Oracle® Enterprise Manager

Configuration Change Console Installation Guide

10*g* Version 10.2.0.5 for Windows or UNIX

E15311-01

June 2009

ORACLE®

Oracle Enterprise Manager Configuration Change Console Installation Guide, 10*g* Version 10.2.0.5 for Windows or UNIX

E15311-01

Primary Author: Leo Cloutier

Contributing Author: Jerry Russell

Contributor: Daniel Hynes

Contents

4 Server Pre-Installation Tasks

5 Installing and Uninstalling the Configuration Change Console Server for Microsoft Windows

6 Installing and Uninstalling the Configuration Change Console Server for Linux

7 Overview of Configuration Change Console Agent

8 Agent Installation General Prerequisites

14 Securing the Configuration Change Console

15 Installing and Configuring BI Publisher Reports

16 Installing and Configuring Change Management Server Integration

Preface

This guide describes the installation 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 Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711.

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-win32.exe -i console
```

```
Agent-win32.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 the number of devices being monitored.The first table shows monthly 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. If your database purging configured for 90 days, these numbers must be multiplied by 3.

Table 1–1 Example Monthly Event Counts vs. Number of Agents

Number of Agents	Low Change Rate (5 changes per agent per day)	Nominal Change Rate (30 changes per agent per day)	High Change Rate (100 changes per agent per day)	Very High Change Rate (500 changes per agent per day)
100	15K	90K	300K	1.5M
250	39K	234K	780K	3.9M
500	78K	468K	1.6M	8.0M
1000	155K	930K	3.1M	15.5M
2500	388K	2.3M	7.8M	--
5000	775K	4.7M	15.5M	--
10000	1.6M	9.3M	--	--
15000	2.3M	13.8M	--	--

(Note: Cells with "--" represent extremely large environments that may require special configurations beyond what is supported with the out-of-the-box product.)

The next table shows the estimated Configuration Change Console tablespaces size versus the number of changes in the environment. The number of changes shown in the table 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 table 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 table by three.

Table 1–2 Minimum Tablespace Size vs. Change Counts

Total number of changes stored in repository	GATEWAY Tablespace	GATEWAY_ LGDATA Tablespace	GATEWAY_INDEX Tablespace	Total Minimum Tablespace size
100K	2GB	2GB	4GB	8GB
500K	2GB	2GB	4GB	8GB
1.0M	3GB	2GB	4GB	9GB
5.0M	4GB	3GB	6GB	13GB
10.0M	6GB	4GB	8GB	18GB
20.0M	8GB	12GB	24GB	34GB
50.0M	10GB	30GB	60GB	100GB
100.0M	15GB	60GB	120GB	195GB

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 table does not include other tablespaces such as TEMP and UNDO or Redo logs. You must allocate an appropriate amount of disk space for these 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 1–3 Recommended Size for Environments

Number of Agents	Change Rate	Database Hosts	CPUs/Host	Physical Memory	Minimum Disk Space
100	Nominal	1	1 dual-core 3 GHz	4 GB	30 GB

Table 1–3 (Cont.) Recommended Size for Environments

Number of Agents	Change Rate	Database Hosts	CPUs/Host	Physical Memory	Minimum Disk Space
1000	Nominal	1	2 dual-core 3 GHz	4 GB	40 GB
5000	Nominal	1	--	8 GB	60 GB
15,000	Nominal	1	4 dual-core 3 GHz	8 GB	150 GB
1000	Very High	1	4 dual-core 3 GHz	8 GB	150 GB

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.

1.3 Considerations For High Scale Environments

When setting up a database for a high change rate environment, there are several factors that must be taken into account. Use the following recommendations regarding the database the Configuration Change Console uses for its repository.

1.3.1 Fast Disk, Filesystem I/O for REDO Logs

The disk on which the REDO logs are located should be as fast as possible and should be dedicated for REDO logs only. If your database uses a RAID disk structure, the REDO logs should be located on disks using RAID1. A RAID5 disk layout is too slow for the REDO logs. In addition, you can alternate REDO logs onto different disks to minimize the effect of the archiver on the log writer.

If the disk on which the REDO logs is on is too slow, or if the filesystem I/O to the REDO log files is too slow, the database will see transaction timeouts due to high I/O waits on the logs.

1.3.2 Log Writer Write Performance and I/O Subsystem Settings

Whenever possible, the database should make use of the best/optimal performance settings supported for Oracle DB performance in the available I/O subsystem in the environment. For example, the Oracle database can make use of Direct I/O bypassing Vendor/OS buffer cache in writes to redo log as well as data files. In addition the Oracle database can also make use of Asynchronous I/O. By default, Oracle DB initialization parameter *disk_asynch_io* is set to true (useful for ASM/raw devices usage). The parameter *filesystemio_options* should also be checked to ensure the proper value is used for your environment. For Operating System and File Systems where Direct I/O as well as Async I/O is supported, the database should be configured to make use of it.

1.3.3 VLM Configuration for Windows 32-Bit

The Oracle DB process in Windows can only make use of extra RAM available through PAE/AWE above the 4GB limit for data segments (buffer cache) only. All other process address space components need to fit within the theoretical 1.7 or 2.7GB limit (in case of /3GB).

Also the AWE_WINDOW_MEMORY setting must be set in the registry as mentioned here and it must be greater than or equal to 1GB default limit.

The requirements for taking advantage of this support are:

1. The computer on which Oracle Database is installed must have more than 4 GB of memory.
2. The operating system must be configured to take advantage of Physical Address Extensions (PAE) by adding the /PAE switch in *boot.ini*. See Microsoft Knowledge Base article Q268363 for instructions on modifying *boot.ini* to enable PAE.
3. It is advisable to enable 4GT support by adding the /3GB parameter in *boot.ini*. See Microsoft Knowledge Base article Q171793 for additional requirements and instructions on modifying *boot.ini* to enable 4GT.
4. The user account under which Oracle Database runs (typically the LocalSystem account), must have the *Lock memory pages* Windows 2000 and Windows XP privilege.
5. USE_INDIRECT_DATA_BUFFERS=TRUE must be present in the initialization parameter file for the database instance that will use VLM support. If this parameter is not set, then Oracle Database 10*g* Release 1 (10.1) or later behaves in exactly the same way as previous releases. Initialization parameters DB_BLOCK_BUFFERS and DB_BLOCK_SIZE must be set to values you have chosen for Oracle Database.
6. The total number of bytes of database buffers (that is, DB_BLOCK_BUFFERS multiplied by DB_BLOCK_SIZE) is no longer limited to 3 GB.

   Dynamic SGA and multiple block size are not supported with VLM. When VLM is enabled, the following new buffer cache parameters are not supported:

   DB_CACHE_SIZE
   DB_2K_CACHE_SIZE
   DB_4K_CACHE_SIZE
   DB_8K_CACHE_SIZE
   DB_16K_CACHE_SIZE
   DB_32K_CACHE_SIZE

7. Registry parameter AWE_WINDOW_MEMORY must be created and set in the appropriate key for your Oracle home. This parameter is specified in bytes and has a default value of 1 GB. AWE_WINDOW_MEMORY tells Oracle Database how much of its 3 GB address space to reserve for mapping in database buffers. This memory comes from the 3 GB virtual address space in Oracle Database, so its value must be less than 3 GB. Setting this parameter to a large value has the effect of using more of the address space for buffers and using less AWE memory for buffers. However, since accessing AWE buffers is somewhat slower than accessing virtual address space buffers, Oracle recommends that you tune these parameters to be as large as possible without adversely limiting database operations.

   In general, the higher AWE_WINDOW_MEMORY is set, the fewer connections and memory allocations will be possible for Oracle Database. The lower AWE_WINDOW_MEMORY is set, the lower the performance.
8. Once this parameter is set, Oracle Database can be started and will function exactly the same as before except that more database buffers are available to the instance. In addition, disk I/O may be reduced because more Oracle Database data blocks can be cached in the System Global Area (SGA).

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 10*g* (version 10.2.0.4 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 Change 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, check mark **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 *Administration* 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 an environment with a large number of agents, you should allocate 4 GB for the TEMP tablespace and 4 GB for the UNDO tablespace.

2.2.3 Configuring REDO Logs

For an evaluation environment or production environment with a small number of agents and low change rate, the out-of-the-box REDO log settings should be sufficient.

For an environment with a large number of agents or high change rate, more redo logs and redo log groups may be needed. Given the potential high transaction rate of Configuration Change Console, each redo log should be at least 500MB in size. Check with your database administrator for guidelines on how to properly configure the REDO log management.

2.2.4 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.

2.2.5 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.

2.2.5.1 Configuring Number of Connections

When sizing your database, you should consider the number of concurrent processes and sessions your database has configured.

