Oracle® Enterprise Manager

Configuration Change Console Installation Guide

10*g* Version 10.2.0.4 for Windows or UNIX

E12914-02

November 2008

ORACLE®

Oracle Enterprise Manager Configuration Change Console Installation Guide, 10*g* Version 10.2.0.4 for Windows or UNIX

E12914-02

Primary Author: Leo Cloutier

Contributing Author: Jerry Russell

Contributor: Daniel Hynes

Contents

9 Installing the Agent On UNIX Platforms

Preface

This guide describes the isntallation procedures of the Oracle Enterprise Manager Configuration Change Console.

Audience

This document describes the procedures and considerations for installing the Configuration Change Console. This book is primarily directed at Administrators who are responsible for the installation and maintenance of the product.

For more information on Configuration Change Console, administrators and users should read the *Oracle Enterprise Manager Configuration Change Console User's Guide*.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at `http://www.consumer.att.com/relay/tty/standard2.html`. After the

AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

Configuration Change Console Navigation

The Configuration Change Console user interface is composed of four primary parts. There is a region at the top which contains navigation tabs with drop down menus and other links for common actions. To navigate the drop down menu, the TAB key or equivalent will move across the tabs. Pressing the Return key will open the drop-down menu. Pressing the Enter key again will close it. When a tab drop-down menu is open, press the Tab key to navigate to the screen you want to open.

Below this region is an iframe which contains three functional areas. The first area is the header for the page which can have a header and a subheading. There are also icons for reloading the page, printing the current page, showing/hiding the filter bar, and showing the context sensitive help (new window) for the current page.

The next region is the filter bar. A filter bar will be hidden for any screen where there is no appropriate filter content. You can toggle showing/hiding this filter content by clicking on the filter bar icon in the header row. This region has an H1 level tag at the beginning to indicate the start of the filter bar and to provide a point to jump to in navigation.

The final region is the page content. All content will be shown in this area. This region has an H1 level tag at the beginning to indicate the start of the content area and to provide a point to jump to in navigation.

Synthesized Controls

The Configuration Change Console has a few areas where an action or link may cause a change somewhere else on the screen.

1. In some filter bars in screens, making a selection from a drop down will cause the entire page to reload to populate filter bars that are below the selected filter bar. If a change to a form element in a filter bar causes a page to reload, all other information that has already been selected above the most recently changed element will be preserved.

   An example of this can be found when you navigate to the following screen:

   Policy --> Operations Management --> Component

   Selecting the first filter bar option and changing it to *Predefined Components* will cause the entire page to automatically load and change the view from *Custom Components* to *Predefined Components*.

2. Screens in which rules are edited have a control with multiple form elements in one horizontal line. This row is rendered as a structural table. There is a link at the bottom right of this table labeled *Add Instance* that adds a new row to the end of the table to allow a new rule to be added. This is the only case where clicking on a link will affect some element above the area where the click happened.

   An example of this can be found on the following screen:

   Policy --> Operations Management --> Components

   After creating a component, click on the 0 link under Rule Sets. Then add a new rule set. Click on the **Edit Rules** link for the rule set. There will be a table with one row for a rule set available. Clicking on the **Add Instance** link to the bottom right of this table will add another row.

Disabling Screen Autoreloading

The product utilizes auto reloading of some screens, such as on the dashboard to reload the page every five minutes. If needed for accessibility purposes, this can be disabled product-wide by following these steps:

1. Stop the Configuration Change Console Server service
2. Connect to the database as the gateway user:

   ```
   sqlplus gateway/password@sid
   ```

   Where you replace password with the password for the gateway user, and sid with the sid of the database you created at product installation time. If you used a username other than gateway, also change this username here as well.
3. Execute the following SQL statements:

   ```
   update serverproperty set prop_value=0 where prop_name =
   'autoreload_enabled';
   ```

   ```
   commit;
   ```
4. Restart the Configuration Change Console Server

There is still one case where autoloading is not disabled and this is in a part of the jsp code that checks every five minutes to determine whether the session is still active. If the session is lost, then the user will be redirected to the login page with a note that their session expired. This cannot be changed, however the session timeout period can be extended. There is another section in this document related to this server property.

Installing the Server and Agents

Both the agent and server installer use a third party installation product that has the capability to install in a text-based console mode. Instead of launching the graphical installer, you can launch the installer from a DOS prompt or Unix console by typing one of the following two commands:

```
Server.exe -i console
```

```
Agent-win.exe -i console
```

You will then walk through the installation steps in the console.

You can also use a pre-filled response file and perform a silent installation where there is no interactive actions.

For more information about both of these options, see the server or agent installation sections of the *Configuration Change Console Installation Guide*.

Stylesheet

The product uses one stylesheet */gateway/stylesheet.css* for its screens other than the login screen. This style sheet can be found in the following directory and can be changed as needed.

CCC Install Directory}\deploy\activereasoning.ear\gateway.war\stylesheet.css

After making changes to the stylesheet, you should stop and start the Configuration Change Console Server service to ensure it is not cached in the web container.

The most commonly used style classes are:

- *Headerstl, SimpleHeaderstl, DashboardHeaderstl* - For table headers
- *Datastl* - Used for all content in tables and on screen

- *Buttonstl* - Used for form buttons
- *ErrorDatastl, WarningDatastl, SuccessDatastl* - Used for on screen messages

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Database Installation Pre-Installation Tasks

The installation of the Configuration Change Console and its components must be executed in the order documented below:

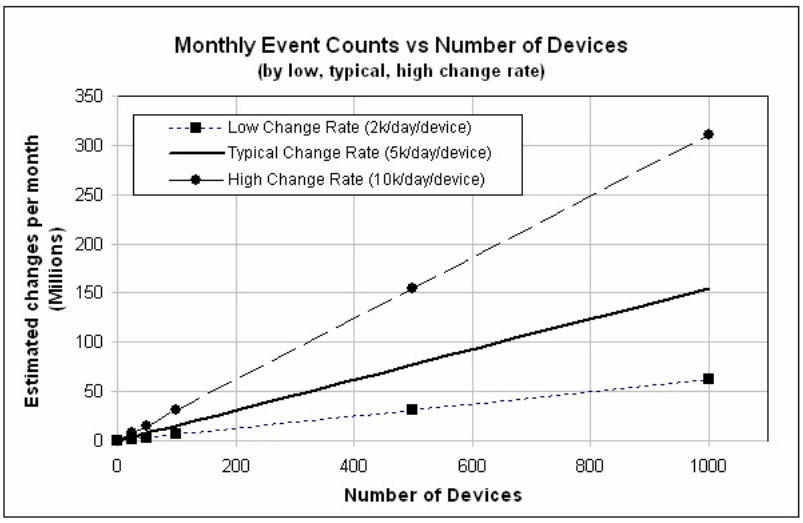
1. Oracle database installation and configuration
2. Configuration Change Console Server installation and configuration
3. Configuration Change Console Agent installation

Before installing the database, read through the following preparatory tasks.

1.1 Determining Database Size

This section provides a guideline for database sizing. It does not necessarily reflect every environment.

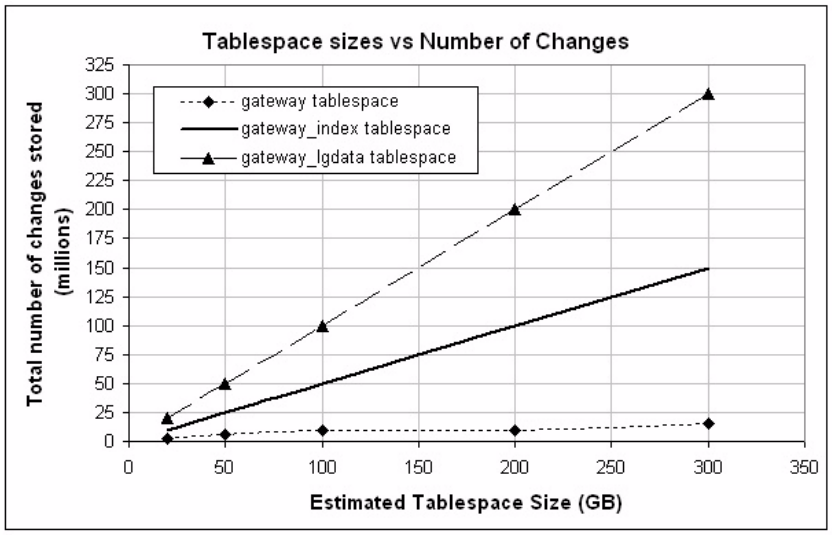
The size of the database correlates with the number of expected changes, rather than to the number of devices in the infrastructure. The first graph shows some change counts that might exist in some environments based on the expected change rates. A low change rate would mean that not very many changes happen on the rules sets that are configured. These can be used as a guideline when estimating how many changes you might expect to collect over a month.



The next graph shows the estimated tablespace size versus the number of changes in the environment. The number of changes shown in the graph reflects the number of changes the application can retain in its repository. If you have your data purging set

to three months, then you would find the number of changes you expect in a three month period. The previous graph showed some example total change counts for one month.

If you were storing events for three months, you would need to multiply the estimated change counts in the previous graph by three.



Note that if the tablespace is not sufficient in size, there may be data loss should the database become full. Once the database reaches its capacity you will receive an error message in your server log. You will be able to see this under the *Administration* > *Server Reports* > *Server and Database Logs* screen. Any new data will not be saved and users will not be able to log in to the product. To prevent data loss and user lockout, it is best to over-estimate the space needed for your database or leave a small buffer of disk space for auto-extension of the tablespace.

This graph does not include other tablespaces such as TEMP and UNDO. You must allocate an appropriate amount of disk space for these tablespaces based on your own best practices.

1.2 System Requirements

The specific operating system requirements for the database server are contingent on the required database size. All operating systems on which an Oracle database can operate are supported.

The following table lists some suggestions for various sizes of environments. These can change depending on many factors in a specific customer environment, but can be used as a rough guideline to follow.

Table 1–1 Recommended Size for Environments

Deployment Size Disk Space	Host	CPU/Host	Physical Memory	Minimums Recommended
25 Agents (typical rate change)	1	1 (3Ghz)	2 GB	65 GB
250 Agents (typical rate change)	1	2 (3Ghz)	4 GB	150 GB

Table 1–1 (Cont.) Recommended Size for Environments

Deployment Size Disk Space	Host	CPU/Host	Physical Memory	Minimums Recommended
1000 Agents (typical rate change)	1	4 (3Ghz)	4 GB	550 GB
10,000 Agents (typical rate change)	1	8 (3Ghz)	8 GB	2.3 TB

Deployment sizes are based on the sizing section in the documentation above. Total Recommended Disk Space includes the three Configuration Change Console tablespaces as well as Database software, Temp, and Undo tablespace size. Minimum recommended disk space is based on saving raw events for only 3 months and utilizing the majority of Configuration Change Console features.

2

Database Installation

Before creating the database for the Configuration Change Console, you first need to install the software for the Oracle database. The server will work with an Oracle 9*i* (version 9.2.0.6 or greater), or 10*g* (version 10.2.0.2 or greater) database on any operating system. The product requires *Oracle Database Enterprise Edition*. Standard Edition will not work because features such as partitioning, bitmap indexes and materialized views are used.

A basic installation requires three tablespaces totalling 8 gigabytes of space in addition to the space required for the Oracle database software.

Please refer to the Oracle installation guide for the database you are installing for more information about how to install the software.

2.1 Creating the Database

Once you have the Oracle database software installed, you need to create a database instance for the Configuration Change Console server to use for its repository. The instructions displayed here apply to an Oracle 10*g* database running on Windows. The process is the same for Unix-based databases as well.

1. On the machine featuring your Oracle database installation, click *Start -> Run*
2. From the Run box, enter `dbca` in the **Open** field. Click **OK**. This will launch the Database Configuration Assistant.
3. The welcome screen will display. Click **Next**.
4. Select the operation **Create a Database**, and click **Next**.
5. Select **General Purpose** and click **Next**.
6. Enter `gateway` in the **Global Database Name** field. The **SID** field will populate automatically. This is the suggested name for the database as it is used throughout the documentation. Click **Next**.
7. Configure the management options according to how you normally manage your databases. By default, Enterprise Manager and Database Control will be selected. Click **Next**.
8. Specify the password for the *sys* account. You will need to know this password later in the installation. Click **Next**.
9. Select the storage mechanism you would like to use for the database. This will depend on your environment. The default option is *File System*. Click **Next**.
10. Select the locations for database files. This will depend on your environment. The default is *Use Database File Locations from Template*. Click **Next**.

11. Specify your recovery options. This setting depends on your environment. If you are unsure, use the default settings. click **Next**.
12. No sample schemas or scripts are to be run during this database creation. Click **Next**.
13. On the Memory tab, set the amount of memory you want to use for this database. If you are on a database server dedicated to Configuration Chanage Console, increase the memory to fully utilize the server.
14. On the Character Sets tab, select **Use Unicode (AL32UTF8)**.
15. Under the Connection Model tab, select **Dedicated Server Mode**. Click **Next**.
16. Review the Database Storage settings and change according to your environment requirements. Click **Next**.
17. On the final screen, checkmark **Create Database** and click **Finish**.
18. On the summary screen, verify all parameters and correct any errors, the click **OK**.

2.2 Configuring the Database

Follow these steps to configure the database:

1. Start Oracle Enterprise Manager Database Control. From the Start menu, navigate to *Programs --> Oracle-OraDb10g home1* and then click on **Database Control - gateway**.
2. Log into Database Control as the *sys* user with the *sysdba* role.

2.2.1 Creating Tablespaces

In this section, you will create the following tablespaces. Even if you use a different name for the database SID, you must use the tablespace names specified in this document.

- GATEWAY
- GATEWAY_LGDATA
- GATEWAY_INDEX

When configuring the tablespace sizes, you must first determine the database size from the *Determining the Database Size* section. For this example we will assume the minimum size which is suitable for an evaluation set up with up to 20 agents.

- The GATEWAY tablespace should be a minimum of 2 GB for a production environment
- The GATEWAY_LGDATA tablespace should be a minimum of 2 GB but must be large enough to accommodate any expected data growth
- The GATEWAY_INDEX tablespace is typically twice as big as the GATEWAY_ LGDATA tablespace
- The GATEWAY_INDEX tablespace should be a minimum of 4 GB but must be large enough to accommodate any expected data growth

Follow these steps to create the tablespace manually. See below for instructions on finding a script to help with tablespace creation:

1. From the *Database Instance: Gateway* screen, click on the *Administraion* tab.

2. Navigate to *Database Administration --> Storage* and then click on the **Tablespaces** link.
3. Click **Create**.
4. Enter *gateway* in the **Name** field. You can leave all other tablespace settings the same or change them depending on your environment.
5. Click **Add** under the *Datafiles* section.
6. Enter the file system name for the datafile. For example, *gateway_01*
7. Set the file size for this datafile. If using the minimum requirements discussed above, enter *2 GB*.
8. Click **Continue**.
9. Add more datafiles if necessary, depending on Oracle database recommendations for maximum datafile size on your operating system.
10. Click **Create**.
11. A screen should appear indicating the creation of the tablespace. Click **OK**.
12. Repeat steps 1 through 11 for the *GATEWAY_LGDATA* and *GATEWAY_INDEX* tablespace. Substitute the tablespace name, datafile name, and size to match what is required for each tablespace.

2.2.1.1 Scripts for Generating Tablespaces

If you do not want to create the tablespaces manually, there is a script available with the product. Locate the *oracle-install.zip* file that comes with the Configuration Change Console media. Unzip this file and locate the file *oracle-install\scripts\dbstructure\tablespaces.sql*.

You can modify this script and run it to create the tablespaces. Note that this script will not work without customization for your environment.

2.2.2 Customizing the Temp and Undo Tablespaces

For an evaluation environment for the Configuration Change Console, the out-of-the-box TEMP and UNDO tablespace sizes should be sufficient.

For a typical medium-sized production environment (up to 2000 agents), you should allocate 12 GB for the TEMP tablespace and 12 GB for the UNDO tablespace.

2.2.3 Creating the Gateway User

The *users.sql* script is used to create the gateway user. Copy the *oracle-install* folder from the Configuration Change Console media to a folder installed on your system (parent directory where you placed the oracle-install folder is referred to as <BASE_PATH> in this document).

The *users.sql* script can be found in the following location:

<BASE_PATH>\oracle-install\scripts\dbstructure\users.sql

Note: The Oracle database and tablespaces must already exist as documented above before creating the user.

To create the gateway user, open a command prompt and enter the following command:

```
sqlplus /nolog
```

Log in as the *sys* user with dba privileges where <*password*> is the sys account password:

```
connect sys/<password>@gateway as sysdba
```

Run the *users.sql* script by typing the following where you replace <*BASEPATH*> with the directory to where you copied oracle-install:

```
@<BASE_PATH>\oracle-install\scripts\dbstructure\users.sql
```

You will be prompted to delete an existing user. If you are performing a fresh install, ignore the error message that the user could not be found. If you have a user already configured on the system that you would like to replace, then enter this user name here.

At the prompt, enter the user name for the user that the server will connect as to the database. The suggested user name is *gateway*. Enter a password for the user when prompted. The password will not be shown to the screen.

At the prompt, enter a **role name**. The suggested role name is `gateway_dba`. This step creates a specific role for database maintenance and other assignments. The user you are creating will automatically be assigned to this new role.

2.2.4 Configuring Oracle Initialization Parameters

The configuration of initialization parameters for the database instance should be created according to your typical production standard configurations.

For Oracle 10*g*, the default initialization parameters are known to work out of the box with the Configuration Change Console server.

If you are using an Oracle 9*i* database, there are a few initialization parameters that are required to be set before the product can work. The following are the settings that must be changed from default:

```
pga_aggregate_target=0
```

```
workarea_size_policy='MANUAL'
```

2.2.4.1 Configuring Number of Connections

When sizing your database, you should consider the number of concurrent connections and processes to allow. In a small environment, the default settings for the database will work. For a large environment, especially one with a clustered Configuration Change Console server, you must provide 300 processes per server (primary and secondary) adn 330 sessions per server (primary and secondary) that you will have in your cluster.

2.2.5 Loading the Configuration Change Console Schema

Load the schema and seed-data for the Configuration Change Console by following these steps:

1. Open a command window or shell
2. Change your directory to <*BASE_PATH*>*/oracle-install* where you copied this directory from the Configuration Change Console media.

3. At a prompt, run the following command:

   ```
   DBCreateEE.bat gateway password sid  > dbload.out
   ```

   On UNIX, use the following procedure where you replace *password* with your gateway user password and replace *sid* with the name of the database.:

   ```
   dbcreateee.sh gateway password sid  > dbload.out
   ```

4. Once the script is finished running, open the *dbload.out* file and review it to ensure there are no errors. This is a very important step as any errors caused at database schema load time will most likely cause failures in the server operation.

