch=b64 -S kill
-a exit,always -F arch=b64 -S rename
-a exit,always -F arch=b64 -S unlink
-a exit,always -F arch=b64 -S symlinkat
-a exit,always -F arch=b64 -S mount
-a exit,always -F arch=b64 -S fchmod
-a exit,always -F arch=b64 -S mknodat
-a exit,always -F arch=b64 -S execve
-a exit,always -F arch=b64 -S chown
-a exit,always -F arch=b64 -S open
-a exit,always -F arch=b64 -S exit_group
-a exit,always -F arch=b64 -S utime
-a exit,always -F arch=b64 -S adjtimex
-a exit,always -F arch=b64 -S renameat
```

```
-a exit,always -F arch=b64 -S close
-a exit,always -F arch=b64 -S creat
-a exit,always -F arch=b64 -S symlink
-a exit,always -F arch=b64 -S fchown
-a exit,always -F arch=b64 -S utimes
-a exit,always -F arch=b64 -S link
-a exit,always -F arch=b64 -S settimeofday
-a exit,always -F arch=b64 -S fchmodat
-a exit,always -F arch=b64 -S lchown
-a exit,always -F arch=b64 -S umount2
-a exit,always -F arch=b64 -S chmod
-a exit,always -F arch=b64 -S linkat
-a exit,always -F arch=b64 -S fork
-a exit,always -F arch=b64 -S mknod
-a exit,always -F arch=b64 -S vfork
-a exit,always -F arch=b64 -S vfork
```