For a non-clustered installation, Weblogic is configured to use, at most, 200 JDBC connections. The database should be configured to have 250 processes and 375 sessions (1.5 x processes). If you increase the Weblogic JDBC pool size, the database must be adjusted accordingly.

For a large environment, the cluster configuration determines how many connections will be needed in the database. For example, if you have a clustered environment with a Primary Server, 3 Secondary Servers, and 4 Messaging Brokers, you may have the Weblogic JDBC connection pool set to 300 connections. The determination of the number of connections is described in more detail in Section 5.4.5, "Adjusting the

Database Connection Sizes" related to Cluster Installations. With these 4 servers connecting to the database, Weblogic will consume, at most, 1200 connections. To support this, the database will need 1250 processes and 1875 sessions.

2.2.6 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 7, "Overview of Configuration Change Console Agent" or Chapter 14, "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

Number of Agents	Change Rate	Server Hosts	CPU/Host	Physical Memory	Minimum Disk Space per Host
100	Nominal	1 host (no clustering)	1 dual-core 3 GHz	4 GB	30 GB
1000	Nominal	1 host (no clustering)	2 dual-core 3 GHz	4 GB	30 GB
5000	Nominal	3 hosts (clustered with 1 primary, 2 secondaries, 2 Messaging brokers)	2 dual-core 3 GHz	8 GB	100 GB
15,000	Nominal	4 hosts (clustered with 1 primary, 3 secondaries, 2 Messaging brokers)	2 dual-core 3 GHz	8 GB	100 GB

Table 3–1 (Cont.) Recommended Sizes for Environments

Number of Agents	Change Rate	Server Hosts	CPU/Host	Physical Memory	Minimum Disk Space per Host
1000	Very High	4 hosts (clustered with 1 primary, 3 secondaries, 2 Messaging brokers)	2 dual-core 3 GHz	8 GB	100 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 a small number of agents and change rate, although minimum requirement would be one server host, you can use clustering with 1 primary and 2 secondaries and 2 Messaging Brokers so that you have a secondary available to process events in case one of them is down.

Any host that has a Messaging Broker should have enough disk space available to allow for the broker to queue up messages from agents that cannot be processed in a timely manner by the servers. Configuration Change Console is designed to allow agent messages queue up into the messaging broker servers, so that if the primary, secondary servers, and database are under high load, the agent messages are not lost and can be processed at a later time. For a production environment, it is best to provide at least 50GB of disk space for each messaging broker to ensure messages from agents are not lost when the servers cannot process bursts of events.

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 *Oracle Enterprise Linux V4*, *V5* or equivalent. There is a separate installer for the Windows and Linux platforms.

When running the Configuration Change Console server, the X Windows subsystem is required for graph generation. If X Windows is not installed/configured properly or if

the shell under which the server starts does not have a DISPLAY set, then graph generation will fail throughout the product.

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.

3.1.6 User Privileges When Installing the Configuration Change Console Server on UNIX

The following information applies to all Unix platforms on which Configuration Change Console server can be installed.

The Configuration Change Console server should be installed as root if you want the server to register a service that can start at the time your server starts. Also, to be able to specify certain ports (for example: port 80 and 443) for the web-based console, you need to have the proper privilege when running the server.

The product relies on the X-Windows subsystem for its graph generation code so the user that the Configuration Change Console server runs as must have access to this subsystem.

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. Each physical device in a cluster that has a primary or server installed must be able to connect to the database.

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 product.

> **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.

See the operating system instructions for equivalent configurations on UNIX operating systems.

Configure the Configuration Change Console server to expose the external NIC properly by using the following procedure for Windows:

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. For completely proper operation of the Configuration Change Console, all of the system clocks for the agents, jms brokers, and servers should have their clocks synchronized. Failure to use synchronized times will result in events appearing to be stamped with the wrong time, failed change management reconciliation, failed notifications and possibly missed events.

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 on Windows, 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.

See the operating system instructions for equivalent configurations on UNIX operating systems.

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 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 for Microsoft Windows

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

When installing any of the server components (Primary server, Secondary server, or Messaging Broker server), the file *server_win32.part2* must be in the same directory where *server_win32.exe* is located. This additional file is required for installation of the server elements.

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-win32.exe** file from the Configuration Change Console media. The Installer will take a few moments to initialize. Ensure that the same directory from where you are running this installation also has the file **server-win32.part2** as this file is also required for installation. The installer will not proceed if this file is missing.
2. Click **Next** when the Introduction screen appears
3. Specify the *installation directory* or choose the *default*. Click **Next**.
4. Choose the type of installation being performed. In this case, you would choose **Non-Clustered**, then click **Next**.
5. Choose server type as **Primary** (with bundled Admin Server), then click **Next**.
6. Note that the Oracle database must be installed and running properly before the Configuration Change Console can be installed.

   Click **Next** if you have the Oracle database installed and followed the steps to create the gateway database or **Cancel** if you still need to perform these steps.
7. 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**.

8. 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.

9. 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**.
10. Enter your **organization name** and click **Next**. If you will be installing multiple instances of Configuration Change Console, the organization name should reflect the name of your IT organization, such as "West Coast Operations" versus "East Coast Operations". This organization name can be used if creating BI Publisher Reports that span multiple instances of Configuration Change Console Server.
11. 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.
12. 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.
13. 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.
14. Click **Next**.
15. 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 Config Change Console PrimaryServer*. Additionally, the Weblogic admin console service called *Oracle Config Change Console AdminServer* is created. If you do not start this service at install time, you can go to the Services Control Panel at any time to start it.
16. 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. If you specify the maximum memory to be larger than your server OS is configured to handle, the service will fail to start.

17. 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.
18. 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 and any number of messaging broker servers. All of these servers will belong to the same Oracle Weblogic domain called *ConfigChangeConsole*. This domain is set up automatically when you start performing the installation steps in this chapter.

In a clustered environment, you must be sure you install all three types of servers (primary, secondary, and messaging broker) to ensure that the product will operate properly. In environments with many agents, there may be more messaging brokers installed in the cluster than there are secondary servers. As a guideline, there should be at least one messaging broker for every 3000 agents. Adding too many messaging brokers and secondaries, however, will also put more load on your database as the number of simultaneous writes of events to the database is based on the number of Messaging Brokers multiplied by the number of Secondaries. If you do not define enough brokers and secondaries, then messages will back up in the Messaging Brokers and the processing of them will be delayed.

If you install an environment as clustered, you must have a primary server with its built in admin server, at least one secondary, and at least one messaging broker. If you do not have at least one secondary and messaging broker, events will not be captured from agents.

All of the servers in the cluster (Primary server, Secondary Servers, and Messaging Broker Servers) should be in the same network segment to reduce the chance of connection problems or slow performance due to network latency. The ping latency should be less than 0.5ms between the servers.

You cannot install a Secondary Server on the same physical host as the Primary Server.

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

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-win32.exe** file from the Configuration Change Console media. The Installer will take a few moments to initialize. Ensure that the same directory from where you are running this installation also has the file *server-win32.part2* as this file is also required for installation. The installer will not proceed if this file is missing.
2. Click **Next** when the Introduction screen appears
3. Specify the installation directory or choose the default. Click **Next**.
4. Choose the type of installation being performed. In this case you would choose **Clustered**, then click **Next**.
5. Choose server type as **Primary (with bundled Admin Server)**, then click **Next**.
6. Note that the Oracle database must be installed and running properly before the Configuration Change Console can be installed. Click **Next** if you have the Oracle database installed and followed the steps to create the gateway database or **Cancel** if you still need to perform these steps. If you click Cancel, you must reinstall the Configuration Change Console at a later time.
7. 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**.
8. Enter your organization name. Click **Next**. If you will be installing multiple independent instances of Configuration Change Console, the organization name should reflect the name of your IT organization, such as "West Coast Operations" versus "East Coast Operations". This organization name can be used if creating BI Publisher Reports that span multiple instances of Configuration Change Console Server.
9. 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**.
10. 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.

11. 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.
12. 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**.
13. 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.
14. 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 CCC PrimaryServer*. If you do not start this service at install time, you can go to the Services Control Panel at any time to start it.
15. 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. If you specify the maximum memory to be larger than your server OS is configured to handle, the service will fail to start.
16. 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.
17. 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 the size of the deployment. Note: The Secondary Server cannot be installed on the machine on which the Primary Server is installed.

1. Double-click on the **server-win32.exe** file from the Configuration Change Console media. The Installer will take a few moments to initialize. Ensure that the same directory from where you are running this installation also contains the file *server-win32.part2* as this file is also required for installation. The installer will not proceed if this file is missing.