5. At this point, database installation is finished and you can now move on to the Configuration Change Console Server installation.

3

Server Installation Prerequisites

The installation of the Configuration Change Console and its components must be executed in the order documented below:

1. Oracle database installation and configuration
2. Configuration Change Console Server installation and configuration
3. Configuration Change Console Agent installation

When you have completed the installation, refer to Chapter 6, "Overview of Configuration Change Console Agent" or Chapter 12, "Securing the Configuration Change Console" for more information about installing your agent component.

3.1 System Requirements

The specific operating system requirements for the Configuration Change Console server are contingent on the size of your deployment.

The following table lists some suggestions for various sizes of environments. These can change depending on many factors in a specific customer environment, but can be used as a rough guideline to follow.

Table 3–1 Recommended Sizes for Environments

Deployment Size Recommended	Host	CPU/Host	Physical Memory	Minimum Disk Space Recommended
25 Agents (typical rate change)	1 (no clustering)	1 (3 Ghz)	2 GB	15 GB
250 Agents (typical rate change)	1 (no clustering)	2 (3 Ghz)	4 GB	20 GB
1000 Agents (typical rate change)	3 (clustered) 1 primary, 2 secondaries	4 (3 Ghz)	4 GB	50 GB
10,000 Agents (typical rate change)	6 (clustered) 1 primary, 5 secondaries	4 (3 Ghz)	4 GB	50 GB

Deployment sizes are based on the sizing section in the database prerequisites chapter of this install guide. For clustered environments, the primary server does not process incoming messages as it does in the non-clustered installation, but handles all other processing. This means that typically you would have at least 2 secondaries if you were using a clustered environment.

These sizing guidelines are assuming minimum hardware desired for the environment. There can be more secondaries than needed and the benefit is not only better load balancing but also failover if one secondary cannot process incoming events from agents.

In a production environment with 250 agents, although minimum requirement would be one server host, it is recommended that you use clustering with one primary and 2 secondaries so that you have a secondary available to process events in case one of them is down.

3.1.1 Internet Browsers

The following browser versions are compatible with the Configuration Change Console:

Browser	Version
Internet Explorer	7.0 and above
Firefox	1.2 and above

3.1.2 Operating System

The server on which the Configuration Change Console Server will be installed should be running *Windows 2000 Server*, *Windows 2003 Enterprise Edition, or Windows XP*.

3.1.3 Service Pack and Patch

The device on which the Configuration Change Console Server will be installed should always have the latest Service Pack and Patches.

3.1.4 Display Settings

The display colors should be set to 256 or more colors. The resolution should be 1280 x 768 or higher.

3.1.5 User Privileges When Installing the Configuration Change Console Server on Windows

The following information applies to all supported platforms in the Microsoft Windows family. This includes Windows 2000 and Windows 2003. The Configuration Change Console Server must be installed by a user with *Administrator* permissions. Additionally, all files that are created by this Administrator must have *NT Authority/SYSTEM change* permissions. The services that are created during installation will be run as the *SYSTEM* user as is normal with Windows services.

By default, all NT Administrators are granted *NT Authority/SYSTEM change* permissions. If they have been modified, you must assign *NT Authority/SYSTEM change* permissions to the entire installation directory.

4

Server Pre-Installation Tasks

The following chapter describes the tasks you must complete before installing the Configuration Change Console.

4.1 Network Card Configuration

The ideal Configuration Change Console server utilizes two Network Interface Cards (NIC); one NIC attaches to the external network to allow agents and web browsers to connect to the server. The second NIC attaches to a private network connecting directly to the database, as illustrated in the diagram below. When the Configuration Change Console server starts up, it provides services through the external NIC. The Configuration Change Console server must be configured to identify which NIC card is assigned to the external network.

This configuration allows the server to have a dedicated network interface for database traffic. Typically the interface will also extend across a faster networking medium than the external network. Typically the external network is 100 MBpS and the Private connection is 1 GBpS for database traffic. The Configuration Change Console server is a database intensive server.

Warning: It is very important that the Configuration Change Console server is connected through the external network NIC. If the server is connected through the private NIC, the agents will not connect to the Server.

4.1.1 NIC Configuration

If the device on which you installed the Configuration Change Console Server has multiple NIC cards, you must ensure that the primary NIC card for external connections is the one you will use for agent configuration. When you install an agent, you will provide an IP/hostname for the server. The NIC card with which this IP is associated must have higher priority than other NIC cards, otherwise the agent will receive a different IP than what is set at installation.

Note: If you configure a specific IP for the server when installing an agent, but then notice in the agent's logs that during start up it attempts to connect to a different IP, this is because the NIC card priority discussed in this section is not set properly.

Configure the Configuration Change Console server to connect to the external NIC by using the following procedure:

1. Go to *Start --> Settings --> Control Panel* and double-click **Network Connections**.
2. From the menu bar, click *Advanced* --> **Advanced Settings**.
3. Select the second **NIC**, for example, **Local Area Connection 2**, and click the **Up Arrow**. The NIC is now configured as the private NIC. Click **Ok**.

Note: It is recommended that you rename the Local Area Connections to a more descriptive name to ease troubleshooting efforts. For example, rename *NIC 1* as *External Connection* and *NIC 2* as *Private Connection*.

4.1.2 NIC Verification

To verify that the Configuration Change Console server connects to the external NIC, from the server ping the host name of the server, not the Configuration Change Console Server IP address. If the ping resolves the hostname to the private NIC, the agents will not be able to connect to the server.

4.2 Server and Database Clock Synchronization

Follow the recommendations below to synchronize the server and database clock.

4.2.1 Synchronize the Configuration Change Console Server Clock With the Network

Synchronizing the Configuration Change Console server clock to your network depends on what best suits your environment. For instance, if you have a dedicated server that serves network time, you may want to install that client on the Configuration Change Console server.

4.2.2 Synchronize the Oracle Server Clock With the Configuration Change Console Server Clock

An offset between the clock on the Configuration Change Console server and the clocks on the managed devices may affect notifications and file configuration updates as described below:

- If the clock on the managed device is ahead of the clock on the Configuration Change Console server, notifications and updates to file configurations will be delayed by the deviation time.
- If the clock on the Configuration Change Console server is ahead of the clock on the managed device, the result is contingent on the deviation time. The servers can tolerate a deviation of less than two minutes between the clocks. Note that a deviation greater than seven minutes may cause notifications and file configurations to be lost.

To synchronize the Oracle Database server clock with the Configuration Change Console server clock, follow these steps:

1. On the database server, from the Network and Dial-up Connections panel, right-mouse click on the *Local Area Connection* link. When the next screen appears, verify that the following components are selected:
   - Client for Microsoft Networks
   - File and Printer Sharing for Microsoft Networks

Click **Ok**.

2. On the database server, go to *Programs --> Accessories --> System Tools --> Scheduled Tasks* and double-click on **Add Scheduled Task**.
3. Click **Next** when the Scheduled Task Wizard screen appears.
4. Select the **Command Prompt** option.
5. Enter a descriptive title. Select the option **Daily** for this task to be performed daily. Click **Next**.
6. Select **12:00 AM** as the Start Time. Select the option **Every Day** and enter the **current date** as the Start Date. Click **Next**.
7. Enter an **account name** and **password**. This account must have administrative privileges on this server. Click **Next**.
8. Select the option **Open advanced properties for this task when I click Finish**. Click **Finish**.
9. When you click Finish in the previous step, the next screen will appear. From the *Task tab*, in the **Run** field verify that the path matches the following path where you replace *cccserver* with the **hostname** of the Configuration Change Console server.:

   C:\WINNT\system32\net.exe time \\cccserver /set /yes

   Click **Ok**.
10. From the *Schedule tab*, click the **Advanced** button.
    - Verify that the **End Date** option is not selected.
    - Verify that the **Repeat Task** option is selected and enter the value as it suits your environment; this is typically every 10 minutes.
    - Select the **Duration** option and enter `24` in the **Hour** field. Click **Ok**.
11. From the *Settings tab*, verify that the option **Stop the task if it runs** is selected, and enter `5` in the **Minutes** field. Verify that all options under **Power Management** are unchecked.

    Click **Ok**. A summary message will indicate the settings for the task.

4.3 SNMP Server Configuration

If you want to receive notifications on an SNMP Server when a configured event is triggered, you must configure your SNMP servers.

To receive SNMP notifications from the Configuration Change Console server, use two MIB files in conjunction with your SNMP/MIB software. These files, *AR-SMI.mib* and *AR-NOTIF.mib* can be found in the appendix of this document.

Compile both of these files using your SNMP/MIB manager software so that your SNMP server will be able to handle and interpret them correctly. Because each SMNP Management client is unique in the way it handles the implementation of these files, consult the documentation for your SNMP management software for the necessary process.

> **Note:** The AR MIB files have been tested using FineConnection to verify correct syntax and successful compilation. The source for both files is also available under the Appendix section of this document.

4.4 Mail Server Configuration

When setting up your mail server for use with the Configuration Change Console, you must specify an email account to be used for receiving and acknowledging notifications from the product via email. This account will automatically have its Inbox purged every few minutes, so be sure to not use an account that is used for any other purpose.

The server can connect to a POP3 or IMAP mail account to receive mail. It sends mail using SMTP.

5

Installing and Uninstalling the Configuration Change Console Server

This chapter describes the process for installing the Configuration Change Console Server.

5.1 Installing a Non-Clustered Configuration Change Console Server

Follow these steps to install the Configuration Change Console Server without clustering. This environment is suitable for very small deployments with a few agents and a low change rate.

1. Double-click on the **server.exe** file from the Configuration Change Console media. The Installer will take a few moments to initialize.
2. Click **Next** when the Introduction screen appears
3. Specify the *installation directory* or choose the *default*. Click **Next**.
4. Choose server type as Primary (without cluster support). Click **Next**.
5. Note that the Oracle database must be installed and running on this machine before the Configuration Change Console can be installed.

   Click **Next** if you have Oracle installed or **Cancel** if you still must install Oracle. If you click Cancel, you must reinstall the Configuration Change Console at a later time.
6. The Oracle database instance that is dedicated for Configuration Change Console must already be set up and running. The next screen configures the Configuration Change Console Server to access Oracle.

   Enter the following information:

   - **Database IP**. Enter the IP address of the server where the database was installed.
   - **Database Port**. The default value is 1521.
   - **Database SID**. The SID of the database as configured during the database installation. Set this value during database installation. The default and recommended SID is *gateway*.
   - **Username**. The Oracle database user. Set this value during database installation. The default and recommended username is *gateway*.
   - **Password**. Enter the user password. The password will be stored in an encrypted form during installation so that it cannot be read by anyone attempting to access the database directly.

Click **Next**.

7. Enter the following information:

> **Note:** If invalid data is entered, an error message will appear. The last statement on the error message indicates the reason for failure. If you receive any errors, review the error messages for details.

8. Enter your **organization name** and click **Next**.
9. Enter the password for the weblogic console administrator account. The user name for this account is *weblogic*. This is the account that you can use to log into the Weblogic Administration Console to manage your Weblogic deployment on which Configuration Change Console runs.
10. Enter the **password** for the built-in administrator account. This is the account you use to log into the Configuration Change Console user interface initially. You can change the password at a later time through the Administration features of the interface.
11. Enter the ports to use for the server. There are two ports configured here; HTTP is used for access to the web-based console, and HTTPS is used for secure access to the web-based console and also for agents to communicate with the server. Whatever port you use for HTTPS, you will need to know when you install the agents.
12. Click **Next**.
13. Specify whether you would like the server to start up automatically after it has finished installing. The installation will create a new Windows service called *Oracle Configuration Change Console Server*. If you do not start this service at install time, you can go to the Services Control Panel at any time to start it.
14. Specify the **minimum** and **maximum** amount of memory allocated to the Configuration Change Console server keeping the recommendations below in mind. Click **Next**.

> **Note:** If invalid data is entered, an error message will appear. The last statement on the error message indicates the reason for failure. If you receive any errors, review the error messages for details.

If the Configuration Change Console is the only major application running on your system, you can allocate up to 80% of all system memory to the Configuration Change Console. Remember that you must leave at least 128 MB for the Operating System to operate. If your memory allocation exceeds 1400 MB, be sure to configure your server to support more than 1 GB of memory for any process such as using the Windows 3G/4G tuning capabilities.

15. Review the *Pre-installation Summary* screen and click **Install**. If you would like to make changes to your configuration, click **Previous** to return to previously viewed screens.
16. The installation will take a few minutes to complete. A screen will indicate the installation progress. Click **Done** when the *Install Complete* screen appears.

5.2 Logging Into the Configuration Change Console Server

Once installation of the server has finished at the Oracle Configuration Change Console Server service has been started, you can log into the web-based user interface using a web browser. The URL can be one of the following:

http://hostname:port (where port is the HTTP port configured at installation)

https://hostname:port (where port is the HTTPS port configured at installation)

If you installed using the default HTTP port of 80 and default HTTPS port of 443, you do not need to use the port number in the URL.

The only username that exists out of the box is *administrator*, all lower case. The password will be the password you set for the administrator account when going through the server installer.

If you connect via HTTPS, you will get an alert about the certificate not being from a trusted certificate authority. The installation will install a certificate that has been created at installation time. This certificate is a self-signed certificate by the server. If you want to continue to use this self-signed certificate, then users will need to accept this certificate in their browser.

If you would like to load your own certificate for HTTPS communication, you can refer to the documentation for Oracle Weblogic Server 10.3 for instructions on how to set your own certificate from a trusted certificate authority (CA).

In a clustered environment, only the primary server provides access to the full web-based interface to use the product.

5.3 Logging Into the Oracle Weblogic Console

When you installed the Configuration Change Console Server, the Weblogic console was also configured. You can log into the web-based console interface using a web browser. The URL can be one of the following:

http://hostname:port/console (where port is the HTTP port configured at installation)

https://hostname:port/console (where port is the HTTPS port configured at installation)

> **Note:** Please consult your system or network administrator to determine which port should be used in your environment. The chosen port number must be used throughout the install process and must be matched when installing the agents. If you alter this value, please alter all entries in this install that reference the default ports (80 for HTTP and 443 for HTTPS.

If you installed using the default HTTP port of 80 and default HTTPS port of 443, you do not need to use the port number in the URL.

The user name will be *weblogic* and the password will be the one you set during installation for the Weblogic administration account.

If you have installed a clustered Configuration Change Console deployment, the default HTTP port for the admin server will be 8080 and 8090 for HTTP access.

5.4 Installing a Clustered Configuration Change Console Environment

This section outlines the steps required to install and configure the Configuration Change Console environment for clustering. In a clustered environment, there will be one primary server and any number of secondary servers. All of these servers will belong to the same domain, ConfigChangeConsole in Oracle Weblogic server.

If you install an environment as clustered, you must have a primary server and at least one secondary. If you do not have at least one secondary, events will not be captured from agents.

All the servers in the cluster (Primary server and Secondaries) should be in the same network segment or else the network connection of all servers in the cluster will be very slow.

All the hosts in the cluster must be able to parse the Fully Qualfied domain name of each other. You can test by pinging the fully qualified name of each server from the primary server and vice-versa.

All servers in the cluster should have the same install path for best performance. For example, the default is *C:\oracle\ConfigurationChangeConsoleServer*. Throughout this section, *$USER_INSTALL_DIR$* refers to the server installation directory.

5.4.1 Installing the Primary Server

Follow these steps to install the primary server for a clustered Configuration Change Console environment:

1. Double-click on the *server.exe* file from the Configuration Change Console media. The Installer will take a few moments to initialize.
2. Click **Next** when the Introduction screen appears
3. Specify the installation directory or choose the default. Click **Next**.
4. Choose server type as **Primary** (with clustering support), then click **Next**.
5. Note that the Oracle database must be installed and running on this machine before the Configuration Change Console can be installed. Click **Next** if you have Oracle installed or **Cancel** if you still must install Oracle. If you click Cancel, you must reinstall the Configuration Change Console at a later time.
6. The Oracle database instance that is dedicated for Configuration Change Console must already be set up and running. The next screen configures the Configuration Change Console Server to access Oracle.

   Enter the following information:

   - **Database IP**. Enter the IP address of the server where the database was installed
   - **Database Port**. The default value is 1521.
   - **Database SID**. The SID of the database as configured during the database installation. Set this value during database installation. The default and recommended SID is gateway.
   - **Username**. The Oracle database user. Set this value during database installation. The default and recommended username is gateway.
   - **Password**. Enter the user password. The password will be stored in an encrypted form during installation so that it cannot be read by anyone attempting to access the database directly. Click **Next**.

7. Enter your organization name. Click **Next**.
8. Enter a key phrase for the two certificate keystores that the server uses to store SSL certificates. You may need these pass phrases at a later time to import new certificates. Click **Next**.
9. Enter the **Password** for the weblogic console administrator account. The **Username** for this account is weblogic. This is the account that you can use to log into the Weblogic Administration Console to manage your Weblogic deployment on which Configuration Change Console runs.
10. Enter the **Password** for the built-in administrator account. This is the account you use to log into the Configuration Change Console user interface initially. You can change the password at a later time through the Administration features of the interface.
11. Enter the ports to use for the primary server. There are two ports configured here; HTTP and HTTPS. HTTP is used for access to the web-based console, and HTTPS is used for secure access to the web-based console and also for agents to communicate with the server. Whatever port you use for HTTPS, you will need to know when you install the agents. Click **Next**.
12. Enter the ports to use for the cluster admin server. There are two ports configured here; HTTP is used for access to the web-based console. You will need to provide the admin server IP and HTTPS port when you install any secondary servers in your cluster.
13. Specify whether you would like the server to start up automatically after it has finished installing. The installation will create a new Windows service called *Oracle Configuration Change Console Server*. If you do not start this service at install time, you can go to the Services Control Panel at any time to start it.
14. Specify the minimum and maximum amount of memory allocated to the Configuration Change Console server keeping the recommendations below in mind. Click **Next**.

    Note: If invalid data is entered, an error message will appear. The last statement on the error message indicates the reason for failure. If you receive any errors, review the error messages for details.

    If the Configuration Change Console is the only major application running on your system, you can allocate up to 80% of all system memory to the Configuration Change Console. Remember that you must leave at least 128 MB for the Operating System to operate. If your memory allocation exceeds 1400 MB, be sure to configure your server to support more than 1 GB of memory for any process such as using the Windows 3G/4G tuning capabilities.
15. Review the Pre-installation Summary screen and click **Install**. If you would like to make changes to your configuration, click **Previous** to return to previously viewed screens.
16. The installation will take a few minutes to complete. A screen will indicate the installation progress. Click **Done** when the Install Complete screen appears.