2. Click **Next** when the Introduction screen appears.
3. Specify the installation directory or choose the default. Click **Next**.
4. Choose the type of installation being performed. In this case, you would choose **Clustered**, then click **Next**.
5. Choose a server type of **Secondary**, then click **Next**. Note that installing a secondary server will not include any messaging broker servers, so you must install one or more messaging brokers after installing your secondaries. The secondary and messaging brokers are separated so that each can have the most amount of memory available for a java process. A Java virtual machine will be limited in how much memory is available to it based on Java and the Operating System (typically about 1.4 GB for Windows 32-bit).
6. 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`.
7. 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**.
8. Enter the hostname and ports for the admin server which was installed with the Primary server. The HTTP and HTTPS port was set when installing the primary server. The default HTTP port is 8080 and the HTTPS port value is 8090. You may have provided different port numbers for the admin server at the time the Primary Server was installed.
9. Enter the ports to use for the secondary 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. You will need to know which port you use for HTTPS when you install the agents. Click **Next**.
10. 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. If you specify the maximum memory to be larger than your server OS is configured to handle, the service will fail to start.
11. 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.
12. The installation will take a few minutes to complete. A screen will indicate the installation progress. Click **Done** when the Install Complete screen appears.

13. After the installation of a secondary server is finished, open a DOS window and navigate into the *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole* directory. Then run the *setServer.cmd* command from the command line. You will need to enter the password for the Admin Server console (This password was set for the weblogic admin user when installing the Primary Server). You will also need to enter the key phrase you chose for the two certificate keystores that this secondary server uses to store SSL certificates. After responding to the prompts, this secondary server will be merged into the existing domain that was created when installing the Primary Server.

    The installation will create a new Windows service called *Oracle Config Change Console X* where *X* will be replaced with the name you gave to the secondary server installation (for example: *SecondaryServer1*). You can go to the Services Control Panel to start this secondary server after you have finished all other components and followed the steps under Section 5.4.4, "Post Installation Steps for Cluster Installation".

5.4.3 Installing a Messaging Broker Server

Follow these steps to install the messaging broker server. You can install multiple standalone brokers on the same physical host and they can be on the same host as other cluster components.

1. Double-click on the **server-win32.exe** file from the Configuration Change Console media. The Installer will take a few moments to initialize. Ensure that the same directory from where you are running this installation also has the file *server-win32.part2* as this file is also required for installation. The installer will not proceed if this file is missing.
2. Click **Next** when the *Introduction* screen appears.
3. Specify the installation directory or choose the default. Click **Next**.
4. Choose the type of installation being performed. In this case you would choose **Clustered**, then click **Next**.
5. Choose server type as **Messaging Broker**, then click **Next**.
6. Specify the name of the messaging broker instance. The name should be of the format *MessagingBrokerX* where you replace *X* with the broker number starting from 1. For instance, the first standalone broker server would be called *MessagingBroker1*.
7. 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**.
8. Enter the hostname and ports for the admin server which was installed with the Primary server. The HTTP and HTTPS port was set when installing the primary server. The default HTTP port is 8080 and HTTPS port value is 8090. You may have provided different port numbers for the admin server at the time the Primary Server was installed.
9. Enter the ports to use for this messaging broker server. There are two ports configured here; HTTP and HTTPS. HTTPS is used for agents to communicate with this messaging broker server. You will need to know the port you use for HTTPS when you install the agents. Click **Next**.
10. Specify the minimum and maximum amount of memory allocated to the Configuration Change Console Messaging Broker 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. If you specify the maximum memory to be larger than your server OS is configured to handle, the service will fail to start.

11. 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.
12. The installation will take a few minutes to complete. A screen will indicate the installation progress. Click **Done** when the *Install Complete* screen appears.
13. After the installation of a secondary server is finished, open a DOS window and navigate to the *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole* directory. Then run the *setServer.cmd* command from the command line. You will need to enter the password for the Admin Server console (This password was set for the weblogic admin user when installing the Primary Server). You will also need to enter the key phrase you chose for the two certificate keystores that this secondary server uses to store SSL certificates. After responding to the prompts, this secondary server will be merged into the existing domain that was created when installing the Primary Server.

    The installation will create a new Windows service called *Oracle Config Change Console X* where *X* will be replaced with the name you gave to the messaging broker server installation (for example: *MessagingBroker1*). You can go to the Services Control Panel to start this secondary server after you have finished all other components and followed the steps under Section 5.4.4, "Post Installation Steps for Cluster Installation".

5.4.4 Post Installation Steps for Cluster Installation

The following steps must be performed after installing all of the components of the cluster. If you add another member to the cluster at a later time, these steps must be performed for the new member as well.

5.4.4.1 Exporting And Importing the SSL Certificates Into Servers

Because all Configuration Change Console Servers communicate over an SSL channel, SSL needs to be configured before starting a secondary server or messaging broker. Follow the steps below to export or import the certificates into servers. If keytool is not in your path, then use the full path name to access the tool that was installed along with the server (for example: *C:\oracle\ConfigurationChangeConsoleServer\bea\jrockit_160_05\bin\keytool*):

1. Navigate to the *$USER_INSTALL_DIR$\bea\wls\server\lib* directory of the currently installed secondary server or messaging broker.
2. Execute either of the following two commands:

    keytool -export -file SecondaryServerX.cer -alias weblogic -keystore weblogicOCC.jks

keytool -export -file MessagingBrokerX.cer -alias weblogic -keystore weblogicOCC.jks

SecondaryServerX.cer or *MessagingBrokerX.cer* is the file name of cert of current server *SecondaryServerX* or *MessagingBrokerX* is the server name that you just installed.

3. Copy this cert file into the directory *$USER_INSTALL_DIR$\bea\wls\server\lib* of the Primary Server.
4. Navigate to the *$USER_INSTALL_DIR$\bea\wls\server\lib* directory of the primary server.
5. On the server on which the Primary Server is installed, execute either of the following two commands:

   keytool -import -alias SecondaryServerX -file SecondaryServerX.cer -keystore weblogicOCCTrust.jks

   keytool -import -alias MessagingBrokerX -file MessagingBrokerX.cer -keystore weblogicOCCTrust.jks

   SecondaryServerX or *MessagingBrokerX* will be used as the alias in the primary server's trust Keystore (*weblogicOCCTrust.jks*) file to uniquely identify it.
6. When prompted to enter the password, please input the password that you had chosen during the Primary Server installation for the *weblogicOCCTrust.jks* keystore file. At the prompt when choosing either the Yes or No option, choose **Yes**.

   This completes importing of the new secondary server or messaging broker into the primary server's trust key store files. You can remove the *.cer* files created for the purpose of importing and exporting.
7. Repeat the above steps for all Secondary servers and Messaging Broker Servers.
8. Copy the *weblogicOCCTrust.jks* file of Primary Server to all Secondary Servers or Messaging Brokers. You need to overwrite all the *weblogicOCCTrust.jks* files of those servers.

Note: Each time you install a new Secondary Server or JMS Broker, you must repeat these steps. Following that, you should restart all servers.

5.4.4.2 Copying the Required Files From Primary to the Secondary

Follow these steps to copy the required files from Primary to Secondary Servers.

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

8. Copy the file *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\servers\PrimaryServer\security\boot.properties* from the Primary Server to the directory *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\servers\{SecondaryServerX}\security* on the Secondary Server.

5.4.4.3 Copying the Required Files From Primary to the Messaging Broker

Follow these steps to copy the required files from Primary to Messaging Broker Servers:

1. Delete all the files in *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\security* of the Messaging Broker.

2. Copy all the files from *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\security* of Primary to the same directory on the Messaging Broker.

3. Copy the following file *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\fileRealm.properties* from the Primary Server to the same location on the Messaging Broker.

4. Delete all the files and sub-directories of *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\config* in the Messaging Broker.

5. Copy all files from *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\config* of the Primary Server into the same directory location on the Messaging Broker.

6. Copy the file *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\servers\PrimaryServer\security\boot.properties* from Primary Server to the directory *$USER_INSTALL_DIR$\bea\user_projects\domains\ConfigChangeConsole\servers\{MessagingBrokerX}\security* on the Messaging Broker.

5.4.5 Adjusting the Database Connection Sizes

The Configuration Change Console database must be tuned to work with the increased number of secondary servers and/or Messaging brokers.

The database pool configuration for the Weblogic cluster is set based on a single server, but the connection pool size applies to each Primary and Secondary server in the cluster. For example, if you set the JDBC connection pool size to 200 and have 1 primary server and 5 secondary servers, a total of 1200 JDBC connections will be available across the cluster.

The number of JDBC connections to specify in the database settings is based on several factors. One major factor is the number of Message Driven Beans (MDBs) configured

for the servers. An MDB is the processing unit that handles incoming messages from the Messaging Broker Servers.

With the out-of-box configuration, a non-clustered installation has less than 110. To support the MDBs, and other internal processing as well as user UI connections, the JDBC pool should be set to 200 connections for the non-clustered installation.

With the out-of-box configuration, each Primary and Secondary server has no more than 60 MDBs. For the clustered environment, the maximum consumed MDBs for each secondary must be multiplied by the number of Messaging Broker servers installed in the cluster since each secondary server will have MDBs that connect to each Messaging Broker. As an example, if you have a clustered environment with a Primary Server, 3 Secondaries and 4 Messaging brokers, each secondary server will have 60 x 4 = 240 MDBs. To support other internal processing as well as user UI connections, the JDBS pool size should be set to 300 connections for the clustered-installation. If you add another Messaging broker to the cluster, then at least 60 more connections should be added to the Weblogic JDBC pool size. This setting applies to each Primary and Secondary in the cluster.

Adding a Messaging broker can help for failover and handling high loads, but it also will result in more parallel executions into the database which requires your database to be scaled to handle the larger load.

The Weblogic JDBC pool size setting can be configured through the Weblogic administrative console or by editing the file *{install dir}/bea/user_projects/domains/ConfigChangeConsole/config/jdbc/OracleDS-jdbc.xml* and adjusting the max-capacity setting.

You will need to ensure that your database is properly sized to match the size of the Configuration Change Console cluster you need for your environment. The number of agents does not affect how many database connections are needed as only the Primary Server and Secondary servers will connect to the database.

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 CCC PrimaryServer* from the list to uninstall the primary server. If you are uninstalling a component in a cluster other than the primary server, each component will start with *Oracle Enterprise Manager CCC*.
3. Follow the prompts to uninstall all parts of the server.

6

Installing and Uninstalling the Configuration Change Console Server for Linux

This chapter discusses any variations from the instructions specified earlier on installing and uninstalling Configuration Change Console on Windows. All steps for Windows can be followed except for any differences specified here.

6.1 Environment Requirements

The Configuration Change Console Primary Server requires the X-Windows subsystem to be installed for graphics generation on the browser-based interface.

You must install the servers as the root user to ensure that the daemons are configured properly so that the Configuration Change Console server can start when the server starts up. If you install as a non-root user, the installation will work but the server will not be able to start as a daemon.

When running the servers, consider whether your environment blocks the ports you can access for your software based on the user the server will run as. For instance, if your OS is configured to not allow a regular user to run software to use port 80 and 443 and you want these ports to be used for the Configuration Change Console server, then the server must run as root.

6.1.1 Requirement For Servers With Low Activity

In order to generate random numbers that are not predictable, SSL security code relies upon *entropy* on a machine. Entropy is activity such as mouse movement, disk IO, or network traffic. If entropy is minimal or non-existent, then the random number generator will be slow and security operations may time out. This may disrupt activities such as booting a managed server into a domain using a secure admin channel. This issue generally occurs for a period after startup. Once sufficient entropy has been achieved on a JVM, the random number generator should be satisfied for the lifetime of the installation.

By default, the Configuration Change Console assumes that the server has low entropy, so a setting is enabled to use */dev/urandom* as a source of entropy for the Weblogic startup. This weakens the security between the cluster elements in production environments.

If you want to disable */dev/urandom* to ensure a more secure environment, edit the following files:

{install_directory}/bea/user_projects/domains/ConfigChangeConsole/adminwrapper.conf

{install_directory}/bea/user_projects/domains/ConfigChangeConsole/wrapper.conf

Comment out the entry in the log file that sets the *java.security.egd* setting. The following is an example. Note that the number 5 in this line might be different in your installation and should not be changed. The only action required to enable this workaround is to comment out this line:

#wrapper.java.additional.5=-Djava.security.egd=file:///dev/urandom

Turning off this setting will cause the Weblogic server for Configuration Change Console to take a very long time to start. It is also possible that the startup will fail to generate the proper content for SSL communication which will result in the cluster members not being able to communicate with each other.

The alternative to using the *java.security.egd* setting is to contact your operating system vendor to obtain a patch to ensure that a low entropy server will not block random number generation.

6.2 Installer Files

The installer for Linux is named depending on the architecture of the server you are installing on. For instance, *server-linux-x86-32bit.bin* is used to install on any 32 bit x86 hardware. Ensure that the file *server-linux-x86-32bit.part2* is in the same directory as the main installer. It will be required during installation. Both of these files must have the execute bit enabled for the installer to start.

To start installation in Linux, use either of the following:

./server-linux-x86-32bit.bin for graphical installer

./server-linux-x86-32bit.bin -i console for console based installer

6.3 Daemon Processes

The installation of any type of server will result in an init daemon to be configured. The daemon that is created will depend on the name of the server in a similar way as defined for the Windows installation above. You will find the daemon control script under */etc/init.d* directory after installation. You can start or stop each server the same way you would with any other daemon process using the following commands:

```
/etc/init.d/daemonname start
```

```
/etc/init.d/daeomonname stop
```

The value *daemonname* in this case will start with EMCCC and end with the name of the Configuration Change Console server component, for example *EMCCCAdminServer*, *EMCCCPrimaryServer*, *EMCCCSecondaryServer1*, and so on.

If you did not install the server as root, you must start the server manually from the command line. You can do this by opening a shell and changing your directory to the following:

$USER_INSTALL_DIR$/bea/user_projects/domains/ConfigChangeConsole

Run the executable according to the name of the server you installed:

Table 6–1 Server Commands According to Type of Server

Type	Command
For primary w/o clustering:	./PrimaryServer -c wrapper.conf

Table 6–1 (Cont.) Server Commands According to Type of Server

Type	Command
For primary w/clustering: (two services need to be started)	./PrimaryServer -c wrapper.conf ./AdminServer -c adminwrapper.conf
For Secondary:	./SecondaryServer1 -c wrapper.conf
For Messaging Broker:	./MessagingBroker1 -c wrapper.conf

For the last two, replace the name of the server you gave at installation as the executable in this command.

6.4 Uninstalling the Configuration Change Console on Linux

This section describes how to uninstall the Configuration Change Console Server for the Linux Operating System.

From the command prompt, go to the server uninstaller directory. For example:

```
cd /root/oracle/ConfigurationChangeConsoleServer/UninstallerData
```

Run the uninstaller, where *ServerName* is the name of the Configuration Change Console server component being uninstalled, for example, *PrimaryServer*, *SecondaryServer1*, and so on, by typing the following command:

```
./Uninstall_Oracle_Enterprise_Manager_Configuration_Change_
Console_ServerName
```

7

Overview of Configuration Change Console Agent

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

7.1 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.

7.2 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 Activity. Changes to structure, content, or database user login/logout activity in a database for Oracle and Microsoft SQL databases
- Windows Registry. Changes to registry keys or values
- Active Directory/LDAP Server. Changes to objects in an LDAP-compliant server or Microsoft Active Directory
- SNMP Traps. Collect configuration and alert data through SNMP trap mechanism. This capability can be used to monitor configuration changes of network hardware such as a firewall by configuring the firewall to send SNMP traps to Configuration Change Console when a configuration change occurs

7.3 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 Activity. Detects and records file create, delete, modify, and rename actions on content or attributes. It can also can detect reads of a file. For each file activity collected data points include complete file name, date/time of change, event type, and user id of the user account who performed the action. For most operating systems, additional configuration is required to capture user ID, as documented below.
- Process Activity. 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.
- Operating System User Activity. Detects and records user logon/logoff events. On some operating systems it can also detect SU activity and will record the originating user as well as the user into whom is being su-ed. For each user change event collected data points include user ID (account ID), event type, connection type, source host, and data/time of event.

7.4 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.

7.5 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.

7.6 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.

7.7 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.

8

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 non-clustered or clustered 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.

8.1 System Requirements for All Platforms

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

8.1.1 Hardware Requirements

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

Table 8–1

Operating System	Available Hard Drive Space	Total System Memory
Microsoft Windows (XP, 2000, 2003 and NT4.0)	150 MB	512 MB
Linux (Oracle Enterprise Linux 4, 5, Red Hat V3, V4, 7.3) x86 32 Bit and 64 Bit	150 MB	512 MB
HP-UX 11.23 PA-RISC and Itanium 64-bit	250 MB	512 MB
IBM AIX 5.3	250 MB	512 MB
Sun Solaris 8, 9, 10	250 MB	512 MB
OS/400 V5R4	250 MB	512 MB

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

8.2 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 Primary and Messaging Broker Servers' IP and HTTPS ports. 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(s).
- Administrator role account on Primary 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.

9

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.

9.1 Special Instructions for Windows NT 4.0 or Missing WMI

This section discusses information about the Windows NT 4.0 agent installation. Follow the steps here before installing the agent as described later in this chapter. This section is also applicable if you are using a newer version of Windows but have removed the WMI (Windows Management Instrumentation) from the server.

> **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.

9.1.1 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.

9.1.2 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.

9.1.2.1 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

9.1.2.2 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

9.1.2.3 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.

9.1.2.4 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.

9.2 Windows XP, 2000, 2003 Agent Installation

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

9.2.1 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.