5.4.2 Installing the Secondary Server

Follow these steps to install a secondary server for a clustered Configuration Change Console environment. You may install one or many secondaries in the cluster to support size of deployment.

1. Double-click on the *server.exe* file from the Configuration Change Console media. The Installer will take a few moments to initialize.
2. Click **Next** when the Introduction screen appears.
3. Specify the installation directory or choose the default. Click **Next**.
4. Choose server type as **Secondary Server**, then click **Next**.
5. Specify the name of the secondary server. The name should be of the format *SecondaryServerX* where you replace X with the secondary number starting from 1. For instance, the first secondary server would be called `SecondaryServer1`.
6. Enter a key phrase for the two certificate keystores that the server uses to store SSL certificates. You may need these pass phrases at a later time to import new certificates. Click **Next**.
7. Enter the hostname and port for the admin server which was installed with the Primary server. The HTTPS port was set when installing the primary server. The default port value was 8090.
8. Enter the ports to use for the primary server. There are two ports configured here; HTTP and HTTPS. HTTP is used for access to the web-based console, and HTTPS is used for secure access to the web-based console and also for agents to communicate with the server. Whatever port you use for HTTPS, you will need to know when you install the agents. Click **Next**.
9. Specify the minimum and maximum amount of memory allocated to the Configuration Change Console server keeping the recommendations below in mind. Click **Next**.

   Note: If invalid data is entered, an error message will appear. The last statement on the error message indicates the reason for failure. If you receive any errors, review the error messages for details.

   If the Configuration Change Console is the only major application running on your system, you can allocate up to 80% of all system memory to the Configuration Change Console. Remember that you must leave at least 128 MB for the operating system to operate. If your memory allocation exceeds 1400 MB, be sure to configure your server to support more than 1 GB of memory for any process such as using the Windows 3G/4G tuning capabilities.
10. Review the Pre-installation Summary screen and click **Install**. If you would like to make changes to your configuration, click **Previous** to return to previously viewed screens.
11. The installation will take a few minutes to complete. A screen will indicate the installation progress. Click **Done** when the Install Complete screen appears.

5.4.3 Post Installation Steps for Cluster

After the installation of a secondary is finished, you need to perform the following steps manually in your cluster:

1. Login to the host which is hosting the Admin server and Primary Server.
2. Open the following file using notepad or any text editor:

   $USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\config\config.xml
3. Look for the following commented xml segment which defines an example SecondaryServer.

```
<!--server>
    <name>SecondaryServer1</name>
    <ssl>
      <enabled>true</enabled>
      <listen-port>7002</listen-port>
    </ssl>
    <machine xsi:nil="true"></machine>
    <listen-port>7001</listen-port>
    <listen-port-enabled>true</listen-port-enabled>
    <cluster>CCCC</cluster>
    <listen-address>your host address</listen-address>
    <java-compiler>javac</java-compiler>
    <jta-migratable-target>
      <user-preferred-server>SecondaryServer1</user-preferred-server>
      <cluster>CCCC</cluster>
    </jta-migratable-target>
    <client-cert-proxy-enabled>false</client-cert-proxy-enabled>
  </server-->
```

4. In the above block, replace the value in *<listen-address>your host address</listen-address>* with the Fully Qualified Domain Name of the secondary server.
5. Replace *<listen-port>7001</listen-port>* and *<listen-port>7002</listen-port>* with this secondary server's port and ssl-port respectively that you configured during the secondary server install.
6. In the block *<name>SecondaryServer1</name>* and *<user-preferred-server>SecondaryServer1</user-preferred-server>* replace it with the the name of the Secondary Server that you just installed. You specified the name during installation. For the first secondary server, you should use `SecondaryServer1`, then next would be `SecondaryServer2` and so on.
7. Uncomment this entire xml block to have the new secondary server defined. You can do this by either:
   - Changing the begin tag from *<!--Server>* to *<server>*
   - Changing the end tag from *</server-->* to *</server>*

   You can copy this block for any addtional secondary servers you may want to add, and modify the entries to reflect the settings of the new secondary server.
8. Look for the following block and uncomment it. Replace *SecondaryServer1* with the name of the secondary server you chose.

```
<!--migratable-target>
    <name>SecondaryServer1 (migratable)</name>
    <notes>This is a system generated default migratable target for a server.
Do not delete manually.</notes>
    <user-preferred-server>SecondaryServer1</user-preferred-server>
    <cluster>CCCC</cluster>
  </migratable-target-->
```

To uncomment, change *<!--migratable-target>* to *<migratable-target>* and *</migratable-target-->* to *</migratable-target>*. You need to add this block for any additional secondary servers you add.

5.4.3.1 Adding An Extra JMS Server For Your Cluster

If you want to add an extra jms server, please find the following two blocks in *config.xml* and uncomment them. Again replace the name under *target* which is *SecondaryServer1* to reflect the name of your secondary server.

```
<!--jms-server>
    <name>SlaveJMSServer</name>
    <target>SecondaryServer1</target>
    <persistent-store>SlaveFS</persistent-store>
  </jms-server-->

  <!--file-store>
    <name>SlaveFS</name>
<directory>C:\oracle\ConfigurationChangeConsoleServer\domains\ConfigChangeConsole\
masterJmsFileStore</directory>
    <target>SecondaryServer1</target>
  </file-store-->
```

To uncomment, make the following changes:

```
<!-- jms-server> to <jms-server>
     </jms-server--> to </jms-server>
     <!--file-store> to <file-store>
    </file-store--> to </file-store>
```

You will then have an extra jms server.

5.4.3.2 Configuring SSL

Because all Configuration Change Console Servers communicate over an SSL channel, SSL needs to be configured before starting the secondary server. This can be done through the Admin Server Console by accessing the following URL:

https://IP:PORT/console

The IP is the network IP or host name of the server on which you installed the primary and admin server. The port is the admin server HTTPS port. The default ssl admin server port is 8090, but may have been changed during installation of the primary server.

You need to provide the admin server username(weblogic) and password you set at install time to log in to this console.

1. In the Change Center of the Administration Console, click **Lock & Edit**
2. In the left pane of the Console, expand Environment and select **Servers**.
3. Click the name of the server for which you want to configure the identity and trust keystores. This is already configured for the primary server during install.
4. Select a secodary sever you wish to confgure.
5. Select *Configuration --> Keystores*.
6. In the Keystores field, select the option *Custom Identity and Custom Trust*. This will be the method for storing and managing private keys/digital certificate pairs and trusted CA certificates.

7. In the Identity section, define attributes of the identity keystore.

   Custom Identity Keystore:

   Provide the absolute path of the identity keystore.

   Specify the following value where $USER_INSTALL_DIR is the root path that you used for your secondary server installation:

   $USER_INSTALL_DIR$\bea\wls\server\lib\weblogicOCC.jks

8. Custom Identity Keystore Type: The type of the keystore. Specify JKS as the value. JKS stands for Java Key Store. If left blank, it defaults to JKS.
9. Custom Identity Keystore Passphrase: The password you will enter when reading or writing to the keystore. Input the password that you used when configuring the secondary server's weblogicOCC.jks file.
10. In the Trust section, define properties for the trust keystore.

    Custom Trust Keystore: Provide the absolute path of the trust keystore where *$USER_INSTALL_DIR$* is the path where you installed your secondary server.

    Enter *$USER_INSTALL_DIR$\bea\wls\server\lib\weblogicOCCTrust.jks*

11. Custom Trust Keystore Type: The type of the keystore. Specify JKS as the value.
12. Custom Trust Keystore Passphrase: The password used for reading or writing to the keystore. Input password that you used for secondary server's *weblogicOCCTrust.jks* file when installing the secondary server.
13. Click **Save**.
14. Select *Configuration --> SSL* page.
15. In the Identity and Trust locations section, choose the *Keystores* option.
16. In the Private Key Alias section, input **weblogic** as alias.
17. Input the password that you used for secondary server's *weblogicOCC.jks* file.
18. Click **Save**.
19. In the Change Center of the Administration Console, click **Activate Changes**.
20. After all of the above steps are performed using the admin server console, you should import this secondary's certificates into all other server's trust keystore files.
21. The certs of all other servers must be imported into the secondary's trust keystore file. This can be accomplished using the steps described in the next section.

5.4.3.3 Exporting And Importing the Certificates Into Servers

Follow these steps to export or import the certificates into servers:

1. Navigate to the *$USER_INSTALL_DIR$\bea\wls\server\lib* directory of each server.
2. Execute the following command:

   ```
   keytool -export -file primary.test.com.cer -alias weblogic
   -keystore weblogicOCC.jks
   ```

   primary.test.com.cer is the file name of cert on primary host

   primary.test.com is the domain name of current host.(primary)

3. In this current scenario, you would execute the above command on the primary server host. *primary.test.com* is the fully qualified domain name of the primary host.
4. When prompted to enter the password, please input the password that you had chosen during the server installation for *weblogicOCC.jks keystore* file.
5. Bring this cert file into the directory *$USER_INSTALL_DIR$\bea\wls\server\lib* of the secondary server. If you have more than one secondary server, copy this file to all the secondary servers.
6. In the secondary server execute the following command:

   ```
   keytool -import -alias primary.test.com -file
   primary.test.com.cer -keystore weblogicOCCTrust.jks
   ```

   primary.test.com will be used as the alias in secondary server's trust keystore(weblogicOCCTrust.jks)file to uniquely identify it.
7. When prompted to enter the password, please input the password that you had chosen during server installation for the *weblogicOCCTrust.jks* keystore file. At the prompt to chose either the Yes or No option, choose **Yes**. Go to all the secondary servers and import the same way.

   This completes importing of the new secondary server into all other server's trust key store files.
8. Now you must export the certificates from all the secondary servers including the new secondary server and import them into rest of the servers including the primary.

   For example go to the directory *$USER_INSTALL_DIR$\bea\wls\server\lib* of the secondary server and export the certificate using the following command where *secondary.test.com* is the fully qualified domain name of the secondary:

   ```
   keytool -export -file secondary.test.com.cer -alias weblogic
   -keystore weblogicOCC.jks
   ```
9. Import this file into primary server and rest of the servers using:

   ```
   keytool -import -alias secondary.test.com -file
   secondary.test.com.cer -keystore weblogicOCCTrust.jks
   ```
10. Repeat steps 8 and 9 above to export the certs from each of the servers and import them to other servers. You can remove all the *.cer* files created for the purpose of importing and exporting.

5.4.3.4 Copying the Required Files From Primary to the Secondary

Follow these steps to copy the required files from primary to secondary:

1. Delete all the files in *$USER_INSTALL_DIR$\deploy\activereasoning.ear\config\keystore* of the secondary.
2. Copy all the files in *$USER_INSTALL_DIR$\deploy\activereasoning.ear\config\keystore* of the pirmary server into the same directory location on the secondary server.
3. Delete all the files in *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\security* of the secondary server.
4. Copy all the files from *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\security* of primary into the same location on the secondary server.

5. Copy the following file from the primary server into the same path on the secondary server:

   $USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\fileRealm.properties

6. Delete all the files and sub-directories of *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\config* in the secondary server.

7. Copy from the primary, the whole of sub-directory structure config into: *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\config* of the secondary server. You can use the *dos xcopy* command to accomplish this.

8. Create the following new directory in the secondary. *{SecondaryServerX}* is the server name you have used during install such as *SecondaryServer1*.

   $USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\servers\{SecondaryServerX}\security

9. Copy the the file from primary server to the directory created in the previous step:

   $USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\servers\PrimaryServer\security\boot.properties

5.4.3.5 Adjusting the JDBC Connection Pool Sizes

Based on the number of secondary servers in the cluster, you need to increase the connection pool size and correspondingly increase the number of connections the database can handle. Also the database must be tuned to work with the increased number of connections.

As an example, if you have:

- A primary and secondary, jdbc connection pool requires a max connection setting of 200. This is the default value.
- A primary and two secondary servers, jdbc connection pool requires a max setting of 270.

For each additional secondary server, add 120 more connections.

The jdbc connection pool setting can be modified by going through the weblogic admin console. Follow these steps:

1. Click **Lock & Edit**
2. In the Domain Configurations, select *jdbc --> Data Sources*
3. Select **OracleDS**
4. In the Settings for *OracleDS*, click on **Connection Pool**. Set Maximum Capacity to the desired value based on the suggestions above for required number of connections. Click **Save**.

Also, as mentioned above, the database must be tuned to handle the new connection pool.

5.5 Uninstalling the Configuration Change Console

This section describes how to uninstall the Configuration Change Console Server.

Note: Prior to uninstalling the server, you must first uninstall all agents.

To manually uninstall the Configuration Change Console Server, follow these steps:

1. Go to **Start**, choose **Control Panel** , and then select **Add/Remove Programs**.
2. Select *Oracle Enterprise Manager Configuration Change Console Server* from the list to uninstall the agent.
3. Follow the prompts to uninstall all parts of the server.

6

Overview of Configuration Change Console Agent

This chapter provides an overview of the Configuration Change Console agent .

6.1 Overview

The Configuration Change Console captures a broad data set directly from the IT infrastructure to support troubleshooting, change management, and compliance.

All data collection is performed by the Configuration Change Console Agent. Agents are installed and run on each server in the IT infrastructure that will be monitored and managed by the Configuration Change Console. The agent works with the operating system and security capabilities of the server to collect required data. Once collected, data is sent to a dedicated Configuration Change Console server for analysis and processing.

The agent runs as a service on Windows servers, as a daemon process on all UNIX platforms.

6.2 Data Collection

The collected data includes the following:

- OS Change Events. Changes to files, process starts and stops, and user logins and logoffs
- Resource Utilization. System resource utilization by user, process, file and server
- Archived Files. Copies of files as they change
- Server Configuration. Current system resources and configuration
- Database Changes. Changes to structure or data in a database for Oracle and MS SQL databases
- Windows Registry. Changes to registry keys or values
- LDAP Server. Changes to objects in an LDAP-compliant server
- SNMP Traps. Collect configuration and alert data through SNMP trap mechanism

6.3 OS Change Events

OS Change events detect modifications made by people and applications to the IT environment. By recording these often small changes to files, processes, and users, the

Configuration Change Console is able to reconstruct sequences of activities that have been carried out. Detected change events include:

- File Change. Detects and records file create, delete, modify, and rename events. For each file change event collected data points include complete file name, date/time of change, event type, and user id of the user account who made the change. For most operating systems, additional configuration is required to capture user ID, as documented below.
- Process Change. Detects and records process start and stop events. For each process change event collected data points include process name, process ID, process user, event type, and date/time of event.
- User Change. Detects and records user logon / logoff events. For each user change event collected data points include user ID (account ID), event type, connection type, source host, and data/time of event.

6.4 Resource Utilization

The following sections provides a list of resource utilizations:

- Process Resource Utilization. Records the CPU and memory utilized by a process. Utilization data is collected every three seconds and then reported every five minutes. Data points include:
  - Process. Name, ID, parent process ID, creation date/time, end date/time, and process user.
  - CPU. Average, minimum, and maximum. CPU utilization during the five minute reporting interval; standard deviation of the average. CPU is recorded as or usage units and presented as percentages.
  - Memory. Average, minimum, and maximum memory utilization during the five minute reporting interval; standard deviation of the average.
- User Resource Utilization. Records the CPU utilization of all processes having the selected user as the process user. Data points include user id, date/time of reporting interval, average CPU utilization during the reporting interval, total number of processes run during the reporting interval.
- File Resource Utilization. Records the size of a file as it changes over time. Data points include file name, average size of file, maximum size of file, minimum size of file, and number of changes detected during the reporting interval (5 minutes) when the change was recorded. Data is collected every time a file change is detected.
- Total CPU Utilization. Overall CPU utilization for a selected server. Calculated as the sum of the CPU used by each process running on that server during the reporting interval.
- Total Memory. Overall memory utilization for a selected server. Data points include memory used and the swap/virtual memory used. Collected and reported every five minutes.
- File System Utilization. Overall utilization of each file system. Data points include total available storage and the amount of storage currently being used. Collected and reported every five minutes.

6.5 Archiving

Archiving captures and stores copies of a specified object as the contents of the object change. Up to five versions of each object are saved. Versions can be compared to identify the specific changes made to the contents. You can specify how many instances of each file to save through the server user interface.

6.6 Server Configuration

Server configuration is collected and updated every 15 minutes. Past configurations are not saved. Server Configuration data points include:

- File Archiving: Saves a copy of a specified file each time the contents of the file are changed. Archiving may be enabled for up to 50 files per managed device.
- Device Name. Detected from sever configuration.
- Device OS. Detected from server configuration.
- User Specified Identifiers. Asset tag, description and owning team are optional fields specified by the user at time of configuration. They are not automatically updated by server configuration.
- CPU. Processor count. Model and clock speed of each processor.
- Network configuration. Number of configured interfaces. IP address, MAC address, and manufacturer of each interface.
- Storage. Capacity and current utilization.
- Memory. Total available, used, free, swap free, and virtual.
- Detected Users. List of all user accounts on the server and the date and time each account last logged in.

6.7 Additional Data Collection Requirements

All data collection requires installation of the appropriate Configuration Change Console agent on the monitored server. Most data sets are collected using only the Configuration Change Console agent and standard server and operating system interfaces.

Some data sets require additional settings or software for some operating systems. Additional data collection requirements are as follows:

- Windows Logon/Logoff Events. Requires security auditing for logon/logoff events to be enabled.
- Windows File Change User ID. Requires files system auditing to be enabled for the files systems/directories where it is necessary to report the user id associated with a file change. If auditing is not enabled file changes are detected but the user ID associated with the change is not available.
- AIX File Change User ID. The user ID associated with a file change is not available on AIX systems due to limitations within the AIX operating system.
- Linux File Change User ID. Requires installation of a kernel module provide by Oracle. Kernel module loads dynamically and does not require a recompilation of the OS. Without the kernel module, file changes are detected by polling and the user ID associated with the change is not available.

All data sets not listed here are collected by the standard Configuration Change Console agent.

7

Agent Installation General Prerequisites

The installation of the Configuration Change Console and its components must be executed in the order listed below:

1. Oracle database installation and configuration
2. Configuration Change Console Server installation and configuration
3. Configuration Change Console Agent installation

Refer to the *Configuration Change Console Database Installation* chapters and *Configuration Change Console Server Installation* chapters for information on how to install the database and server.

7.1 System Requirements for All Platforms

The following section provides information on system requirements for all platforms.