9.2.2 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 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*, for example, where you put host name and port for each Primary and Messaging Broker server. 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) and password for the Configuration Change Console Server. This is used to verify that the person installing the agent is authorized to do so. This username/password combination are only used at agent install time and the user can either be disabled or have the password changed after agent install without any issues.
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.

9.2.3 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**.

9.2.4 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**. You can also choose specific users if you are only monitoring for changes by specific users in Configuration Change Console rules. The rules will filter the results by user as well, so even if you enable audit for everyone, only users that you want to monitor changes of in Configuration Change Console will be captured
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. If you extend the monitoring time for file events because you expect the change rate to be lower, you need to ensure that the audit log in Windows is large enough to capture the events.
15. Click **Apply** and **OK** to exit.

9.2.5 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.

9.3 Windows NT 4.0 Agent Installation

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

9.3.1 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.

9.3.2 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 9.2.2, "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.

9.3.3 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**

9.3.4 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.

9.4 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 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.

9.6 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

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.

10.1 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.

10.1.1 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-linux-32bit.bin`

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-windows 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. If you are using a clustered environment, use *t3s://hostname1:port1,hostname2:port2,hostname3:port3*, for example, where you put host name and port for each Messaging Broker server. 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 username (the default is administrator) and password for the Configuration Change Console Server. This is used to verify that the person installing the agent is authorized to do so. This username/password combination is only used at agent install time and the user can either be disabled or have the password changed after agent install without any issues.
9. Next, you will be asked whether your server has auditing features enabled or not. The auditing requirements are different for each operating system. For Linux it means that you have the required kernel files available so that the kernel module can be compiled. For Solaris, it means you have the Solaris BSM installed and configured for the agent's use. If you choose no for this question, you will not be monitoring file changes in real time, but will be using the polling file monitoring capability. It is recommended that you read the requirements for each specific operating system to enable the appropriate auditing settings and then answer yes to this question when installing the agent.
10. The *Summary* screen will display. Verify that the install folder is correct and then click **Install** to proceed with the installation.
11. Click **Done** when the Installation Complete screen appears to exit the installer.

10.1.2 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.

For each Unix operating system the service is set to start up with the operating system if the agent was installed. You can find the startup and kill script links under the appropriate *rcX.d* directory. There is no manual maintenance needed on these unless you want to change the startup/shutdown behavior at operating system startup/shutdown time.

10.1.3 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
```

10.1.4 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 privileges 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*.

10.1.5 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 shell window

2. Change your directory to *{agent_install_dir}/bin*
3. Run the script: *resetauth.sh*
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.

10.1.6 Log Files

The product logs are located in the agent installation directory under the logs directory. For example, */root/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

10.2 Linux Agent Installation

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

10.2.1 Linux Agent Installation Prerequisites

Before installing the Linux Agent you must have the Kernel Development package installed for the exact same kernel version of Linux. You can check this by first performing a *uname -a* and recording the kernel version (such as *2.4.21-37.0.0.4.ELhugemem*). Next, look at the RPM registry to make sure the kernel-level package for this specific version is installed. It is very important that the development package version matches the version number exactly. Failure to match the version will cause the compiled kernel module to fail when trying to insert the module into the kernel.

You must also ensure that the version of gcc being used matches that with which the kernel was built. You can look at */proc/version* to see what gcc version the kernel was built with and then run *gcc -version* to see what version of gcc is being used. These two versions should match.

For agent operation, the file */boot/System.map-{version}* must also exist where {version} must match the kernel version you see when you run the *uname -a* command. This file contains system symbols that are needed to decode the kernel symbols we are monitoring for real-time changes. Without this file, real-time file monitoring will not function. This file is standard on all default Linux installations.

When the Linux agent is installed, a script will run to check for all of these dependencies and will inform you if there are missing requirements. The installation will continue to work, but the real-time file monitoring will not function until the module is built manually. The instructions for recovering from this is detailed below in the section "Kernel Module Compilation Issues".

If you make changes in the future to the version of the Linux kernel version, you should recompile the loadable kernel module to ensure it always matches the version of your server kernel. Instructions on how to recompile the module are in the section "Kernel Module Compilation Issues" below.

10.2.2 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 CDROM drive. Mount the disk.
3. At the prompt, copy the *agent-linux-x86-32bit.bin* file or *agent-linux-x86-64bit.bin* from the CD to the */tmp* directory depending on which type of processor your server has.
4. Start the installer by entering either of the following commands depending on the processor type your server has at the prompt:

   ```
   /tmp/agent-linux-x86-32bit.bin -i console
   ```

   ```
   /tmp/agent-linux-x86-64bit.bin -i console
   ```

   If you want to launch the graphical installer under X-Windows, leave off the -i console part of the command.
5. 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 indicating whether this succeeded or not. If there is a failure, or you find that there is an error in *logs/FileRunning.log* indicating that the real time file monitoring module cannot start, see the section Kernel Module Compilation Issues.
6. After installation, delete the installation files in the *tmp* directory with the command:

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

10.2.3 Kernel Module Compilation Issues

There are three ways that may indicate that there was a problem in loading the Linux kernel module. At installation time of the Linux agent, you may have received an error message towards the end of installation that compilation of the kernel module failed.

Alternatively, you may have noticed that you do not receive real-time file changes on the Configuration Change Console Server UI for file changes that you know should occur.

Finally, when examining the FileRunning.log file under {agent install directory}/logs, you may see errors indicating that the kernel module could not be loaded or used for various reasons.

If you encounter any of these issues, then most likely there was a problem with compiling or inserting the Linux kernel module at run time.

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* and *build.log* file under *{agent install directory}/logs* to see if there are any errors that might be resolvable
4. If there are no errors when executing *compmod.sh*, check the bin directory and see if a file *auditmodule*.ko* was created after execution of *compmod.sh*. If there is, you can attempt to manually load the module to see if there are any errors. Use the following command where you replace *{audit module file name}* with the entire name of the *.ko* file that was created from *compmod.sh*:

   ```
   insmod {audit module file name}
   ```

   If you have no errors during this, you can check the module list again by using the grep command above. If the audit module now appears, then the file monitoring capability should work once you restart the agent.

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 the following information with your support ticket:

Output of the command: *uname -a*

Output of the command: *grep –i /proc/modules*

Output of the command: *rpm –q –a |grep –i kernel-devel*

The *make.log* and *build.log* files from the *{agent install dir}/logs directory*

The file *{agent install dir}/logs/FileRunning.log*

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

If you patch the kernel of your OS, you need to recompile the auditmodule kernel module using the steps outlined earlier to match the new kernel version. You will also need to install the kernel-devel package that matches the same version as the patched kernel

10.3 Solaris Agent Installation

Use the following steps to install the Solaris agent:

1. Log in to the Solaris server as the root user.
2. From the Configuration Change Console Installation media, copy the *agent-solaris-sparc.bin* file to the */tmp* directory and make sure the installer is executable by typing:

   ```
   chmod +x agent-solaris-sparc.bin
   ```

3. For the remainder of the installation instructions, refer to the UNIX Agent Installation: Console Mode section, starting with Step 2.

10.3.1 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`

10.3.2 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.

10.3.3 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.

10.3.4 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.

10.3.5 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.

10.3.6 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.

10.4 HP-UX 11.23 Agent Installation

This section describes the procedure for installing the agent on an HP-UX server. The Configuration Change Console Agent supports HP-UX 11.23 on the 32-bit or 64-bit PA-RISC and IA64 processor. Please read the prerequisites carefully to obtain the necessary software and patches before you begin the installation. Instructions for using the HPUX 32-bit PA-RISC agent on HPUX 11.11 are in the next section.

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.x, 3.x and 4.x. We recommend you to install the latest 4.x version.

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

10.4.1 Prerequisites

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

Table 10–1 Hardware Prerequisites

Operating System	HPUX 11i v2
CPU	At least a PA RISC 1.1

10.4.1.1 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

Table 10–2 HIDS Patches

Operating System	HP-UX 11i v2
Patch	PHKL_34798 s700_800 11.23 HIDS cumulative patch

10.4.2 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.

10.4.2.1 HIDS Preinstallation

The HIDS application must be installed before the agent is installed. The HIDS 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 application is as follows:

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

Refer to the HIDS documentation, Host Intrusion System from HP.com for installation and configuration instructions for your HP-UX version.

10.4.3 HP-UX 11i 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_34798 s700_800 11.23 HIDS cumulative patch (for HPUX 11i v2)

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`

10.4.4 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
```

10.4.5 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

.

10.4.6 Installing the Agent

Refer to the UNIX Agent Installation section earlier in this chapter for installation instructions.

To start and stop the service, run the following commands from the command line. For HPUX, the */etc/init.d* folder is not used as described in the general Unix section above.

```
/usr/sbin/arprobe start

/usr/sbin/arprobe stop
```

10.5 AIX Agent Installation

The following section describes the installation process for installing AIX agents. The current agent only supports AIX5.3 since the Java JVM1.5 is not available for earlier versions of AIX.

10.5.1 Installation Prerequisites

To improve system performance, install the AIX 5.3 5300-08 Service Pack 5 or higher before installing the AIX 5.3 agent. The maintenance package is available from the IBM.

10.5.2 Installing the Agent

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

To start and stop the service, run the following commands from the command line. For AIX, the */etc/init.d* folder is not used as described in the general Unix section above.

```
/usr/sbin/arprobe start

/usr/sbin/arprobe stop
```

10.5.3 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 exit 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"
```

10.6 HP-UX 11.11 Agent Installation

This section describes the procedure for installing the agent on an HP-UX 11.11 server on the 32-bit or 64-bit PA-RISC processor. 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.x, 3.x and 4.x. Oracle recommends you to install the latest 4.x version.

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

10.6.1 Prerequisites

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

10.6.1.1 HIDS Patches

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

10.6.2 HIDS Overview

HIDS auditing features work 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.

10.6.2.1 HIDS Preinstallation

The HIDS application must be installed before the agent is installed. The HIDS 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 application is as follows:

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

Refer to the HIDS documentation, Host Intrusion System from HP.com for installation and configuration instructions for your HP-UX version.

Table 10–3 Hardware Prerequisites

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

Table 10–4 HIDS Patches

Type	Value
Operating System	HP-UX 11i v1
Patch	PHSS_26560

Table 10–5 HP Java Runtime Patches

Patch	Description
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.

Table 10–5 (Cont.) HP Java Runtime Patches

Patch	Description
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 that causes hangs. This patch MUST be installed for JRE version 1.3.1.11 or later.
PHSS_30049	Solves problem with dld while loading native libraries for class ServerSocket.

Table 10–6 HIDS Patches

Operating System	HP-UX 11iv1
Patch	PHKL_26074
	s700_800 11.11 libaudit.a cumulative patch

10.6.3 HP-UX 11i, 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`

10.6.4 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
```

10.6.5 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* file 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:

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

10.6.6 Installing the Agent

Refer to the UNIX Agent Installation section earlier in this chapter for installation instructions.

To start and stop the service, run the following commands from the command line. For HPUX, the */etc/init.d* folder is not used as described in the general Unix section above.

```
/usr/sbin/arprobe start
```

```
/usr/sbin/arprobe stop
```

11

Installing the Agent on OS/400

This section outlines the steps you need to follow to install the agent on the OS/400 operating system. This release currently supports version V5R4 and above. This installation process is quite different than for other operating systems, so be sure to follow the steps closely.

11.1 Agent Capabilities

The majority of capabilities of the Configuration Change Console will work on the OS/400. There are some limitations however.

Like other operating systems, the agent supports

- File creation, modifications, renames and deletes
- Process starts and stops
- User logins and logouts
- Current system resources and configurations
- Changes to OS/400 system values

There are some limitations to the OS/400 agent:

- The source machine IP for user logins cannot be captured
- Directory delete actions cannot be captured

11.2 Prerequisites

Since the agent will create a new user profile, it must be run by a user with "Security Officer" authority.

11.2.1 Java Requirements

The Configuration Change Console agent requires that you install JDK version 1.5 on your OS/400 server. In addition, the Java Group PTF SD99291 must also be installed. Make sure that IBM Toolbox for Java (5722-JC1) and IBM Developer Kit for Java (5722-JV1) and Java Developer Kit 5.0 (5722-JV1) are installed.

11.2.2 Installing the Java Group PTF SF99291

For detailed installation instructions, follow the instructions included in the PTF.

Obtain and install the Java Group PTF SF99291 by performing the following steps:

1. From the command line on your OS/400 system, type `GO PTF`

2. From the screen, select option 8
3. Specify PTF type 1 (for all PTFs) and automatic IPL Y

Verify that the proper version of the Java Group PTF has been installed by executing the following command:

```
WRKPTFGRP SF99291
```

The output should be below.

```
Opt    PTF Group           Level         Status
       SF99291              18           Installed
```

After Java Group PTF SF99291 installed, please edit the java.security file under the */QIBM/ProdData/Java400/jdk15/lib/security* directory. You will see the following content:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL
security.provider.7=com.ibm.i5os.jsse.JSSEProvider

#
# List of Sun providers and their preference orders (see above):
#
#security.provider.1=sun.security.provider.Sun
#security.provider.2=sun.security.rsa.SunRsaSign
#security.provider.3=com.sun.net.ssl.internal.ssl.Provider
#security.provider.4=com.sun.crypto.provider.SunJCE
#security.provider.5=sun.security.jgss.SunProvider
#security.provider.6=com.sun.security.sasl.Provider
```

Comment out the first block of security providers for IBM and uncomment the providers from Sun. After you make the changes, your file should look like the following:

```
#security.provider.1=sun.security.provider.Sun
#security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
#security.provider.3=com.ibm.crypto.provider.IBMJCE
#security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
#security.provider.5=com.ibm.security.cert.IBMCertPath
#security.provider.6=com.ibm.security.sasl.IBMSASL
#security.provider.7=com.ibm.i5os.jsse.JSSEProvider

#
# List of Sun providers and their preference orders (see above):
#
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
```

11.3 OS/400 Agent Installation

The following steps outline how to install the agent on OS/400. If any errors occur during these installation steps, refer to the section below on how to solve the most common installation errors.

1. Mount the Oracle Configuration Change Console Media on the OS/400 server you want to install the agent on. The two files that you need from the media are:
   - *Agent-os400/Installprobe.sh*
   - *Agent-os400/Installprobe.jar*
2. Log into the OS400 server with a user account with elevated security permissions
3. Start QShell by typing `QSH`
4. Change the working directory to the directory where the two install files are located. If you install from the CD, it will typically be mounted under */QOPT*.
5. Run the script *installprobe.sh*. The script will output the following usage parameters needed.

   ```
   Usage: <JNDI_PROVIDER_URL> <INSTALL_LIB> <INSTALL_DIR> <USER_ADMIN> <USER_
   NORMAL>

   JNDI_PROVIDER_URL : (Required) Enter the server connection URL. For
   NON-CLUSTERED, you can enter t3s://host:sslPort. For CLUSTERED, you can enter
   t3s://host1:sslPort1,host2:sslPort2

   INSTALL_LIB : (Optional) The library to contain probe. Default value is
   $DEFAULT_INSTALL_LIB

   INSTALL_DIR : (Optional) The directory to contain probe. Default value is
   $DEFAULT_INSTALL_DIR

   Notes: you can type '-' to use the default value
   ```

6. Run the script installprobe.sh with the proper parameters. For example:

   ```
   ./installprobe.sh t3s://host1:port1 Agent - - -
   ```

   Where you replace host1 with the hostname or IP of your primary server and port1 with the ssl port (443 by default). If you have a clustered server instance, you change the second parameter to list the primary server and all of the messaging broker servers like this example where there is one primary server and two additional messaging broker servers:

   ```
   ./installprobe.sh t3s://host1:port1,host2:port2,host3:port3 Agent - - -
   ```

   Running this command will place the agent in the library named Agent in the */arprobe* directory.

   This install script might show some warning messages if the library, directory or users being created already exist.

7. When you see the following prompt, type "y" and **Enter** to start the agent installation. Press any other key if you want to abort the installation at this point.

   ```
   Do you want to install the Configuration Change Console Agent?
   (y - install, any other key to exit)
   ```

8. After the installation is finished, change the directory to the {agent install dir}/bin directory. Run the following script to set the user and password on the

Configuration Change Console Server that you can authenticate this agent with. The user must have the administrator or super-administrator product role.