7.1.1 Hardware Requirements

The following table depicts the minimum hardware requirements for each supported platform:

Table 7–1

Operating System	Hard Drive	Memory
Windows (XP, 2000, 2003 and NT4.0)	150 MB	512 MB
Linux (Oracle Enterprise Linux 4, 5, Red Hat V3, V4, 7.3)	150 MB	512 MB
HPUX 11.11 (11i), 11.23	250 MB	512 MB
AIX 5.3	250 MB	512 MB
Solaris 8, 9, 10	250 MB	512 MB

The values in the table are minimum requirements; settings may depend on your environment.

7.2 Preparing for Installation

The following items are prerequisites for all platforms:

- Service Pack and Patch. Please review the prerequisites for each supported platform to ensure that the most recent service pack or patch is installed. Additionally, each supported platform may have prerequisites specific to that

system. These platform specific prerequisites are documented in their respective sections.

- Configuration Change Console Server IP and HTTPS port. Obtain the IP and the HTTPS (443 by default) port that was set during server installation. This information is used to specify how the agents will communicate with the server.
- Administrator account on Server: When installing the agent, you must authenticate with the server. To do this, the installer will prompt you for an administrator role user name and password on the server. If you do not have an account, you must get one from the Configuration Change Console administrator first.

8

Installing the Agent On Windows Platforms

This section documents installation instructions for all supported Windows platforms.

The agent must be installed or uninstalled by a user with Administrator permissions. Additionally, all files that are created by this Administrator must have NT Authority/SYSTEM change permissions. The agent will run as a service under the *SYSTEM* user account. This applies to all platforms in the Windows NT family. This includes Windows NT4.0, Windows 2000, and Windows 2003.

Note that by default, all NT Administrators are granted NT Authority/SYSTEM change permissions. If they have been modified, you must assign NT Authority/SYSTEM change permissions to the entire installation directory.

8.1 Installation Information

The following sections discusss information about the Windows installation.

Note: This installation section is only applicable if you are installing an agent on Windows NT 4.0, or if WMI has been removed from the Windows installation.

8.1.1 How to Add NT Authority Change Permissions

After the agent installation is complete, you can add Change Permissions in one of the following two ways:

- From the command prompt, execute the following command to set the permissions on the Configuration Change Console Agent Installation directory:

  ```
  cacls c:\oracle\ConfigurationChangeConsoleAgent /T /E /G
  SYSTEM:C
  ```

- From Windows Explorer, do the following:

  1. Right-click on the *Agent Installation directory*.
  2. From the *Security tab*, confirm that **SYSTEM** is included in the list. If it is not included, you must add it.

8.1.2 Windows Management Instrumentation

Windows Management Instrumentation (WMI) enhances your ability to monitor and control system information and allows you to manage remote servers from a central location. For more information on WMI, refer to the *WMI White Paper* from the Microsoft Website.

Agents installed on Windows NT 4.0 platforms require WMI version 1.5 to be installed on the system in order for the agent to collect the full range of data available. Windows 2000 typically comes prepackaged with WMI version 1.5. If WMI is already installed on the system you must verify that it is version 1.5. It is recommended that you upgrade an existing WMI installation by following the steps in the WMI Versions and Upgrades section of this document.

The NT 4.0 agent installer detects whether WMI is installed, and if you select to install WMI, the agent installer will proceed to install WMI version 1.5 on your system. As part of the WMI installation, you must reboot the system after the agent installation completes.

If you choose not to install or upgrade WMI to version 1.5, the installer provides you the option of using the agent without the features provided by WMI 1.5. The alternative to using WMI is the NT 4.0 Lite version which must be used when WMI does not exist on the system or version 1.5 is not available.

Note: There is a risk of data loss if WMI becomes unavailable or is disconnected.

8.1.2.1 Data Collection with WMI

The Configuration Change Console Agent works with WMI to collect the full set of data:

- File creation, modification, renaming and deletions
- File archiving
- Process starts and stops
- User logins and logoffs
- System resource utilization by user, process, file and server
- Current system resources and configurations

8.1.2.2 Data Collection with NT 4.0 Lite

The NT 4.0 Lite version, installed without WMI, will limit the data set collected by the agent; only the following set of data will be displayed:

- System configurations
- Creating, modifying, renaming and deleting files
- File archiving
- Device names associated with the file changes

Note that the following data will not be collected:

- Process starts and stops
- User logins and logoffs
- Performance data such as Memory usage, CPU usage, and Disk usage
- Does not provide Access Control

8.1.2.3 WMI Versions and Upgrades

The agent will not detect what version of WMI is installed on your system. If you have an older version of WMI, you must upgrade it before installing the agent.

Note: Upgrading the WMI application may affect other applications on your system that are dependent or interface with the WMI application. Therefore, you should review the ramifications an upgrade to the WMI application may have on your IT infrastructure before proceeding.

To check which version of WMI is installed on your system, follow these steps:

1. In Windows Explorer, go to *C:\WINNT\system32\wbem*
2. Right-click on the *WinMgmt.exe* file and select **Properties**
3. From the *Version tab*, verify that the WMI file version indicates 1.5. If you have an older version of WMI, proceed to the next section for instructions on upgrading to WMI 1.5.

8.1.2.4 How to upgrade to WMI 1.5

Download and execute the *wmint4.exe* file from the Microsoft Download Center.

Refer to the Microsoft Download Center website for system requirements and detailed instructions for upgrading the WMI application on your system.

8.2 Windows 2000 and 2003 Agent Installation

The following sections describe the installation procedure for Windows 2000 Agent.

8.2.1 System Requirements

Before installing the agent, verify that you have at least the following installed on the device where the agent will be installed:

- Latest Service Pack
- For Windows 2000 only, Patch Q828020

You can obtain the patch from Microsoft's website. The Service Pack and the Patch are required to successfully monitor and log login/logout events for users.

8.2.2 Installing the Agent

To install the Agent on a Windows-based platform, follow these steps:

1. From the Configuration Change Console Installation CD, run the **agent-win.exe** file. The installation screen appears. The first screen of the installer explains how to navigate through the installer screens.

   Click **Next**.

2. Specify the directory where you would like to install the agent. The default directory, *C:\oracle\ConfigurationChangeConsoleAgent* is entered as the default path.

   Click **Next** to install to the specified location.

3. A check happens to ensure the minimum version of WMI is installed. This may only be an issue if you are installing the agent on a Windows NT 4.0 server.

> **Note:** Upgrading the WMI application may affect other applications on your system that are dependent or interface with the WMI application. Therefore, you should review the ramifications an upgrade to the WMI application may have on your IT infrastructure before proceeding.

4. The *Configure Agent screen* is displayed. Complete these steps:
   - Enter the **Agent ID**. If this field is left blank, an agent ID will be automatically assigned. During a normal installation, you should leave the Agent ID field blank.
   - Enter the Configuration Change Console server URL. The URL has the format *t3s://hostname:port* where hostname is the host the primary server is located at if using a non-clustered environment. If you are using a clustered environment, use *t3s://hostname1:port1,hostname2:port2,hostname3:port3*, etc where you put host name and port for each server (primary and secondary). Click **Next**.
   - Select **True** or **False** depending on whether to automatically start the service after the install. If you select False, you must manually start the agent from the Windows Services control panel. The service name will be *Oracle Configuration Change Console Agent*.
   - Click **Next**
5. You will be asked for an administrator username (the default is administrator) for the Configuration Change Console Server. This is used to verify that the person installing the agent is authorized to do so.
6. The *Summary screen* will display. Verify that the install folder is correct, and click **Install** to proceed with the installation.

Click **Done** when the Installation Complete screen appears to exit the installer.

8.2.3 Starting and Stopping the Agent

The agent should start automatically if you selected that option during installation. If you selected *False* in Step 3, or in the event that the agent does not start automatically, follow these steps:

1. Go to *Start --> Control Panel --> Administrative Tools --> Services*
2. Right-click on the **Oracle Configuration Change Console Agent service** and click **Start**

To stop the agent, right-click on the **Oracle Configuration Change Console Agent service** and click **Stop**.

8.2.4 Enabling Complete Real-Time Monitoring for the Windows Agent

The real time Windows agent modules rely on various capabilities of the operating system to collect all of the information on events. One part of this is to capture the user that made changes from the Windows Event Log. If you do not configure Windows to capture users that make changes, the agent will not capture this information, however it will still capture that a change happened and when it happened.

To configure the event log to work with real time monitoring, perform the following steps:

1. From the Explorer, select the directory that is being monitored, right-click and select **Properties**
2. Go to the *Security tab*
3. Click the **Advanced** button
4. Select the *Auditing tab*
5. Click the **Add** button. (In Microsoft XP, double click the **Auditing Entries** window)
6. Select the Name **Everyone** and click **OK**
7. Select the following options (Successful and/or Failed) from the Access window:
   - Create Files/Write Data
   - Create Folders/Append Data
   - Delete Files Subfolders and Files
   - Delete
8. Click **OK** to exit out of the screen
9. Repeat steps 1 through 7 for all other monitored directories
10. Go *Start --> Settings --> Control Panel --> Administrative Tools --> Local Security Policy --> Local Policies --> Audit Policy*. Double-click, and turn on the following policies (Success and/or Failure):
    - Audit account logon events
    - Audit logon events
    - Audit object access
11. Close the *Local Security Settings screen*
12. Go to *Start --> Settings --> Control Panel -->Administrative Tools --> Event Viewer*
13. Select **System Log**, and click on **Action** from the menu bar and select **Properties**
14. From the *System Log Properties panel*, on the *General tab*, set the **Maximum log size** to at least 5120 KB (5 megabytes) and select **Overwrite Events as Needed**. Note that the log size depends on the number of events generated in the system during a one-minute reporting interval. The log size must be large enough to accommodate those events.
15. Click **Apply** and **OK** to exit.

8.2.5 Verifying The Configuration

To verify that the device records login and logout events, follow these steps:

1. Log out of the device and then log back into the device.
2. Go to *Start --> Settings --> Control Panel --> Administrative Tools --> Event Viewer*
3. Select **Security Log** and go to *View --> Filter*. Select **Security for the Event Source** and **Logon/Logoff** for the Category fields
4. Click **Ok**

The Event Viewer should have the activity recorded as Event 528.

8.2.6 Log Files

The agent keeps logs of all failures or other application specific events to the Application Log. To view the logs:

Go to *Start --> Settings --> Control Panel--> Administrative Tools --> Event Viewer*

Click **Application Log** to view the logs. The product logs are located in the agent installation directory under the logs directory. For example, *c:\oracle\ConfigurationChangeConsoleAgent\logs*. Here is a list of some of the most common logs that you may need to refer to resolve issues:

Probe.log -- General product log for warnings or critical messages

Probe-err.log -- Only the errors that have caused a problem on the agent

8.2.7 Uninstalling the Agent

The agent must be uninstalled by a user with Administrator privileges.

To manually uninstall the agent, go to *Start --> Control Panel --> Add/Remove Programs* and select **Oracle Enterprise Manager Configuration Change Console Agent** from the list to uninstall the agent.

8.2.8 Reauthorizing the Agent With the Server

If for some reason the authorization credentials that you supply at agent installation time are incorrect, you can manually force the authorization to run again. You may notice that authorization might have failed because the agent never registered with the server by looking at the Administration > Devices > Devices screen on the Server.

To force reauthorization, follow these steps:

1. Open a DOS window
2. Change your directory to {agent_install_dir}/bin
3. Run the script: resetauth.bat
4. Answer the prompts providing a user name and password for an administrator-role user in the Configuration Change Console Server

For security reasons, if authentication fails, no message is sent back to the agent indicating this failure.

8.3 Windows NT 4.0 Agent Installation

The following sections describe the installation procedure for Windows NT 4.0 Agent.

8.3.1 System Requirements

The following are system requirements for installing the agent on a Windows NT 4.0 platform:

- NTFS file system. Windows NT proprietary file system that supports file-level security, compression and auditing.
- Service Pack 4. This Service Pack can be downloaded from the Microsoft website.
- WMI 1.5. If WMI is not installed on your system, you will need to assign the agent the NT Lite agent schedule template through the Compliance Solution user

interface. See the *Agent Administration* section of the *Compliance Solutions Users Guide* for more information.

8.3.2 Installing the Agent

To install the agent on a Windows NT 4.0 based platform, follow the same instructions as installing an agent on Windows 2000 as described in Section 8.2.2, "Installing the Agent".

During installation, the installer will verify that WMI has been installed. If you do not have WMI installed, you will either need to install WMI 1.5 or greater or use a lite version of the Windows agent.

8.3.3 Starting and Stopping the Agent

The agent should start automatically. If you selected "False" in Step 3 above, or in the event that the agent does not start automatically:

1. Go to *Start --> Control Panel --> Administrative Tools --> Services*
2. Right-click on the **Oracle Configuration Change Console Agent service** and click **Start**
3. To stop the agent, right-click on the **Oracle Configuration Change Console Agent service** and click **Stop**

8.3.4 Enabling Complete Real-Time Monitoring for the Windows Agent

The real time Windows agent modules rely on various capabilities of the operating system to collect all of the information on events. One part of this is to capture the user that made changes from the Windows Event Log. If you do not configure Windows to capture users that make changes, the agent will not capture this information, however it will still capture that a change happened and when it happened.

To configure the event log to work with real time monitoring, perform the following steps:

1. Go to *Start --> Programs --> Administrative Tools --> User Manager for Domains*
2. From the *User Manager screen*, click **Policies** from the menu bar and select **Audit Policy**. The next screen appears
3. From the *Audit Policy screen*, verify that the following options are selected:
   - Audit These Events
   - Login and Logoff
   - File and Object Access
4. From Explorer, select the directory that is being monitored, right-click and select **Properties**.
5. Go to the *Security tab*
6. Click **Auditing**
7. From the *Directory Auditing screen*, highlight **Everyone** and verify that **Write and Delete** are both selected under the *Success* column.

8.3.5 Log Files

The agent keeps logs of all failures or other application specific events to the Application Log. To view the logs, go to *Start --> Control Panel --> Administrative Tools --> Event Viewer*.

Click **Application** to view the logs. The product logs are located in the agent installation directory under the logs directory. For example, *c:\oracle\ConfigurationChangeConsoleAgent\logs*. Here is a list of some of the most common logs that you may need to refer to resolve issues:

Probe.log -- General product log for warnings or critical messages

Probe-err.log -- Only the errors that have caused a problem on the agent

8.3.6 Uninstalling the Agent

The agent must be uninstalled by a user with Administrator privileges.

To manually uninstall the agent, go to *Start --> Control Panel --> Add/Remove Programs* and select **Oracle Enterprise Manager Configuration Change Console Agent** from the list to uninstall the agent.

9

Installing the Agent On UNIX Platforms

This section outlines the steps to install an agent on Unix. There are also sections later in this book that relate to specific requirements for certain operating systems. Please be sure to review those sections as well.

9.1 UNIX Agent Installation

The following sections describe the process for installing the UNIX agents in console or graphical mode. Some operating systems have specific steps you must follow in addition to the standard Unix installation steps.

9.1.1 Installing the Agent

At any point during a console-based installation process, to return to the previous prompt, type **Back**.

To install the agents, you must log in as root. Later when the agent is running, it can run as any user as long as specific steps are followed as discussed later in this chapter.

1. Copy the *agent-x.bin* file from the Configuration Change Console Installation media where *-x* will indicate which operating system the agent installer is for.

   Ensure that the file is executable by using the following command where *<agent executable>* is the installation file for the specific platform:

   chmod +x <agent executable>

   For example: `chmod +x agent -lin.bin`

   For the Linux installation agent there are rules that must be followed that are specifc to Linux. Be sure to review Linux-based chapters.

2. From the Configuration Change Console Installation media, type the following command where *<agent executable>* is the installation file for the specific platform listed in the table above.

   To run the installer from the command line:

   `./<agent executable> -i console`

   To run the installer under X with a graphics-based installer:

   `./<agentexecutable>`

3. An introduction screen appears. Press **Enter** to proceed.

4. You will next be prompted for the agent installation directory.

5. Press **Enter** to accept the default installation directory or enter your own path for installation.
6. Enter the Configuration Change Console server URL. The URL has the format *t3s://hostname:port* where hostname is the host the primary server is located at if using a non-clustered environment. The Port is the HTTPS port of that server (default was 443 during server installation). If you are using a clustered environment, use *t3s://hostname1:port1,hostname2:port2,hostname3:port3*, etc where you put host name and port for each server (primary and secondary). Click **Next**.
7. The next section asks if you want to automatically start the agent after installation or not. To automatically start the agent after the installation, press **Enter**. If you do not want the agent to start automatically, enter **2.** Press **Enter**. You will need to start the agent manually if you do not set it to start automatically. Instructions for starting the agent using *\etc\init.d\arprobe* are discussed later in this chapter.
8. You will be asked for an administrator user name (default is *administrator*) for the Configuratioin Change Console Server. This is used to verify that the person installing the agent is authorized to do so.
9. The *Summary* screen will display. Verify that the install folder is correct and then click **Install** to proceed with the installation.
10. Click **Done** when the Installation Complete screen appears to exit the installer.

9.1.2 Starting and Stopping the Agent

The agent should start automatically if you chose to have it start during installation. In the event that it does not, from the command prompt type the following commands:

```
cd /etc/init.d/

./arprobe start
```

To stop the agent, type: `./arprobe stop`

> **Note:** You must be the root user to start the agent unless you follow the steps below on setting up the agent to operate as a non-root user.

9.1.3 Uninstalling the Agent

You must log in as root to uninstall the agent. The manual steps to uninstall the agent are:

From the command prompt, go to the agent uninstaller directory. For example, if you installed as root, you would type:

```
cd /root/oracle/ConfigurationChangeConsoleAgent/UninstallerData
```

Run the uninstaller by typing:

```
./Uninstall_Configuration_Change_Console_Agent
```

9.1.4 Running Agents As a Non-Root User

By default, agents are expected to run as the root user on Unix. You can configure the agents however after installation to run as a non-root user following the steps outlined below.

File Permissions

The first thing that needs to be changed are the file ownership for the agent files. The installer sets all files and directories for the agent to be owned by root (the user doing the install) and permissions are turned off completely for GROUP and OTHER USERS. If another user should see these files, then ownership of the files and directories must be changed from root to the desired owning user. The following is an example of how you change this, where you replace newuser with the login name of the user that will own the agent and change {agent_install_dir} to the full path of where the agent is installed:

```
chown -R newuser {agent_install_dir}
```

It is not recommended that you add permissions for the GROUP or OTHER USERS to see the files as they have secure information in these directories.

Set Binaries to Run

Two binaries that come with the agent need elevated priviledges to run to collect needed data. To allow this, do the following:

1. Stop the agent if it is running
2. Change your directory to {agent_install_dir}/bin where you installed the agent.
3. Run the following commands:

   chown root filewatcha

   chown root filewatchp

   chmod a+s filewatcha

   chmod a+s filewatchp
4. Edit the file */etc/rc.d/init.d/arprobe* and replace every instance of `$PROBE_HOME/bin/probe` with `sudo -u newuser "$PROBE_HOME/bin/probe".`
5. Start the agent. At this point, the agent should be running as user *newuser*.

9.2 Linux Agent Installation

The following sections describe the procedure for installing the Linux agent.

9.2.1 Linux Agent Installation Prerequisites

Before installing the Linux Agent you must have the Kernel Development package installed. The Kernel Development package is required because a loadable kernel module is compiled at installation time.

9.2.2 Installing the Agent

To install the Linux Agent, follow these steps. Note that all standard and recent packages must be installed before installing the agent.

1. Open a terminal window on the managed server. You must be logged in as root.
2. Insert the Configuration Change Console Installation media into your CD Rom drive. Mount the disk.
3. At the prompt, copy the *agent-lin.bin* file from the CD to the *tmp* directory with the following command where */mnt/cdrom* is the path to the mounted cd:

   ```
   cp /mnt/cdrom/agent-lin.* /tmp
   ```

4. Change directory to the *temp* directory by entering the command `cd /tmp` at the prompt

   You will need to change the *agent-lin.bin* filename to match your version of Linux.

   The following names should be used for Redhat Linux. For Oracle Enterprise Linux, rename to the same target name based on which Redhat Linux kernel matches the Oracle Enterprise Linux kernel to which you are deploying:

   - RedHat Linux v3: agent-lin-v3.bin
   - RedHat Linux v4: agent-lin-v4.bin
   - RedHat Linux v7.3: agent-lin-73.bin

5. From the temp directory, rename the file with the following command where *versionFileName* is the corresponding filename listed above:

   ```
   mv agent-lin.bin versionFileName
   ```

6. Run the new file by entering the following command at the prompt, where *versionFileName* is the new filename you renamed agent-lin.bin to:

   ```
   ./versionFileName -i console
   ```

   If you want to launch the graphical installer, leave off the *-i console* switch.

   The installer may take a few moments to load. Once ready, the introduction screen will display. The installation screens are the same that you see in this installation guide for Windows and for Unix above. Please refer to the Windows installation section for a walk-through of the screens you will configure.

7. One additional step that occurs towards the end of installation is the compilation of a loadable kernel module that is for real time file monitoring. You may notice a status message as to whether this succeeded or not.

8. After installation, delete the installation files in the *tmp* directory with the command:

   ```
   rm -i agent-lin*
   ```

9. Change directory to */root/oracle/ConfigurationChangeConsoleAgent/bin*

10. At the prompt enter: `./compmod.sh`

9.2.3 Kernel Module Compilation Issues

If you get a message during installation that compiling native audit modules failed, or if you are unable to get file events reported back to the server, compilation of the Linux auditing kernel module may have failed.

You can confirm if the auditmodule was loaded properly by running the following command.

```
grep -i auditmodule /proc/modules
```

If you do not get any output, then the auditmodule is not loaded and the agent will not be able to do real time file monitoring.

You can attempt to force the audit module to rebuild by following these steps:

1. Open a shell and change to the directory where you installed the agent, for example, `/root/oracle/ConfigurationChangeConsoleAgent/bin`

2. At the prompt enter `./compmod.sh`

3. Look at the *make.log* file and see if there are any errors that might be resolvable

If the module still is not able to load, and if you need to contact Oracle support about the issue, please be sure to include your make.log file and the output of the following command with your support ticket:

uname -a

This information will help Oracle to determine if the agent's real time file monitoring audit module can be built on your environment.

9.3 Solaris Agent Installation

Use the following steps to install the Solaris agent:

1. At the command prompt, log on to the Managed Server. You must be logged in as root.
2. From the Configuration Change Console Installation CD sent with the application, verify that the *agent-sol.bin* file is an executable, by typing:

   `chmod +x probe.bin`
3. For the remainder of the installation instructions, refer to the UNIX Agent Installation: Console Mode section, starting with Step 2.

9.3.1 Starting and Stopping the Agent

The agent should start automatically. In the event that it does not, from the command prompt, type the following commands:

```
cd /etc/init.d/
./arprobe start
```

Note: To stop the probe, type: `./arprobe stop`

9.3.2 Administrating Auditing on Solaris

The Solaris Audit is part of the Solaris TM SHIELD Basic Security Model (BSM) which provides additional security features. Auditing allows system administrators to monitor events and to detect user account logins and logouts as well as file changes.

If auditing is already enabled on the server, simply verify that the audit system configuration matches the configurations detailed below.

9.3.3 Configuring Solaris Auditing

The audit file can be configured to include specific events. The */etc/security/audit_control* file controls which events will be included in the audit file. This section summarizes the configuration; for further details, refer to the Sun Product Online Documentation site.

For FileRunning/Userrunning, the flags line in the file */etc/security/audit_control* should be set as follows:

```
flags: +fw,+fc,+fd,+lo
```

This configuration enables success/fail auditing for file writes (fw), file creates (fc), file deletes (fd), and login/logout events (lo); where '+' means to only log successful events. The login/logout events are not used by FileRunning but will be used by UserRunning. FileRunning filters the events by throwing away failed events and files

that do not match the include/exclude criteria. However, if you are interested in logging the failed events as well, remove the "+" sign before each event in the flag.

9.3.4 Audit Logs and Disk Space

The audit_control file also has entries to control where the audit logs are stored, and the maximum amount of disk space used by the audit system. The minimum requirement for FileRunning is approximately 5 minutes worth of data stored on the hard drive or the configured reporting interval time.

9.3.5 Auditing Users

The *audit_user* file controls which users are being audited. The settings in this file are for specific users and override the settings in the *audit_control* file, which applies to all users.

9.3.6 Managing Audit Files

FileRunning only reads the audit logs; it does not delete the logs. This might flood the system with log files and prevent it from logging additional events. To manage and delete old audit events while maintaining minimum FileRunnning/UserRunning requirements, do the following:

1. The auditing policy can be set to automatically drop new events (keeping only a count of the dropped events) rather than suspending all processes by running the following command:

   ```
   # auditconfig -setpolicy cnt
   ```

2. Run the following command to force the audit deamon to close the current audit log file and use a new log file.

   ```
   /usr/sbin/audit -s
   ```

3. Run the following command to merge all existing closed auditing log files into a single file with an extension of *.trash* and then delete the files.

   ```
   /usr/sbin/auditreduce -D trash
   ```

4. Run the *crontab* command to periodically run the commands in Step 2 and Step 3 above. The frequency at which these two commands are run can be adjusted based on the anticipated event volume and the amount of disk space allocated to auditing. The only requirement is that the time between the *audit -s* command and the *auditreduce - D* trash command is at least 2 minutes times the reporting interval for FileRunning and UserRunning.

9.3.7 Uninstalling the Agent

You must log in as root to uninstall the agent. To manually uninstall the agent, follow these steps:

1. From the command prompt, go to the agent uninstaller directory. For example, if you installed as root, you would type:

   ```
   cd /root/oracle/ConfigurationChangeConsoleAgent/bin
   ```

2. Run the uninstaller by typing

   ```
   ./Uninstall_Configuration_Change_Console_Agent
   ```

9.3.8 Log Files

The agent keeps logs of all failures or other application specific events to the Application Log. To view the logs:

Go to *Start --> Settings --> Control Panel--> Administrative Tools --> Event Viewer*

Click **Application Log** to view the logs. The product logs are located in the agent installation directory under the logs directory. For example, *c:\oracle\ConfigurationChangeConsoleAgent\logs*. Here is a list of some of the most common logs that you may need to refer to resolve issues:

Probe.log -- General product log for warnings or critical messages

Probe-err.log -- Only the errors that have caused a problem on the agent

9.3.9 Reauthorizing the Agent With the Server

If for some reason the authorization credentials that you supply at agent installation time are incorrect, you can manually force the authorization to run again. You may notice that authorization might have failed because the agent never registered with the server by looking at the Administration > Devices > Devices screen on the Server.

To force reauthorization, follow these steps:

1. Open a DOS window
2. Change your directory to {agent_install_dir}/bin
3. Run the script: resetauth.bat
4. Answer the prompts providing a user name and password for an administrator-role user in the Configuration Change Console Server

For security reasons, if authentication fails, no message is sent back to the agent indicating this failure.

9.4 HP-UX Agent Installation

This section describes the procedure for installing the agent on an HP-UX server. The Configuration Change Console Agent currently supports only HP-UX Version 11.11 and 11.23. Please read the prerequisites carefully to obtain the necessary software and patches before you begin the installation.

The HP-UX agent collects and reports data related to file and process changes, system resource utilization, and server configuration. By default, agents on the HP-UX platform do not report the users associated with file changes unless the Intrusion Detection System (HIDS) application is installed on the system. HIDS provides an auditing feature that logs file changes and the users associated with these reported changes.

The Configuration Change Console agent Supports HIDS 2.2 only. If you intend to install HIDS, you must be running HP-UX 11.11i or higher. HP-UX 11.0 is no longer supported.

This document provides basic instructions from the HIDS section of the *HP-UX HIDS System Administrator's Guide*.

9.4.1 Prerequisites

This section describes the prerequisites for installing the HP-UX agent, including all required patches.

Table 9–1 Hardware Prerequisites

Operating System	HP-UX 11i v1
CPU	At least a PA RISC 1.1

Table 9–2 Binary Patches

Operating System	HP-UX 11i v1
Patch	PHSS_26560

Table 9–3 HP Java Runtime Patches

HP-UX 11i v1 Patches
PHKL_25367 Solves kernel thread priority inversion problems.
PHCO_25452 Solves libc problems that cause degradation in Java applications.
PHKL_25614 Solves several memory and thread problems that affect Java performance.
PHKL_25728 Solves hangs in Java apps with large numbers of threads.
PHKL_25729 Solves signal and thread problems that prevent thread cancellation.
PHKL_25840 Solves severe thread performance problems in Java apps with large numbers of threads.
PHKL_25871 Supports Solaris-like semantics for concurrent close (kernel_dscrpt).
PHKL_27091 Solves thread problems that degrade Java apps with large numbers of threads.
PHKL_28489 Solves kernel trap handler problem causing hang after fork().
PHNE_29887 Supports Solaris-like semantics for concurrent close (transport).
PHCO_29960 Solves pthread synchronization causing hangs. This patch MUST be installed for JRE version 1.3.1.11 or later.

Table 9–3 (Cont.) HP Java Runtime Patches

HP-UX 11i v1 Patches
PHSS_30049 Solves problem with dld while loading native libraries for class ServerSocket

9.4.1.1 HIDS Patches

Each operating system may require specific patches to be installed. Additionally, other required patches may be reported by the HIDS 2.2 *CheckInstall* script. The patches and software can be downloaded from the HP website: *http://www.hp.com/*.

Table 9–4 HIDS Patches

Operating System	HP-UX 11.0	HP-UX 11i v1
Patch	No longer supported	PHKL_26074 s700_800 11.11 libaudit.a cumulative patch

9.4.2 HIDS Overview

HIDS auditing features works with the Configuration Change Console agent to provide a list of usernames associated with unauthorized access to files as well as file events such as the addition, creation, modification, and deletion of files.

Agents on the HP-UX platform do not report the users associated with any file changes unless the Intrusion Detection System (HIDS) application is installed and configured on the system.

9.4.2.1 HIDS Preinstallation

The HIDS 2.2 application must be installed before the agent is installed. The HIDS 2.2 application requires patches specific to each supported HP-UX version. For basic prerequisites, see those documented in the Prerequisites section above.

The directory structure for the HIDS 2.2 application is as follows:

- IDS application files: */opt/ids*
- Configuration files: */etc/opt/ids*
- Log files: */var/opt/ids*

Refer to the HIDS 2.2 documentation, *http://www.docs.hp.com/en/J5083-90011/index.html*, for installation and configuration instructions for your HP-UX version.

9.4.3 HP-UX 11.i v1 IDS Installation

Before proceeding with the installation, verify that you have all required patches installed on the system, as documented in the Prerequisites section above. All references to hostname must be replaced by the actual server hostname as provided by your System Administrator.

Follow these steps:

1. From the command prompt, login as *root*
2. Type the following commands:

```
mkdir /var/depot <Enter>
```

```
mkdir /var/depot/ids_11.i_admin+agent <Enter>

mkdir /var/tmp/idspatch_11.i <Enter>

mkdir /var/tmp/idsprod <Enter>
```

3. Copy the following patch into the */idspatch_11.i* directory:

   PHKL_26074 s700_800 11.11 libaudit.a cumulative patch

   Note: HP-UX 11i v1.6 and 11i v2 do not need this patch.

4. Unpack the patch file sets into their separate depots:

   ```
   sh -c 'for i in /var/tmp/idspatch_11.i/PH*; do sh $i; done'
   ```

5. Copy the patch depots into the ids_11.i_admin+agent depot by typing the following command in one line:

   ```
   sh -c 'for i in /var/tmp/idspatch_11.i/PH*.depot; do swcopy
   -s $i \* @ /var/depot/ids_11.i_admin+agent; done'
   ```

6. Download the 11.i IDS product depot into the following directory:

   var/tmp/idsprod/J5083AA_11.i.depot

7. Copy the entire 11.i product into the ids_11.i_admin+agent depot:

   ```
   swcopy -s /var/tmp/idsprod/J5083AA_11.i.depot \* \@
   /var/depot/ids_11.i_admin+agent
   ```

8. Install the IDS software by typing the following command. Note that you must reboot the system after the installation.

   ```
   # swinstall -x autoreboot=true -s hostname:/var/depot/ids_
   11.i_admin+agent \*
   ```

   Note: To start IDS, run the command: `/sbin/init.d/idsagent start`

   To stop IDS, run the command: `/sbin/init.d/idsagent stop`

9.4.4 Post Installation

This section documents the required procedural steps to complete after having installed the HIDS application on the server:

1. After the system has rebooted, run the *IDS_checkInstall* script to verify the HIDS application installation.

   ```
   /opt/ids/bin/IDS_checkInstall
   ```

2. Log in as user *ids* and generate the administrator keys by typing the following at the command prompt:

   ```
   ./IDS_genAdminKeys install
   ```

3. Generate the keys for the agent by typing the following at the command prompt:

   ```
   ./IDS_genAgentCerts
   ```

4. When prompted for which hosts the keys will be generated, type the hostname:

   The key file will be located in: */var/opt/ids/tmp/hostname.tar.Z*

5. Install the agent key by typing the following command:

   ```
   ./IDS_importAgentKeys /var/opt/ids/tmp/hostname.tar.Z
   hostname
   ```

6. Start the agent program by typing the following command:

   ```
   /opt/ids/bin/idsagent
   ```

9.4.5 HIDS Configuration

HIDS log files increase rapidly; however, the Configuration Change Console agent keeps log files truncated to save disk space. To ensure that the log files do not increase in file size while the agent is not running, run a script to periodically truncate the HIDS log files.

A sample script to manage your log files is provided below. You may want to customize the script according to your environment. This script should be run from the *crontab* and the *trunclog.sh* should be an executable file.

Sample contents of the *trunclog.sh* file:

```
#!/bin/sh
filesize=`/bin/ls -l /var/opt/ids/alert.log | /bin/awk '{print $5}'`
if [ "$filesize"  -gt "5000000" ]
then
  rm /var/opt/ids/alert.log
fi

rm /var/opt/ids/ids_1*
```

Sample entry to configure the crontab to run every hour where the bold letters are replaced by the actual path of the *trunclog.sh* file:

0* * * * /<location of script>/trunclog.sh

.

9.4.6 Installing the Agent

Refer to the UNIX Agent Installation: Console Mode section for instructions on installing the HP-UX agent.

9.4.7 Starting and Stopping the Agent

The agent should start automatically. In the event that it does not, from the command prompt, type the following commands:

```
cd /etc/init.d/
```

```
./arprobe start
```

To stop the agent, type: `./arprobe stop`

9.4.8 Uninstalling the Agent

You must log in as root to uninstall the agent. To uninstall the agent manually, follow these steps:

1. From the command prompt, go to the agent uninstaller directory. For example, if you installed by root, you would type:

   ```
   cd /root/oracle/Configuration_Change_Console_Agent
   ```

2. Run the uninstaller by typing:

```
./Uninstall_Configuration_Change_Console_Agent
```

9.4.9 Log Files

The agent keeps logs of all failures or other application specific events to the Application Log. To view the logs:

Go to *Start --> Settings --> Control Panel--> Administrative Tools --> Event Viewer*

Click **Application Log** to view the logs. The product logs are located in the agent installation directory under the logs directory. For example, *c:\oracle\ConfigurationChangeConsoleAgent\logs*. Here is a list of some of the most common logs that you may need to refer to resolve issues:

Probe.log -- General product log for warnings or critical messages

Probe-err.log -- Only the errors that have caused a problem on the agent

9.4.10 Reauthorizing the Agent With the Server

If for some reason the authorization credentials that you supply at agent installation time are incorrect, you can manually force the authorization to run again. You may notice that authorization might have failed because the agent never registered with the server by looking at the Administration > Devices > Devices screen on the Server.

To force reauthorization, follow these steps:

1. Open a DOS window
2. Change your directory to {agent_install_dir}/bin
3. Run the script: resetauth.bat
4. Answer the prompts providing a user name and password for an administrator-role user in the Configuration Change Console Server

For security reasons, if authentication fails, no message is sent back to the agent indicating this failure.

9.5 AIX Agent Installation

The following section describes the installation process for installing AIX agents.

9.5.1 Installation Prerequisites

To improve system performance, install the AIX 5.1 maintenance package ML510008 or higher before installing the AIX 5.1 agent. The maintenance package is available from the following site: *http://www-1.ibm.com/support/docview.wss?uid=isg1IY70781*

9.5.2 Installing the Agent

Refer to the UNIX Agent Installation: Console Mode section for instructions on installing, configuring and uninstalling the AIX agent.

9.5.3 Administering AIX Auditing

The AIX auditing subsystem allows an administrator to record security-relevant information, such as User Logins, Logouts, and file changes, for analysis against existing security policies and detection of security violations.