```
./resetauth.sh
```

11.4 Post Installation Tasks

The following sections describe the required post installation tasks for the OS/400 Agent installation.

11.4.1 Verify Object Auditing for QAUDCTL

Follow these steps:

1. From the main menu screen in OS/400, type the following command and press **Enter**.

   ```
   wrksysval sysval(qaudctl)
   ```

2. From the Work With System Values screen, selection Option 2- Change and press **Enter**.
3. Verify that the following items are included under Auditing Control. If they are not there, enter them manually.

*AUDLVL
*NOQTEMP
*OBJAUD

Note: The QSYS/QAUDJRN journal must exist before you can change the QAUDCTL system value to a value other than *NONE.

11.4.2 Verify Object Auditing for QAUDLVL

Follow these steps:

1. From the main menu screen in OS/400, type the following command and press enter.

   ```
   wrksysval sysval(qaudlvl)
   ```

2. From the Work With System Values screen, selection Option 2- Change and press **Enter**.
3. Verify that the following items are included under Auditing Control. If they are not there, enter them manually.

*CREATE
*DELETE
*SAVRST
*OBJMGT
*SECURITY
*JOBDTA

11.5 Starting and Stopping the Agent

During the agent installation, a subsystem description is created with the same name as the library. The installation process also creates an autostart job entry in the

subsystem. Therefore, to start the agent service, simply start the subsystem; to stop the agent service, end the subsystem.

For example, if the agent was installed in library AGENT, start the service by entering the following at the command prompt and pressing **Enter**:

```
strsbs agent/agent
```

To end the service, type the following at the command prompt and press Enter:

```
endsbs agent *immed
```

11.6 Shutdown/Restart Procedures

To stop the agent during system operations, add the stop command (in the example above, *endsbs agent *immed*) to your shutdown procedures to automatically end the agent with a system shutdown. You may also add the start command to your restart procedures to automatically restart the agent at system restart.

You may also want to add it to the QSTRUP program, so that it starts during the IPL process.

11.7 Uninstalling the Agent

To manually uninstall the agent (assuming the library is called AGENT), follow these steps:

1. Stop the agent by typing the following command in a command prompt and pressing Enter:

   ```
   endsbs agent *immed
   ```

2. Delete the library by typing the following command and prompt and pressing Enter:

   ```
   dltlib agent
   ```

3. Start the qshell by typing the following at the command prompt and pressing **Enter**:

   ```
   qsh
   ```

4. Type the following at the command prompt to delete the agent directory where */targetdir* is the path to the directory where the agent was installed. For example: */ArProbe*:

   ```
   rm –rf /targetdir
   ```

   Note: The rm (remove) command is finished when the qshell session displays a $ character beneath the rm command entry. If you exit the qshell (by pressing F3) prior to the display of the $ character, the rm command will not complete. Wait for the display of the $ character before exiting qshell. Processing of the rm command may take several minutes on your system.

Alternatively, the agent can be uninstalled entirely through a qshell on the AS/400 device where the agent is installed.

1. Start the qshell by typing the following at the command prompt and pressing **Enter**:

```
qsh
```

2. At the command prompt, change directory to the agent installation directory. For example where *arprobe* is the directory of your agent installation:

   ```
   cd /arprobe
   ```

3. Uninstall the agent by typing the following at the command prompt and pressing **Enter**:

   ```
   uninstall.sh
   ```

11.8 Collecting Information Related to Installation Errors

This section details how to print out a job log for any errors encountered during the OS/400 agent installation. An example of an Unsuccessful Installation error message is:

UNSUCCESSFUL INSTALL OF ORACLE CONFIGURATION CHANGE CONSOLE

Follow these steps:

1. Immediately following the receipt of an error message, display the current jobs by typing *DSPJOB* at the command prompt and pressing **F4**.
2. Write down the job, user and number information displayed for the error.
3. At the prompt, enter the following command and press **Enter**.

   ```
   SIGNOFF *LIST
   ```

4. Log back into the OS/400 interface and at the prompt type `WRKJOB` and press F4.
5. On the resulting screen, enter the Job, User, and Number from step 2. Under the option field, input `*SELECT` and press **Enter**.
6. Select option 4. Work with spooled files by entering the number 4 at the prompt. Press **Enter**.
7. Locate QPJOBLOG in the list of spooled files and enter a 2 in the Opt column for the row containing file QPJOBLOG. Press **Enter**.
8. On the resulting screen, specify the network name of your printer in the Printer field and press **Enter**.
9. Sign off and keep the printed log for reference when filing a ticket with Oracle.

12

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.

12.1 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:

- The agent installer. The executable that installs the agent. The actual executable file will be specific to the platform. For example, for a Windows platform, the agent executable will be *agent-win32.exe*; on a 32-bit Linux system, the agent executable will be *agent-linux-x86-32bit.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-win32.exe* executable, the respective *.properties* file should be *agent-win32.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.

12.2 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-win32.exe*, create a properties file with the name *agent-win32.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 12–1 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_PROVIDER_URL	JNDI_PROVIDER_URL is the connection URL for the agent to connect to the messaging broker servers. If you have a nonclustered environment, the value for this field will be of the format t3s://host:port where host is the hostname or IP of the primary server and port is the secure port of the primary server (443 by default). If you have a clustered environment, the value will be like: *t3s://host1:port1,host2:port2,host3:port3* where ach host/port combination is for one of the messaging broker servers
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.

Table 12–1 (Cont.) agent.properties Field Values

Field	Description
AUTHENTICATE_USER	The user name on the server to use for authenticating this agent install.
AUTHENTICATE_PW	The password for the user used for authentication. Note: Since 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-win32.exe* for Windows based platforms.

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

12.2.1 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.

12.3 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.

13

Post Installation Tasks

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

13.1 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.

13.1.1 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.

13.2 Adding Additional Messaging Brokers in a Clustered Environment

If you have previously set up a clustered environment with some number of messaging brokers, you already configured your agents Messaging Broker URL to include the host and SSL port for each broker similar to the following:

t3s://host1:443,host2:443,host3:443…

If you want to add another broker to your cluster, you must first go to each agent and manually modify the {*agent_intsall_dir}/config/probe.properties* file to add the new broker to the field *java.naming.provider.url* before you actually add the new broker to the cluster.

If you add the new broker first, the agent will become aware of the new broker through the cluster, but will not have retrieved that broker's security certificate to be able to communicate with it. This will mean that the broker will not be able to take messages from any agents without being uninstalled and reinstalled again. The agent needs to know of the Messaging Broker server before the server is available.

13.3 Changing the Ports Of the Configuration Change Console Servers

Use the following sections to learn more about changing the ports of the configuration change console servers.

13.3.1 Reconfiguring the Server

The ports for the Configuration Change Console server were set at installation time. If you would like to change the ports after installation, you can edit the Oracle Weblogic config.xml file. This file is located on the Primary Server in the following location:

$USER_INSTALL_DIR$/bea/user_projects/domains/ConfigChangeConsole/config/config.xml

In this XML file, you will see server configuration for all servers. If this server belongs to a cluster, you will also see the server configuration for all other cluster members. The XML tag *<listen-port>* defines the port on which the server is listening to request. There are two for each server installation: one for non-ssl and one for SSL. The following is a sample fragment for a Primary Server installation:

```
<server>
 <name>PrimaryServer</name>
 <max-http-message-size>-1</max-http-message-size>
   <ssl>
     <enabled>true</enabled>
     <listen-port>443</listen-port>
     (…. Additional content removed …. )
   </ssl>
```

```
    <listen-port>80</listen-port>
    <listen-port-enabled>true</listen-port-enabled>
      (…. Additional content removed …. )