Setting up Auditing involves modification of the existing auditing configuration files. To set up auditing:

1. Log into the AIX machine as the root user.
2. Open a terminal window and change directory to */etc/security/audit*
3. Open the config file in vi.
4. Locate the following sections, and update or add the listed values:

```
start:
binmode = off
streammode = on
…
classes:
…
filewatch = PROC_Create,PROC_Delete,FILE_Open,FILE_Write,FILE_Close,FILE_
Link,FILE_Unlink,FILE_Rename,FILE_Owner,FILE_Mode,FILE_Fchmod,FILE_Fchown,FS_
Chdir,FS_Fchdir,FS_Chroot,FS_Mkdir,FS_Rmdir,FILE_Symlink,FILE_Dupfd,FILE_
Mknod,FILE_Utimes

users:
root = filewatch
default = filewatch
```

> **Note:** In this case default refers to all users that are not root. Further note that the last line of the config file should be a blank line.

5. Save your modifications and edit vi.
6. In the same directory (*/etc/security/audit/*) open the file streamcmds in vi.
7. Clear all text from the file. The default configuration for this file is not necessary, as the *FileRunning* agent module will operate as a direct audit reader. Clearing the file helps to reduce CPU usage and improve overall auditing performance.
8. Save the file and exit vi.
9. At the terminal prompt, enter the following command to initialize Auditing at system startup:

```
mkitab "audit:2:once:/usr/sbin/audit start"
```

9.5.4 Application Specific Auditing Functions

Certain agent modules may require extra configuration be done on the machine where the AIX agent is installed.

9.5.4.1 Informix Auditing - Configuring Audit Masks

The InformixAuditMonitor agent module requires Audit Masks to be configured on the machine on which the AIX agent is installed. To configure audit masks, follow these steps:

1. Log into the AIX machine as the root user.
2. Open a terminal window and change directory to *$activereasoningprobe/bin* where *activereasoningprobe* is the directory in which the AIX agent is installed.
3. Open the *ifxaudits* file in vi.
4. Update the following values:

- INFORMIXDIR - The installation directory of the Informix database.
- INFORMIXSERVER - The Informix Database server name
- ONCONFIG - the location of the Informix onconfig file.

5. Save the file and exit vi.
6. Open the file *ifxauditconf* in vi.
7. Modify the events associations for the following event masks, located at the bottom of the *ifxauditconf* file, as needed:
   - DEFAULTMASK - Events to monitor by default.
   - REQUIREMASK - Events which must be audited.
   - EXCLUDEMASK - Events to exclude from auditing.

   Each audit mask can have its member event and event groups modified to suit your needs. Similarly you can also modify the membership of an event group that is included in an audit mask. Note that multiple events and event groups are separated by commas.

   The full list of audit configuration settings, as found within the *ifxauditconf* file, is reprinted in the next section.
8. Optionally, you can create audit masks for specific users by adding lines in the following format where user is the username the event mask is intended for, and events are a list of the individual event mnemonics or event groups, separated by commas:

   ```
   ./ifxaudits -a -u <user> <events>
   ```
9. When finished editing, save the file and exit vi.
10. Run the modified *ifxauditconf* file to create the audit masks by entering the following at the terminal prompt:

    ```
    ./ifxauditconf
    ```
11. You will now use the modified *ifxaudits* file to configure the Informix Audit settings. At the terminal prompt, enter the following two commands:

    ```
    ./ifxaudits -e 0
    ```

    ```
    ./ifxaudits -l 7 -p /home/informix/aaodir
    ```

    Where */home/informix* is the directory of your Informix installation.

9.5.5 Audit Masks and Audit Events

You can specify events that you want to audit in an audit mask. Auditing in Dynamic Server is based on audit events and audit masks. Each audit mask can have its own set of Audit Events to detect. The table below lists the four basic types of audit masks configurable in the *ifxauditconf* file:

Mask Type	Mask Name
Individual user masks	Username
Default mask	_default
Compulsory masks	_require and _exclude
Template masks	_maskname

The following table lists the audit events you can choose to include in, or exclude from monitoring, along with the mnemonic used to specify them in the *ifxauditconf* file. Audit events are defined as database server activities that can be used to alter or query data or be used to possibly reveal the auditing configuration.

Table 9–5 Audit Events

Mnemonic	Event Name
ACTB	Access Table
ADCK	Add Chunk
ADLG	Add Transaction Log
ALFR	Alter Fragment
ALIX	Alter Index
ALOP	Alter Optical Cluster
ALTB	Alter Table
BGTX	Begin Transaction
CLDB	Close Database
CMTX	Commit Transaction
CRAM	Create Audit Mask
CRBS	Create Storage Space
CRDB	Create Database
CRDS	Create Dbspace
CRIX	Create Index
CROP	Create Optical Cluster
CRRL	Create Role
CRSN	Create Synonym
CRSP	Create Stored Procedure
CRTB	Create Table
CRTR	Create Trigger
CRVW	Create View
DLRW	Delete Row
DNCK	Bring Chunk Off-line
DNDM	Disable Disk Mirroring
DRAM	Delete Audit Mask
DRBS	Drop Storage Space
DRCK	Drop Chunk
DRDB	Drop Database
DRDS	Drop Dbspace
DRIX	Drop Index
DRLG	Drop Transaction Log
DROP	Drop Optical Cluster

Table 9–5 (Cont.) Audit Events

Mnemonic	Event Name
DRRL	Drop Role
DRSN	Drop Synonym
DRSP	Drop Stored Procedure
DRTB	Drop Table
DRTR	Drop Trigger
DRVW	Drop View
EXSP	Execute Stored Procedure
GRDB	Grant Database Access
GRFR	Grant Fragment Access
GRRL	Grant Role
GRTB	Grant Table Access
INRW	Insert Row
LGDB	Change Database Log Mode
LKTB	Lock Table
LSAM	List Audit Masks
LSDB	List Databases
MDLG	Modify Transaction Logging
ONAU	onaudit
ONCH	oncheck
ONIN	oninit
ONLG	onlog
ONLO	onload
ONMN	onmonitor
ONMO	onmode
ONPA	onparams
ONSP	onspaces
ONST	onstat
ONTP	ontape
ONUL	onunload
OPDB	Open Database
RDRW	Read Row
RLOP	Release Optical Cluster
RLTX	Rollback Transaction
RMCK	Clear Mirrored Chunks
RNDB	Rename Database
RNTX	Rename Table/Column
RSOP	Reserve Optical Cluster

Table 9–5 (Cont.) Audit Events

Mnemonic	Event Name
RVDB	Revoke Database Access
RVFR	Revoke Fragment Access
RVRL	Revoke Role
RVTB	Revoke Table Access
SCSP	System Command Stored Procedure
STCN	Set Constraint
STDF	Set Debug File
STDP	Set Dabase Password
STDS	Set Dataskip
STEX	Set Explain
STIL	Set Isolation Level
STLM	Set Lock Mode
STOM	Set Object Mode
STOP	Stop Statement
STPR	Set Pdqpriority
STRL	Set Role
STRT	Start Statement
STSA	Set Session Authorization
STSN	Start New Session
STTX	Set Transaction Mode
TMOP	Time Optical Cluster
ULTB	Unlock Table
UPAM	Update Audit Mask
UPCK	Bring Chunk On-line
UPDM	Enable Disk Mirroring
UPRW	Update Current Row
USSP	Update Statistics Stored Procedure
USTB	Update Statistics Table

9.5.6 Log Files

The agent keeps logs of all failures or other application specific events to the Application Log. To view the logs:

Go to *Start --> Settings --> Control Panel--> Administrative Tools --> Event Viewer*

Click **Application Log** to view the logs. The product logs are located in the agent installation directory under the logs directory. For example, *c:\oracle\ConfigurationChangeConsoleAgent\logs*. Here is a list of some of the most common logs that you may need to refer to resolve issues:

Probe.log -- General product log for warnings or critical messages

Probe-err.log -- Only the errors that have caused a problem on the agent

9.5.7 Reauthorizing the Agent With the Server

If for some reason the authorization credentials that you supply at agent installation time are incorrect, you can manually force the authorization to run again. You may notice that authorization might have failed because the agent never registered with the server by looking at the Administration > Devices > Devices screen on the Server.

To force reauthorization, follow these steps:

1. Open a DOS window
2. Change your directory to {agent_install_dir}/bin
3. Run the script: resetauth.bat
4. Answer the prompts providing a user name and password for an administrator-role user in the Configuration Change Console Server

For security reasons, if authentication fails, no message is sent back to the agent indicating this failure.

10

Agent Non-Interactive Silent Installer

The Configuration Change Console Silent Installer installs an agent on your system without displaying any installation screens or requiring any user interaction. Note that an exception occurs in the Windows platform where the initial installer screen will appear shortly before the installation turns to silent mode.

The installer does not inform you when the installation process is completed. The service will automatically start if you configure the agent for auto start.

10.1 Prerequisites and System Requirements

Refer to the prerequisites for each platform documented above for specific patches and other system requirements.

The following files are required to execute the silent installer:

- *agent.exe*. The executable that installs the agent. This is the generic agent executable; the actual executable file will be specific to the platform. For example, for a Windows platform, the agent executable will be agent-win.exe; on a Linux system, the agent executable will be agent-lin.bin.
- *agent.properties*. The text file used to configure the installation. Note that the agent.properties file must match the name of the executable. For instance, for an agent-win.exe executable, the respective .properties file should be agent-win.properties.
- *install.bat* (Windows platform) or *install.sh* (UNIX platform). The installation batch script that will run the installer and perform any customized work required for a particular installation. This script will be created by an administrator based on your specific environment needs and requirements.

> **Note:** The above files should all be stored in the same directory.

See Appendix A for an example *agent.properties* file for doing a silent installation.

10.2 Installing the Agent

To install the agent, do the following:

1. Configure the *agent.properties* file

   Under the agent installation directory, create a properties file with the same name as the agent executable file. For example, if the executable file is *agent-win.exe*, create a properties file with the name *agent-win.properties*. The *agent.properties* file

should contain configuration details specific to the installation environment. Refer to Appendix A for a sample *agent.properties* file.

The *agent.properties* contains the configurable fields described in the table below. All other fields should not be modified.

Table 10–1 agent.properties Field Values

Field	Description
USER_INSTALL_DIR	This is the installation directory for the application. Note that for Windows, the line is escaped. All spaces, colons, and back slashes must be properly escaped with a "\" preceding. For example: \=\\ :=\: For installation to a Program Files in Windows, the proper configuration would be: USER_INSTALL_DIR=C\:\\Program Files\\ConfigurationChangeConsoleAgent
ESCAPED_USER_INSTALL_DIR	This value is the escaped version of the USER_INSTALL_DIR. For all escaped "\", escape again. For example: \=\\\\ For installation to a Program Files in Windows, the proper configuration would be: ESCAPED_USER_INSTALL_DIR=C\:\\\\Program Files\\\\ConfigurationChangeConsoleAgent
JAVA_HOME	The agent has is bundled with its own JRE(1.5.0_15). This is the path the agent will use to find its JRE.
PATH_SEPARATOR	The OS specific separator. The default is to Windows. In UNIX, it is: PATH_SEPARATOR=//
AUTOSTART_*	The agent has an option of automatically starting the service after the installation completes. The values are : "0=do not start the service "1=automatically start the service
JNDI_PORT_*	JNDI_IP is the IP Address (or hostname) of the JMS Broker. The default port number is 443. Please consult your system or network administrator to determine which port should be used in your environment. The chosen port number must be used throughout the agent install process and must be matched when installing the Configuration Change Console. If you alter this value, please alter all entries in this install that reference the default port (23943).
EXTRA_*	This applies to UNIX environments only. These are additional paths used by the agent during run time to find specific libraries and binaries. EXTRA_PATH should point to the bin directory. EXTRA_LD_LIBRARY_PATH should point to the lib directory.
AUDIT_ENABLED	This field indicates whether auditing is enabled on the server. The values are: "1=Audit is enabled "0=Audit is disabled The default value is 1.
AUTHENTICATE_USER	The user name on the server to use for authenticating this agent install.

Table 10–1 (Cont.) agent.properties Field Values

Field	Description
AUTHENTICATE_PW	The password for the user used for authentication. Note: Snce the response file has the PW stored as plain text, you must be sure to remove this response value or the response file itself immediately after installing. Also, you may consider changing the user's password that did the installation after performing installs to ensure the security of this account.

2. Configure the install.bat/install.sh file

   Create an install.bat or install.sh file in the same directory where the agent executable and *agent.properties* files are stored. At minimum, it should contain the following:

```
@echo off
rem run the silent installer
agent.exe
```

   Where *agent.exe* is the specific agent executable for your platform, for example *agent-win.exe* for Windows based platforms.

   Additional customization may be required depending on your specific environment needs.

10.2.1 Generating a Response File

Instead of manually creating a response file, you can have a response file generated for you automatically by going through a normal interactive install (graphical or console). When launching the installer, add the *-r* flag, for example:

./agent-aix.bin -i console -r

After the installation is done, a file, *install.properties,* will be created in the same directory from which the installer was launched. You can use this as a response file for installers by following the steps in the previous section.

10.3 Uninstalling the Agent

If the agent was installed silently, the uninstaller will uninstall the agent silently, as well. Refer to the sections on uninstalling the agent for your specific platform, documented earlier in this document.

11

Post Installation Tasks

This chapter documents tasks that you may need to perform after the agent installation.

11.1 Reconnecting the Agent

There are two ways to reconfigure the Configuration Change Console Agent in order to disconnect it from one Configuration Change Console and re-connect it to another.

The first is to uninstall and re-install the agent using the new Configuration Change Console values. Consult the uninstallation and installation sections pertaining to your platform if you choose to perform a clean install.

The second method requires reconfiguration of the agent manually, which involves editing two configurations files under the agent installation directory structure. In order to make the change in this manner, follow the instructions in the following section.

11.1.1 Reconfiguring the Agent Manually

Follow these steps to reconfigure the agent manually.

1. Stop the agent on each device to be switched to the new Configuration Change Console Server. Use the *Devices screen* in the User Interface to STOP the agent or On the device where the agent is installed, STOP the agent in one of the following ways:

    1. For Windows. Stop the service.

        One approach is to go to *Control Panel --> Administrative Tools --> Computer Management --> Services and Applications --> Services*. Double-click on the Oracle Configuration Change Console Agent service and click **STOP**.

    2. For Unix. Run the following command where *agent_install_dir* is the directory of your agent installation:

        ```
        <agent_install_dir>/bin/arprobe stop
        ```

2. Change the configuration. Edit the following lines in the *<agent_install_dir>/config/probe.properties* file:

    - *java.naming.provider.url=t3s://server_address:port*

        The variable inputs include the new Configuration Change Console server IP JMS port that was specified during installation.

    - *probe.device.id=<PROBE_ID>*

Clear the variable value so the new Configuration Change Console Server can reassign appropriately.

3. Change the baseline value (initiate baseline update). Edit the *<agent_install_dir>/config/schedule.xml* file and change the following variable value from false to true where *agent_install_dir* is the directory of your agent installation:

   ```
   <Schedule doInitialBaseline="true">
   ```

4. Delete (or move to another location) the contents of *<agent_install_dir>/log* directory

5. Start the agent from the managed server.

12

Securing the Configuration Change Console

This section outlines various configurations that can be made after installing the Agents or server to secure your Configuration Change Console installation.

12.1 Securing Agent Files

The directory where the agent is installed must be set to readable only by the user the agent is running as. These files should not be world readable as they contain information that could be used to compromise the security of the agents.

On Unix, the installation will set all files to have Read, Write and Execute permissions revoked for Group or Others.

On Windows, the permissions are not set out of the box. The administrator must set the security rules either locally or from a domain controller to block any other users from reading files in the agent installation directory.

12.2 Securing Server Files

The directory where the server is installed must be set to readable only by the user the server is running as and privileged administrators. These files should not be world readable as they contain information that could be used to compromise the security of the server or agent to server communication.

The permissions are not set out of the box. The administrator must set the security rules either locally or from a domain controller to block any other users from reading files in the server installation directory.

12.3 Configuring JMS Access Control List

All communication between the agents and server uses Java Messaging Services (JMS). By default, the installation of the agent and servers sets the JMS connection to be over JMS with SSL which provides encryption of content being passed. The beta however does not include a mechanism to ensure there is a trust relationship between agent and server. To set up a secure environment, you need to modify the configuration of the JMS provider to create a list of hosts that are allowed to connect to the JMS queues and topics. Configuration Change Console is using the ORMIS protocol for JMS communication under the OC4J container.

ORMIS supports the ability to restrict incoming IP access by defining access control list (ACL) masks. These settings are made with the <*access-mask*> element and its <*host-access*> and <*ip-access*> subelements in the rmi.xml configuration file.

Access controls can be either exclusive or inclusive.

In the exclusive mode, access is denied to all IP addresses or hosts except those specifically included. Use *mode="deny"* in <access-mask>, then specify which particular hosts or IP addresses to allow by using *mode="allow"* in <host-access> or <ip-access> subelements (or both).

In the inclusive mode, access is available to all IP addresses or hosts except those specifically excluded. Use *mode="allow"* in <access-mask>, then specify which particular hosts or IP addresses to deny by using *mode="deny"* in <host-access> or <ip-access> subelements (or both).

The following snippet from *rmi.xml* configures an exclusive mode, allowing access to only localhost and 192.168.1.0. (255.255.255.0 is the applicable subnet mask.)

```
<rmi-server>
….
   <access-mask default="deny">
       <host-access domain="localhost" mode="allow"/>
       <ip-access ip="192.168.1.0" netmask="255.255.255.0"
mode="allow"/>
   </access-mask>
....
</rmi-server>
```

The *rmi.xml* file is located on the server in the following path:

SERVER_INSTALL_PATH/oc4j/j2ee/home/config/rmi.xml

12.4 Changing the SSL Method

The SSL communication between the agent, server and JMS provider uses an anonymous cipher crypt method. This will encrypt the contents, but does not ensure the agent or server is trusted. One way to protect this is through the use of JMS Access Control Lists described above, another is to change the SSL method from anonymous cipher crypt to using certificate based SSL.

The process involves either using an Oracle wallet based certificate and adding an XML snippet such as the following to your rmi.xml configuration file:

```
<ssl-config keystore="/wallets/wallet-server-a/ewallet.p12"
  keystore-password="serverkey-a" />
```

If you want to use Java keystore instead of Oracle Wallet, you would create a keystore using the Java keytool and then add something similar to the following example to your rmi.xml configuration file:

```
<ssl-config keystore="/keystores/keystore_a.jks"
   keystore-password="serverkey-a"/>
```

The *rmi.xml* file is located on the server in the following path:

SERVER_INSTALL_PATH/oc4j/j2ee/home/config/rmi.xml

When using keystores and passwords, the server keystore must contain the signed certificate of any client that is authorized to connect to OC4J through ORMIS, or contain the root CA-issued certificate of the client.

The process of configuring certificate based SSL is documented thoroughly in the *Oracle Containers for J2EE Security Guide 10g (10.1.3.1.0)*. Please see this documentation for additional details

13

Installing and Configuring BI Publisher Reports

This chapter explains how to install and configure BI Publisher Reports.

13.1 Overview of BI Publisher Server

This section provides instructions for installing and integrating BI Publisher Server with the Oracle Enterprise Manager 10g Configuration Change Console Application, for use in Change Report generation.

The installation of the Oracle Enterprise Manager 10g Configuration Change Console Application and its components must be executed in the order listed below:

1. Oracle database installation
2. Configuration Change Console Server installation
3. Agent installations
4. BI Publisher Reports Server installation

Note that the Oracle database is independent of each other and can be installed in any particular order as long as they are both installed before the Oracle Enterprise Manager 10*g* Configuration Change Console Solution and the agent.

13.1.1 System Requirements

The Configuration Change Console can integrate with Oracle BI Publisher for offline report generation. Please review the requirements for installing Oracle BI Publisher prior to installing. These requirements are outlined in the Oracle BI Publisher Installation documentation available online from Oracle.com.

When integrating the Configuration Change Console with BI Publisher, it is not required to have BI Publisher on the same server. It is recommended that BI Publisher be installed on its own server separately from the Configuration Change Console Server to ensure proper load balancing.

13.1.2 Preparing for Installation

Please review the prerequisites for each supported platform to ensure that the most recent service pack or patch is installed.

13.2 Installing BI Publisher Server

This section details all steps involved in installing the BI Publisher Server. For more detailed information covering the individual components of the BI Publisher database please see the BI Publisher Installation Documentation.

Follow these steps to install the BI Publisher Server:

1. Insert Oracle Business Intelligence Publisher Enterprise Version 10.1.3.4 CD into the installation directory.
2. Locate and run the *setup.exe* file in the *win32* directory of the cd.
3. The Oracle Universal Installer will start. Depending on the speed of your machine it may take a few minutes for the initial screen to display. Once loaded, click **Next**.
4. Specify the installation destination (Name and Full Path) on the *Specify File Locations* screen and click **Next**.
5. On the *Select Installation Type* screen select **Basic** option and click **Next**.
6. Set the password for the *oc4jadmin* administrator user and click **Next**.
7. Confirm the installation settings and click **Install**.
8. Install the BI Publisher.
9. After the installation, the installer will initiate the BI Publisher Configuration Assistant automatically. Click **Next** after the configuration.
10. The successful install screen will display. Click **Exit** to end the installation.

13.3 Configuring BI Publisher Server

This section covers the steps involved in Publishing the Oracle Enterprise Manager 10*g* Configuration Change Console Reports to the BI Publisher Server and configuring them for use with the Oracle Enterprise Manager 10*g* Configuration Change Console Application.

13.3.1 Pre-Configuration for BI Publisher Report Publication

Refer to the sections below for instructions you must complete before configuring the BI Pulbisher Report Publication.

13.3.1.1 Creating the Report Folder

To create the report folder, follow these steps:

1. Login the BI Publisher console as administrator role.
2. Click the *Reports* tab and then click the **Create a new folder link** on the left Folder and Report Tasks panel.
3. Input the new folder name (for example, EMReports) and click the **Create** button.
4. The new report folder is created and is listed on the right panel.

13.3.1.2 Creating the JDBC Connection

Follow these steps to create the JDBC connection:

1. Click the *Admin* tab
2. Click the *JDBC Connection* link under the Data Sources section.

3. Click the **Add Data Source** button to add a new JDBC connection. The Data Source Name should be hard-coded as *gateway* because the imported report will use the data source name by default. Click the **Test Connection** button to test whether the configuration is available. Click the **Apply** button to save the configuration.

Note: If during troubleshooting you do not see a list of available BI reports from Configuration Change Console, check to be sure the data source name is 'gateway'.

13.3.1.3 Installing the Schedule Schema

Follow these steps to install the schedule schema:

1. Click the *Admin* tab and click the *Scheduler Configuration* link under the System Maintenance section.
2. Input the database connection configurations (you can use the previous JDBC connection settings or another individual connection settings). Click the **Test Connection** button to test whether the configuration is available. Click the **Install Schema** button to create scheduler schema on the specified database. Click the **Apply** button to finish the configuration.

13.3.2 Configuring BI Publisher Report Publication

Follow the steps below to configure BI Publisher Report Publication:

1. Log in to the BI Publisher console using the administrator role.
2. Click the **Shared Folders** link to open the folder list screen.
3. On the folder list screen click the **EMReports** folder to open the folder.
4. Click the **Upload a report** link on the *Folder and Report Tasks* panel.
5. Click the **Browse…** button and navigate to *[integratedsoftware-install}* *\BIPublisher\Base\10.1.3.4\Reports* folder (The directory integratedsoftware-install will be generated when you unzip the integratedsoftware-install.zip package that you can download at the same location from which you downloaded the server).
6. Select the report package (the .zip file) and click the **Open** button.
7. Click the **Upload** button to finish importing the report.

13.3.3 Integrating BI Publisher

This section provides instructions for configuring the BI Publisher connection parameters through the Oracle Enterprise Manager 10*g* Configuration Change Console application interface.

Follow these steps to integrate BI Publisher:

1. Log into the Oracle Enterprise Manager 10g Configuration Change Console Product interface using the Administrator login.
2. From the Navigation tree, select Administration > Server Administration > Configuration > BI Publisher Server.
3. On the BI Publisher Server Configuration screen enter your server information:
   - **Server IP** - Hostname or IP address of the BI Publisher server

- **User Name** - Username used to access the BI Publisher server. Note that this field is case sensitive
- **Password** - Password used to access the BI Publisher server. This password will need to be re-entered in the Password (verify) field
- **Report Folder** - The folder path should be the corresponding path in BI Publisher. For example, if the folder was created under *Shared Folders* and named *EMReports*, the path should be */EMReports*.
- **WSDL definition** - The definition URL to access BI Publisher's web service API, in the format, where <*host*> is the hostname or IP address of the BI Publisher Reports server, and <*port*> is the port number used to access BI Publisher server. The default port used for BI Publisher is 9704:

  http://<host>:<port>/ xmlpserver/services/PublicReportService?wsdl

4. Click **Save**.

14

Installing and Configuring Change Management Server Integration

This chapter explains how to install and configure integration with a Change Management Server and to be able to determine whether changes that occur are authorized. Additional information related to configuration after the integration is successful is available in the *Configuration Change Console User's Guide*.

14.1 Remedy ARS 6.3 Integration

The integration instructions for Remedy Action Request System (ARS) 6.3 here assume that the following components have already been installed on a server:

- Remedy ARS 6.3
- Remedy Approval Server 5.1
- Remedy Change Management Server 6
- Remedy User client
- Remedy Admin client

14.1.1 Customizing Remedy Installation

Part of the integration effort is to load a custom definition file for the Configuration Change Console. This definition file adds new tabs to the *ChangeRequest* form to capture change events that are releated to the Change Request and also have additional workflow to send ticket updates, people updates and CTI updates to the Configuration Change Console Server.

It is recommended that you review the definition file prior to loading it into your Remedy instance.

The definition file is located in the *integratedsoftware-intall.zip* file that is part of the software distribution available where the server and agent installers were located. After expanding this zip file, look for the directory *Remedy/Base/ARS6.3/definition files*. Inside this directory is the *Remedy63-adapter-Generic.def* file. This is the definition file that must be loaded for integration to occur.

Here are the steps to follow to load the definition file:

1. Start the Remedy ARS Administrator client.
2. Log into your Remedy instance. If you are using an evaluation version of Remedy, you can use the Demo account.

3. In the Server Window, expand the Servers tab in the left pane, then click on the server name your Remedy ARS server is installed on.
4. Go to the Tools Menu, select *Import Definitions > From Definition File…*
5. Select the definition file *Remedy63-adapter-Generic.def* from the *integratedsoftware-install.zip* file as discussed above.
6. Click on Forms to highlight it and click on the **Add>>>** button.
7. Check the **Replace Objects on the Destination Server** checkbox and select **Replace with New type** under the *Handle Conflicting Types* input. Depending on how your Remedy ARS server is set up, you may not want to perform this step and instead may want to customize the definition file before importing. If you are simply integrating with a dedicated instance of the software for testing the Configuration Change Console, it is safe to perform these steps.
8. Click on the **Import** button to start the import.
9. Repeat steps 6 through 8 for *Active Links*.
10. Repeat steps 6 through 8 for *Filters*.
11. After the definition files are loaded, make a specific view of the Change Request form the default view for the user so that it is possible to see the new tabs. This step may not be required depending on how your Remedy server is configured and the user you will be using in the client. Click on the **Forms** link in the left pane to bring up the list of forms in the right pane.
12. Select the form *CHG:Change*, right click and select **Open**.
13. Select *Form Menu*, and then *Manage Views*.
14. Under the *Choose Default View* drop down, select **Administrator**.
15. Select the Administrator label row from the table and the Properties button.
16. In the dialog window that displays, select the checkbox for *Master View for Server Processing* and click **OK**.
17. Save the changes to the form.
18. Exit the Administrator client.

14.1.1.1 Verify the Form Changes

You can verify the form changes were at least partially successful by logging into the Remedy ARS User client and opening the Change Request form and verifying that there are two new tabs added to the right, ActiveR-DetectChanges, and ActiveR-Assigned Category List.

14.1.2 Configuration Changes in Remedy

The following two sections discuss how to mark users to send to Configuration Change Console and how to create new CTI for unauthorized tickets.

14.1.2.1 Marking Users to Send to Configuration Change Console

Once the definitions have been loaded, at least one user in Remedy needs to be marked as being integrated with the Configuration Change Console. These users can be assigned tickets when unauthorized changes are found and new unauthorized tickets are created. You can choose multiple users in Remedy to be available for this, but only one actual user can be selected in the Configuration Change Console from this list.

Follow these steps:

1. Start the Remedy User client and log in as an administrator user.
2. Open the Person Information form and search for an existing person or create a new person.
3. On the form input *AR-SendPersonInfo*, select the **Yes** radio button.
4. Save the person.
5. Repeat for any other people to which you may want to send unauthorized tickets.

All people that have this entry selected will be sent to the Configuration Change Console and will be able to be selected when assigning newly created tickets for unauthorized changes.

14.1.2.2 Create New CTI for Unauthorized Tickets

When the Configuration Change Console finds unauthorized changes, it can create new tickets. To create a ticket, it also needs to have a CTI structure it can assign to those newly created tickets. The following three CTI combinations should be created in the Remedy User client:

- Unauthorized > Unauthorized > Unauthorized
- Unauthorized > Unauthorized > Emergency
- Unauthorized > Unauthorized > Ticket Expiry

Follow these steps:

1. Start the Remedy User client and log in as an administrator user.
2. Open the Configure Categorization form to create a new CTI.
3. On the form, select *Change Request* as the module.
4. Enter Unauthorized as the Category.
5. Enter Unauthorized as the Type.
6. Enter Unauthorized as the Item.
7. Set the status to Active.
8. Save this categorization by clicking on the **Add** button.
9. Repeat steps 3 through 8 for the other two CTI combinations.

14.2 Install Agent for Integration

After customizing your Change Management Server, you can now install an agent that will be used for integration. The agent is the same as any other agent, however not every OS is supported. For a Remedy integration, you may use a Windows agent or an HPUX agent only.

The agent may be installed on the same server that the Change Management software is on, or it can be installed remotely. You may also choose to pick one of your existing agents to be the agent that will provide integration.

The installation process is the same as with any other agent. There are no additional steps other than deciding which agent will act as the Change Management integration agent.

14.3 Integration Steps on the Configuration Change Console Server

To finish the integration, you configure the Configuration Change Console Server to connect to the Change Management Server. The detailed instructions for this are available in the *Configuration Change Console User's Guide* chapter titled, *Integrating with A Change Management Server.*

A

Server Installation Information

This appendix discusses information about MIB files and Gigabyte RAM Tuning

MIB Files

The Following MIB files are for use with your SNMP server, as discussed in the SNMP Server Configuration section. The source can be modified by an administrator to suit your SNMP environment.

```
AR-SMI.mib
-- ****************************************************************
-- AR-SMI.my:  Active Reasoning Structure of Management Information
--
-- December 2004, Arminius Mignea, Jerry Russell
--
-- Copyright (c) 2002-2004 by Active Reasoning, Inc.
-- All rights reserved.
--
-- ****************************************************************
--

AR-SMI DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY,
OBJECT-IDENTITY,
enterprises
FROM SNMPv2-SMI;

activer MODULE-IDENTITY
LAST-UPDATED "200412200000Z"
ORGANIZATION "Active Reasoning, Inc."
CONTACT-INFO
"Active Reasoning
Customer Service

Postal: 1005 Elwell Court
Palo Alto, CA 94303
USA

   Tel: +1 650 404-9900

E-mail: info@activereasoning.com"
DESCRIPTION
"The Structure of Management Information for the
Active Reasoning enterprise."
```

```
REVISION      "200412200000Z"
DESCRIPTION
"Initial version of this MIB module."
::= { enterprises 22307 }-- assigned by IANA

activerProducts OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerProducts is the root OBJECT IDENTIFIER from
which sysObjectID values are assigned.  Actual
values are defined in AR-PRODUCTS-MIB."
::= { activer 1 }

activerAgentCapability OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerAgentCapability provides a root object identifier
from which AGENT-CAPABILITIES values may be assigned."
::= { activer 2 }

activerConfig OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerConfig is the main subtree for configuration mibs."
::= { activer 3 }

activerMgmt OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerMgmt is the main subtree for new mib development."
::= { activer 4 }

activerNotifications OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerNotifications is the main subtree for notifications
(traps) sent by Active Reasoning software."
::= { activer 5 }

activerAdmin OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerAdmin is reserved for administratively assigned
OBJECT IDENTIFIERS, i.e. those not associated with MIB
objects"
::= { activer 6 }

activerModules OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerModules provides a root object identifier
from which MODULE-IDENTITY values may be assigned."
::= { activer 7 }

activerPolicy OBJECT-IDENTITY
         STATUS current
         DESCRIPTION
                "activerPolicy is the root of the Active Reasoning-assigned
OID subtree for use with Policy Management."
         ::= { activer 8 }
```

```
activerExperiment OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"activerExperiment provides a root object identifier
from which experimental mibs may be temporarily
based."
::= { activer 9 }

temporary OBJECT-IDENTITY
STATUScurrent
DESCRIPTION
"Subtree beneath which temporary MIB objects were
placed."
::= { activer 10 }

END


AR-NOTIF.mib
-- ****************************************************************
-- AR-NOTIF.my:  Active Reasoning Notification Definition File
--
-- December 2004, Arminius Mignea
--
-- Copyright (c) 2002-2004 by Active Reasoning, Inc.
-- All rights reserved.
--
-- ****************************************************************
--

AR-NOTIF DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY,
OBJECT-IDENTITY,
OBJECT-TYPE, NOTIFICATION-TYPE,
enterprises
FROM SNMPv2-SMI
activerModules,
activerNotifications
FROM AR-SMI ;

arNotif MODULE-IDENTITY
LAST-UPDATED "200412200000Z"
ORGANIZATION "Active Reasoning, Inc."
CONTACT-INFO
"Active Reasoning
Customer Service

Postal: 1005 Elwell Court
Palo Alto, CA 94303
USA

   Tel: +1 650 404-9900

E-mail: info@activereasoning.com"
DESCRIPTION
"The Definition of Notification sent by OCC product of
Active Reasoning enterprise."
REVISION      "200412200000Z"
```

```
DESCRIPTION
"Initial version of this MIB module."
::= { activerModules 1 }-- assigned by IANA

occNotifMIBObjects OBJECT IDENTIFIER ::= { arNotif 1 }
occNotifConformanceOBJECT IDENTIFIER ::= { arNotif 2 }
occNotifInfoOBJECT IDENTIFIER ::= { occNotifMIBObjects 1 }
occNotifNotificationOBJECT IDENTIFIER ::= { occNotifMIBObjects 2 }

-- Notification information objects

occNotifInfoMessageOBJECT-TYPE
SYNTAXOCTET STRING (SIZE (0..256))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
"The text of the notification message generated by the
OCC server."
::= { occNotifInfo 1 }

-- Notifications

occNotifNotificationSentNOTIFICATION-TYPE
OBJECTS{ occNotifInfoMessage }
STATUScurrent
DESCRIPTION
"This notification is generated by the OCC server when
a policy has a 'send SNMP Trap' action defined."
::= { occNotifNotification 1 }

END
```

Gigabyte RAM Tuning

Although the Configuration Change Console Server cannot be configured for more than about 1.5 GB due to a limit in the Java JVM, if you are running multiple applications on the same server, it may be necessary to tune your Windows installation to allow for more memory to be used for other processes.

Microsoft Windows 2000 Advanced (and Data) Server, and Microsoft Windows Server 2003 feature a method of increasing the available virtual memory within the operating system to 4 GB, referred to as 4 Gigabyte RAM (3GT/4GT) Tuning. Of the 4 GB allocated through 3GT/4GT tuning, 3 GB are set aside for general program use, and 1 GB reserved for use by the operating system.

> **Note:** 4 gigabyte RAM tuning is not fully supported in Windows 2000 Professional, and Windows 2000 server.

To enable 4 Gigabyte RAM tuning, follow these steps:

1. Open a command window by selecting *Start --> Run* from the Start menu and entering *cmd*.
2. Navigate to the root directory of the boot drive for your computer (most often C:\). At the command prompt enter:

   ```
   edit boot.ini
   ```

3. Within the file, locate the following line under the [Operating Systems] section:

multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows Server"

Where Microsoft Windows Server is the directory of your Microsoft installation.

4. At the very end of the line, add the following switch:

   `/3GB`

5. Save the file and exit. You will need to restart your computer before the changes take effect.

B

Sample Agent Properties

The following is a listing of sample agent properties:

```
#    Configuration Change Console Basic Silent Agent Installation Configuration
#    This file should only be used to automate the agent installation
#    This file must be named according the installation file name.  For example
#    if the installation file is agent-win.exe, this file should be
#agent-win.properties

#Install as a silent installation
INSTALLER_UI=Silent

#Authenticate with Server
AUTHENTICATE_USER=administrator
AUTHENTICATE_PW=abcd

#  USER_INSTALL_DIR is the installation directory of the program
USER_INSTALL_DIR=C\:\\ActiveReasoningAgent

#  ESCAPED_USER_INSTALL_DIR.  Some OS allow spaces in the directory name
# this value is the escaped version of that USER_INSTALL_DIR
ESCAPED_USER_INSTALL_DIR=C\:\\\\ActiveReasoningAgent

# Which jre should this installation use... typical installs will use the user_
install_dir\jre
JAVA_HOME=C\:\\ActiveReasoningAgent\\jre

#  UNIX or WINDOWS Style escaped directory listing
#PATH_SEPARATOR=//
PATH_SEPARATOR=\\\\

#  AUTOSTART_TRUE=1  should the agent start immediately after installation
AUTOSTART_TRUE=0

############## PROBE RUNTIME CONFIGURATION #################

#PROBE_ID Assign the agent id
PROBE_ID=

#JNDI CONFIGURATION
JNDI_IP=PrimarySonicBroker.ip.address
JNDI_PORT=23943


#JMS CONFIGURATION
CONNECTIONFACTORY=ConnectionFactory
CF_TCP=1
```

```
#Agent Performance Monitoring
#PERF_OPTION="","Change Data Only"
PERF_OPTION="Performance & Change",""


##########UNIX ADDITIONAL CONFIGURATIONS ####
#UNIX requires additional values to be set during run time.
#These values are where to find specific libraries and binaries

EXTRA_PATH=/tmp/ActiveReasoning/Agent/bin
EXTRA_LD_LIBRARY_PATH=/tmp/ActiveReasoning/lib

#UNIX AUDIT ENABLED/DISABLED
#AUDIT_ENABLED=0
AUDIT_ENABLED=1
```

C

Configuring Oracle Database

This section describes the steps involved in setting up auditing within an Oracle database. If you are going to monitor an Oracle database with a trace component rule set, you will need to perform these steps before events will be captured.

Before configuring auditing it is suggested you review the Auditing Database Use section of the *Oracle Database Administrator's Guide*. This document provides an overview of Oracle's auditing functionality, as well as basic concepts and guidelines for auditing configurations.

Note that this document does not cover all details of configuring and fine tuning the Oracle audit system. Instead, this document serves as an example of the basic steps involved to configure the Oracle audit system, and how to use the Oracle Audit Monitor in conjunction with the Configuration Change Console.

Setting Auditing User Privileges

When you create a component to monitor an Oracle database, you will configure that component with a database user that can log into the database to read the audit trail. This user account should only have read only access to the audit tables only. This user is different than the user that the Configuration Change Console Server uses for its repository.

On the machine on where the Oracle database that will be monitored is installed or remotely:

1. Start the Oracle Enterprise Manager Console.
2. From the main navigation tree select the database instance you wish to audit. (*Network --> Databases --> Database Name*)
3. Log into the database as the system user.
4. From the navigation pane navigate to *Network --> Databases --> Database Name --> Security --> Users*. Select the user you will use for the Configuration Change Console. Note that this should not be a user used by an actual person within your infrastructure. Also, this user only needs read access to audit related tables.
5. Select the *Security tab*. Add the AUDIT SYSTEM privilege to the user by selecting it from the *Available window* and clicking the adjacent down-arrow icon. Optionally do the same for the AUDIT ALL permission. See the following section, Specifying Auditing Options for more information regarding the two permissions. Click **Apply**.

To turn on user privileges, follow these steps:

1. Start the Oracle Enterprise Manager Console.

2. From the main navigation tree select the database instance you wish to audit. (*Network --> Databases --> Database Name*).
3. Log in to the database as a sys user, connecting as SYSDBA.
4. From the navigation pane select *Network --> Databases --> Database Name --> Instance --> Configuration*
5. On the *General tab*, to the right of the navigation pane, click the **All Initialization Parameters…** button.
6. Locate the *audit_trail parameter* listing. Change the value from None to DB. Click **Apply**.
7. This change will require a restart of the database. Select the appropriate restart option and click **OK**.

Specifying Audit Options

Through SQL plus, an Oracle DBA can use audit and noaudit statements to configure audit options for the database.

The audit statement allows you to set audit options at three levels:

Table C–1 Audit Options Table

Level	Effect
Statement	Audits specific SQL statements or groups of statements that affect a particular type of database object. For example, AUDIT TABLE audits the CREATE TABLE, TRUNCATE TABLE, COMMENT ON TABLE, and DELETE [FROM] TABLE statements.
Privilege	Audits SQL statements that are executed under the umbrella of a specified system privilege. For Example, AUDIT CREATE ANY TRIGGER audits statements issued using the CREATE ANY TRIGGER system privilege.
Object	Audits specific statements on specific objects, such as ALTER TABLE on the employee table

In order to use the audit statement to set statement and privilege auditing options a DBA must be assigned AUDIT SYSTEM privileges. In order to use the audit statement to set object audit options, the DBA must own the object to be audited or be assigned the AUDIT ANY privilege within Oracle. Privilege assignments are covered in the following section.

Audit statements that set statement and privilege audit options can also include a BY clause to supply a list of specific users or application proxies to audit, and thus limit the scope of the statement and privilege audit options.

Some examples of audit statements follow below. Feel free to use these as a basis for the audit settings you specify within your database. Once all audit settings are in place you can create application policies, using the Oracle (SQL Trace) agent module with which to monitor the Oracle database instance.

Statement Audit Options (User sessions)

The following statement audits user sessions of users Bill and Lori.

```
AUDIT SESSION
BY scott, lori;
```

Privilege Audit Options

The following statement audits all successful and unsuccessful uses of the DELETE ANY TABLE system privilege:

```
AUDIT DELETE ANY TABLE
  BY ACCESS
  WHENEVER NOT SUCCESSFUL;
```

Object Audit Options

The following statement audits all successful SELECT, INSERT, and DELETE statements on the dept table owned by user jward:

```
AUDIT SELECT, INSERT, DELETE
   ON jward.dept
   BY ACCESS
   WHENEVER SUCCESSFUL;
```

Example Oracle Audit Monitor Configurations

The following command audits all basic statements. Extra statements are not audited.

Audit all by access;

The following statement audits all extra statements:

audit ALTER SEQUENCE,

ALTER TABLE,

DELETE TABLE,

EXECUTE PROCEDURE,

GRANT DIRECTORY,

GRANT PROCEDURE,

GRANT SEQUENCE,

GRANT TABLE,

GRANT TYPE,

INSERT TABLE,

LOCK TABLE,

UPDATE TABLE

by access;

The following command displays audit settings for statements

```
SELECT * FROM DBA_STMT_AUDIT_OPTS;
```

Once you have specified your audit configuration you can then set up a SQL Trace component rule set

D

SQL Server 2000 Database Auditing

The SQL Server 2000 Audit agent module requires you configure the SQL Server Profiler prior to creating component rule sets using the SQL Sever 2000 Audit module. Follow these steps to configure the SQL Server Profiler:

1. Open the SQL Profiler by clicking *Start --> Programs --> Microsoft SQL Server --> Profiler*
2. From the top menu bad select *File --> New --> Trace*
3. The *Connect to SQL Server window* will display. Enter the **IP address** of the SQL Server, **Login name** and **Password** and click **OK**.
4. In the resulting *Trace Properties window*, under the *General tab*, enter a name in the **Trace Name** field.
5. Select the *Events tab*. Under the *Available Event Classes window* expand the Objects node. Select the following elements and click the **Add >>** button.
   - Object:Closed
   - Object:Created
   - Object:Deleted
   - Object:Opened

   Do the same for all elements under the *Security Audit node*.
6. Select the *Data Columns tab*. In the Unselected data window, select the following elements, and click the **Add >>** button. Asterisked (*) elements may already be added.

EventClass *
DBUserName
LoginSid
ObjectName
OwnerName
TextData
ObjectName
OwnerName
TextData *
NTUserName *
SPID*
DatabaseName
HostName
NTDomainName
ObjectType
ServerName

Application Name *
LoginName*
StartTime*

7. Click **Run**

E

User Permissions For Database Monitoring

This section documents the permission requirements for the database monitoring. These steps are only necessary if you have configured the agent to monitor a database. You may modify permissions on an existing account or create a new account with the required permissions.

Refer to the platform that is specific to your database.

MS SQL Server 7/Server 2000

Follow the instructions in this section to set permissions for the user account on an MS SQL Server 2000 Database (SQL Server Standard Edition 7.0) or MS SQL Server 2000 Database (SQL Server Enterprise Edition 2000).

Object Permissions

At a minimum, the user account for database monitoring must have SELECT permissions for the following objects:

- <database>.dbo.sysusers
- <database>.dbo.sysobjects
- <database>.dbo.syscolumns
- <database>.dbo.systypes
- <database>.dbo.sysconstraints

Where <*database*> is the name of a monitored database, for example, "pubs" or "Northwind"

By default, everyone has SELECT permissions to the above system tables. DBAs, may have additional permissions available to them.

Setting User Permissions

The DBA can create a new user account for the purpose of database monitoring or use an existing user account. The DBA does not need to assign "Server Roles" and "Database Access" to this account. However, if the DBA has changed the default settings of some databases for security purposes, the DBA must give "SELECT" permissions of that system tables explicit.

Oracle 8*i*

Follow the instructions in this section to set permissions for the user account on an Oracle 8i Database (*Oracle 8i Enterprise Edition Release 8.1.7.0.0*).

Object Permissions

At a minimum, the account for database monitoring must have SELECT permissions for the following objects:

- sys.dba_tables
- sys.dba_tab_columns
- sys.dba_constraints
- dba_views
- dba_objects

Note: sys.dba_procedures is not a requirement.

Setting User Permissions

Typically, a new account does not have any SELECT permissions for the above objects. The DBA must assign the SELECT_CATALOG_ROLE role to this account. The SELECT_CATALOG_ROLE will make available the above objects as well as other objects. You may then manually set each object's permission level for your user. Keep in mind that if the user wishes to perform SQL queries as part of the Configuration Change Console monitoring, the tables listed above will need to be accessible to the user internally configured in your database Configuration Change Console.

After assigning SELECT_CATALOG_ROLE to this account, the agent can use the account to connect to the Oracle 8*i* server.

Oracle 10g

If you are running an Oracle 10*g* database, follow the instructions in this section to set permissions for the user account.

Object Permissions

At a minimum, the account for database monitoring must have SELECT permissions for the following objects:

- sys.dba_tables
- sys.dba_tab_columns
- sys.dba_constraints
- sys.dba_views
- sys.dba_objects
- sys.dba_procedures

Setting User Permissions

Typically, a new account does not have any SELECT permissions for the above objects. The DBA must assign the SELECT_CATALOG_ROLE role to this account. The

SELECT_CATALOG_ROLE will make available the above objects as well as others. You then have the option to manually set each object's permission level for your user. Keep in mind that if the user wishes to perform SQL queries as part of the Configuration Change Console monitoring, the tables listed above will need to be accessible to the user internally configured in your database Configuration Change Console.

After assigning SELECT_CATALOG_ROLE to this account, the agent can use the account to connect to the Oracle 9*i* or 10*g* server.

F

Agent Configuration File Parameters

Below is a list of parameters and their suggested value in the agent's config file:

<probehome>\config\probe.properties

Table F–1 Agent Configuration File Parameters

Parameter	Suggested Value
Debug=true	This parameter turns debugging on if the value is set to True. The default is False.
ProbeHome=c\:\\oracle\\ConfigurationChangeConsoleAgent	This parameter should match the location where the agent was installed. This is set by the installer and should not be changed. Java reads this property file and uses backslashes ("\") to ESCAPE characters (i.e. like the colon). Thus, if your Agent Home directory is written with backslashes, make sure you use TWO ("\\") otherwise, when Java re-writes this file while the agent is running, it will likely strip your slashes. Also, for this particular entry you can use forward slashed (even on Windows).
LogSize=10001	Indicates how many lines the agent will append to its log file before it overwrites it. If you have the parameter *Debug=true*, then the log file should be larger in size.
java.naming.provider.url=t3s://127.0.0.1:443	This is the URL the agent uses to connect to the server for communication. This is set by the installer and under normal operations does not need to be changed.
FirstRun=true	This parameter is ONLY set to True until after the agent does its first baseline, after which the value is set to False by the agent. The initial value is set by the installer and should not be changed. The agent automatically sets this to False after it successfully performs a baseline. After the first successful baseline, the baseline commands run once per day at 4:00pm PST, midnight GMT.
probe.device.id=3	The agent ID. This value should not be changed.
archive.enabled=false	Enable or disable saving a copy of the XML messages that will be sent to teh server representing real events. The XML archives will be stored in the agent installation folder under *{agent install dir}/archive*
jms.reconnect.minidelay=300 jms.reconnect.maxdelay=600	The time in seconds that the agent will wait between successive reconnects with the JMS server when it is not able to connect to the JMS server. The delay will be a random time between the mindelay and maxdelay value.

G

Oracle Database Auditing

This appendix describes the steps involved in setting up auditing within an Oracle database.

Before configuring auditing it is suggested you review the Appendix - Auditing Database Use section of the *Oracle 10g Database Administrator's Guide* (*http://download-west.oracle.com/docs/cd/A91202_01/901_doc/server.901/a90117/audit.htm*). This document provides an overview of Oracle's auditing functionality, as well as basic concepts and guidelines for auditing configurations. Note that this document requires an Oracle login. If you do not have a login, simply create one through the Oracle site.
(*https://profile.oracle.com/jsp/reg/createUser.jsp?src=1180585&act=5&language=en*)

This document does not cover all details of configuring and fine tuning the Oracle audit system. Instead, this document serves as an example of the basic steps involved to configure the Oracle audit system, and how to use the Oracle Audit Monitor in conjunction with the Configuration Change Console Compliance Solution.

Setting Auditing User Privileges

The Oracle Database user used with the Configuration Change Console compliance solution requires specific user permissions in order to run audit statements within the Oracle database, and thus configure auditing of database events.

On the machine on where Oracle is installed or remotely:

1. Start the Oracle Enterprise Manager Console.
2. From the main navigation tree select the database instance you wish to audit. (*Network -> Databases -> Database Name*)
3. Log into the database as the system user.
4. From the navigation pane navigate to *Network -> Databases -> Database Name -> Security -> Users*. Select the user you will use for the Configuration Change Console compliance solution. Note that this should not be a user used by an actual person within your infrastructure.
5. Select the *Security tab*. Add the AUDIT SYSTEM privilege to the user by selecting it form the Available window and clicking the adjacent down-arrow icon. Optionally do the same for the AUDIT ALL permission. See the following section, Specifying Auditing Options for more information regarding the two permissions. Click **Apply**.

Turning on Auditing

To turn on auditing, follow these steps:

1. Start the Oracle Enterprise Manager Console.
2. From the main navigation tree select the database instance you wish to audit. (*Network --> Databases --> Database Name*).
3. Log in to the database as a sys user, connecting as SYSDBA.
4. From the navigation pane select *Network --> Databases --> Database Name --> Instance --> Configuration*
5. On the General tab, to the right of the navigation pane, click the **All Initialization Parameters… button**.
6. Locate the *audit_trail* parameter listing. Change the value from None to DB. Click **Apply**.
7. This change will require a restart of the database. Select the appropriate restart option and click **OK**.

Specifying Audit Options

Through SQL plus, an Oracle DBA can use audit and noaudit statements to configure audit options for the database.

The audit statement allows you to set audit options at three levels:

Table G–1 Audit Option Levels

Level	Effect
Statement	Audits specific SQL statements or groups of statements that affect a particular type of database object. For example, AUDIT TABLE audits the CREATE TABLE, TRUNCATE TABLE, COMMENT ON TABLE, and DELETE [FROM] TABLE statements.
Privilege	Audits SQL statements that are executed under the umbrella of a specified system privilege. For Example, AUDIT CREATE ANY TRIGGER audits statements issued using the CREATE ANY TRIGGER system privilege.
Object	Audits specific statements on specific objects, such as ALTER TABLE on the employee table

In order to use the audit statement to set statement and privilege auditing options a DBA must be assigned AUDIT SYSTEM privileges. In order to use the audit statement to set object audit options, the DBA must own the object to be audited or be assigned the AUDIT ANY privilege within Oracle. Privilege assignments are covered in the following section.

Audit statements that set statement and privilege audit options can also include a BY clause to supply a list of specific users or application proxies to audit, and thus limit the scope of the statement and privilege audit options.

Some examples of audit statements follow below. Feel free to use these as a basis for the audit settings you specify within your database. Once all audit settings are in place you can create application policies, using the Oracle (SQL Trace) agent module with which to monitor the Oracle database instance.

Statement Audit Options (User Sessions)

The following statement audits user sessions of users Bill and Lori:

```
AUDIT SESSION
BY scott, lori;
```

Privilege Audit Options

The following statement audits all successful and unsuccessful uses of the DELETE ANY TABLE system privilege:

```
AUDIT DELETE ANY TABLE
    BY ACCESS
    WHENEVER NOT SUCCESSFUL;
```

Object Audit Options

The following statement audits all successful SELECT, INSERT, and DELETE statements on the dept table owned by *user jward*:

```
AUDIT SELECT, INSERT, DELETE
     ON jward.dept
     BY ACCESS
     WHENEVER SUCCESSFUL;
```

Example Oracle Audit Monitor Configurations

The following command audits all basic statements. Extra statements are not audited.

```
Audit all by access;
```

The following statement audits all extra statements:

```
audit ALTER SEQUENCE,
ALTER TABLE,
DELETE TABLE,
EXECUTE PROCEDURE,
GRANT DIRECTORY,
GRANT PROCEDURE,
GRANT SEQUENCE,
GRANT TABLE,
GRANT TYPE,
INSERT TABLE,
LOCK TABLE,
UPDATE TABLE
by access;
```

The following command displays audit settings for statements:

```
SELECT * FROM DBA_STMT_AUDIT_OPTS;
```

Once you have specified your audit configuration you can then set up a SQL Trace application policy.

H

Server Configuration Properties

This appendix describes some configurable server properties that can be modified for your environment.

Server Properties Stored In the Repository

Some properties that are used by the server are stored in a table in the Server's repository. This table is called serverproperty. The table below lists some properties that can commonly be configured after the product is installed that do not have a user interface. Other properties not listed here should not be changed from their defaults or have a user interface that controls the value.

You must restart the server service after changing any of these values.

Table H–1 Server Properties Stored In Repository

Property Name	Default Value	Description
websessiontimeout	30	The time in minutes a web-based session will be closed due to inactivity. Making this too large can cause memory problems as unused sessions will still consume memory.
autoreload_enabled	1	For accessibility, this will turn on/off all instances where a page is set to reload automatically at some preconfigured time. Set it to 0 to turn off auto reloading.
archiveprobemessages	false	This option will store all inbound XML messages agents send into files in the server under the *{server install dir}\probearchive* directory. Caution should be used when enabling this because this directory can fill up very fast and must be cleared regularly.
perform_md5_on_change	true	Configure whether agents should capture the md5 of a file when a change occurs and report this information back to the server. You may want to turn this off if it causes too much load on the agent machine.