</server>
```

The port 443 in the example above is the SSL port that is used for HTTPS access to the web-based interface and also for cluster communication. The port 80 is the non-secure HTTP port.

On a non-clustered environment, you can simply save this *config.xml* file and restart the Primary Server for the change to take affect. You must also make sure your agents are reconfigured as explained below.

In a clustered environment, once you save the changes to config.xml, you must copy this config.xml file to the same directory path for all other members of your cluster. All config.xml files in all cluster members should be the same. Then you can restart each cluster server to see the changes take effect. You must also make sure your agents are reconfigured as explained below.

13.3.2 Reconfiguring the Agent Ports

When you change the port the servers are using, the agents may also have to be changed to point to the new ports.

For a non-clustered environment, changing the Primary Server's SSL/HTTPS port will require a change to be made on the agent.

For a clustered environment, only a change to the SSL/HTTPS port of a Messaging Broker server will require the change to be made on the agent.

To make the required change on the agents, edit the file *{agent_install_dir}/config/probe.properties* and find the entry *java.naming.provider.url*. For each host, ensure that the port matches the desired ports now configured on the servers.

14

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.

14.1 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.

14.2 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.

15

Installing and Configuring BI Publisher Reports

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

15.1 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

15.1.1 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.

15.1.2 Preparing for Installation

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

15.2 Installing BI Publisher Server 10.1.3.4.1

This section details all steps involved in installing the BI Publisher Server. For more detailed information covering the individual components of the BI Publisher Server, please see the BI Publisher Installation Documentation. The Configuration Change Console integration is specifically for version 10.1.3.4.1 of BI Publisher.

Follow these steps to install the BI Publisher Server:

1. Insert Oracle Business Intelligence Publisher Enterprise Version 10.1.3.4.1 CD into the server.
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.

15.3 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.

15.3.1 Pre-Configuration for BI Publisher Report Publication

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

15.3.1.1 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.

15.3.1.2 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'.

15.3.1.3 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.

15.3.2 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.

15.3.3 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_v11?wsdl

4. Click **Save**.

15.3.4 Using BI Publisher With Other Locales

When you want to publish BI Publisher reports in other languages that use special fonts such as Chinese or Japanese, you need to ensure that the BI Publisher Java Runtime Environment has the proper fonts available. If you do not deploy the proper fonts, you may see '?' symbols instead of real content.

The *integrated-install.zip* that contained the BI reports also contains a zip file under *nls-fonts/nls-fonts.zip* that has the required font files. To deploy these fonts to your BI Publisher JRE, unzip this file and place the *.ttf files into the following directory:

{BI Publisher install folder}\jdk\jre\lib\fonts

After restarting your BI publisher server, you should now be able to generate reports for languages requiring these fonts.

16

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*.

16.1 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

16.1.1 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 related 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.

16.1.1.1 Verify the Form Changes

You can verify the form changes were 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, *CCC-DetectChanges*, and *CCC-Assigned Category List*.

16.1.2 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.

16.1.2.1 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 *CCC-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.

16.1.2.2 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.

16.2 Remedy ARS 7.0 Integration

The integration instructions for Remedy Action Request System (ARS) 7.0 here assume that the following components have already been installed on a server:

- Remedy ARS 7.0.01
- Remedy Approval Server 7.0.1
- Remedy Assignment Engine 7.01
- BMC Attrium CMDB 2.0.01 (required by Change Management Server)
- Remedy Change Management Server 7.0.03
- Remedy User client
- Remedy Admin client

16.2.1 Customizing Remedy Installation

Part of the integration effort is to load a custom definition file for the Configuration Change Console. This definition file adds form templates to help in customizing your Remedy instance and also adds 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/ARS7.0/definition files*. Inside this directory is the *Remedy70-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 on which your Remedy ARS server is installed
4. Go to the Tools Menu and select **Import Definitions > From Definition File…**
5. Select the definition file *Remedy70-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. Complete the rest of the steps in all sections of this chapter.

16.2.1.1 Customization Tasks to Perform on CHG: Infrastructure Change Form

Follow these steps to customize tasks to perform on the CHG: Infrastructure Change form.

1. Using the Remedy Administrator Client, open the Change Request form, *CHG:Infrastructure Change*
2. At the same time, open the Change Request template form, *CHG:Infra ChangeTmpl*, for lookup purpose only. Do not make changes to this form and do not save this form. The following instructions will direct you to copy fields from the template to the real form.
3. On the *CHG:Infrastructure Change* form, create two new 'pages' on the page field *pagChange*. You will create two new tabs:
   - The first tab will store the changes that have been detected for a ticket and should have a label of *CCCEvents*. The name of the page should be *tabActiveR-Det-Chg*. The page name is referenced by workflow and the product, so it must match exactly whereas the label can be customized.

- The second tab stores possible CTIs that are affected for a given changes. This tab should have a label of *CCCRelatedCTIs* and a page name of *tabActiveR-AsgnCatLst*. The page name is referenced by workflow and the product, so it must match exactly whereas the label can be customized.

Use the form *CHG:Infra ChangeTmpl* as the lookup for identifying the tab field properties for these tabs. Match all field properties on these two new tabs on *CHG:Infrastructure Change* to the corresponding properties on *CHG:Infra ChangeTmpl*. Make sure that the Database Field IDs are the same.

4. Save the *CHG:Infrastructure* Change form.
5. Now copy the fields on each of the tabs (one tab at a time) from *CHG:Infra ChangeTmpl* to *CHG:Infrastructure Change* form. Multiple fields can be copied at the same time by using 'Shift-Click'. Make sure that the Database Field IDs are the same. Only the following fields should be copied:
   - SubmittedByID
   - ModifiedByID
   - SupervisorID
   - CTI-ID
   - CCC-AssetID
   - CCC-IntgTagID
   - tblDetChg
   - tblChgCtiAssn
   - System Name
   - System Type
   - User List
   - Is Device Group Name
   - Stop Ticket Update
   - CCC Ticket Type
   - CCC-Consolidation Tag
6. Copy the field *Preventing a Problem* from *CHG:Infra ChangeTmpl* to *CHG:Infrastructure Change* form.
7. Resize, align and position all of the fields as necessary.
8. Change length of "Summary" to 255 chars (It is 150 by default, but summary of ticket expiry tickets are longer than 150 characters)
9. Save the *CHG:Infrastructure Change* form again.

16.2.1.2 Customization Tasks to Perform On CTM: People Form

Follow these steps to customize tasks to perform on the CTM: People form.

1. Using the Remedy Administrator Client, open the People form, *CTM:People*.
2. Open the People template form, *CTM:PeopleTmpl*, for lookup purpose only. Do not make changes to this form and do not save this form. The following instructions will direct you to copy fields from the template to the real form

3. Copy the fields in the box, *Custom Fields Used by Oracle* from CTM:PeopleTmpl to CTM:People. Multiple fields can be copied at the same time by using 'Shift-Click'. The following fields only should get copied:
   - Box
   - extAR1
   - CCC-SendPersonalInfo
   - CCC-GroupIDs
   - CCC-PersonInGrp
4. Save the form CTM:People

16.2.1.3 Customization Tasks to Perform on PCT:Product Catalog Form

Follow these steps to customize tasks to perform on PCT: Product Catalog form.

1. Using the Remedy Administrator Client, open the Categorization (CTI) form, *PCT:Product Catalog*.
2. Open the Categorization (CTI) template form, *PCT:CatalogTmpl* for lookup purpose only. Do not make changes to this form and do not save this form. The following instructions will direct you to copy fields from the template to the real form.
3. Copy the fields in the box, *Custom Fields Used by Oracle* from *PCT:CatalogTmpl* to *PCT:Product Catalog*. Multiple fields can be copied at the same time by using 'Shift-Click'. Only the following fields should get copied:
   - BoxAR1
   - txtAR1
   - SubmittedByID
   - ModifiedByID
4. Save the form *PCT:Product Catalog*

16.2.1.4 Import Workflow Definitions

Follow these steps to import workflow definitions:

1. Start the Remedy ARS Administrator client and connect to your remedy instance
2. Go to the Tools Menu, select *Import Definitions* > *From Definition File…*
3. Select the definition file **Remedy70-adapter-Generic.def** again.
4. Click on **Filters** to highlight it and click on the **Add** button
5. Click on **Active Links** to highlight it and click on the **Add** button. Do not import the "Forms" again as it will replace the work you did in the last few sections.
6. 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.
7. Click on the **Import** button to start the import.

16.2.1.5 Customize Configuration Change Console Administration Configuration

Follow these steps (do not include quotes when entering text) to customize the console:

1. Using the Remedy User Client, log in to your Remedy7 server.
2. From the Home page, click *Application Administration Console*
3. Create a new company *Oracle Enterprise Manager* with type *Operating Company*
4. Create new organization and location. These values can be set to whatever you would like to represent your organization.
5. Enter the following support Groups hierarchy
   - Support Organization: “IT Compliance”
   - Support Group Name: “IT Monitor”
   - Support Group Role: “Report”
6. Create people
   - Input required fields
   - Support Staff is "Yes"
   - Login id, such as "cccadmin". You can choose any name you want.
   - License Type: Fixed
   - Add Support Group relationship, such as "IT Compliance" to it
   - Add Support Group Functional Role, "Change> Infrastructure Change Manager" to it
7. View *cccadmin* from People Form, and set the field *CCC-SendPersonInfo* to “Yes” and save it.
8. Create Product Catalog for the following, setting the status to Enabled:
   - Unauthorized > Unauthorized > Unauthorized
   - Unauthorized > Unauthorized > Emergency
   - Unauthorized > Unauthorized > Ticket Expiry
9. Create Assignment
   - Events: “Infrastructure Change Manager”
   - Assigned Group: “IT Compliance” (This was created in step 5 above)
   - Company: “Global”
10. Find the “User” form from object list and search for the user *cccadmin*
11. Add more groups to the Permission Group list:

“Infrastructure Change Master”
“Config Categorization Admin”
“Config Group Mapping Admin”
“Contact Organization Admin”
“Contact Location Admin”
“Administrator”
“Asset Admin”
“Contact People Admin”
“Cost Manager”

12. Add the company created above in step 3, *Oracle Enterprise Manager* into the Access Restriction list.

16.2.2 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: *CCCEvents* and *CCCRelatedCTIs*.

16.3 Peregrine Service Center 6.1 Integration

The integration instructions for Peregrine Service Center 6.1 here assume that the Service Center product has already been installed on another server in your environment.

16.3.1 Customizing Service Center Installation

Part of the integration effort is to load a custom definitions file for the Configuration Change Console. This definition file adds custom fields needed by the agent to store Configuration Change Console detected events. It also includes additional workflow to send ticket updates, people updates and categorization updates to the Configuration Change Console Server.

It is recommended that you review the definition file prior to loading it into your Service Center 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 *Peregrine/Base/SC6.1/dictionary files*. Inside this directory are the *ServiceCenter61-adapter-Generic-Additions.unl* and *ServiceCenter61-adapter-Generic-Modifications.unl* files. These are the definition files that must be loaded for integration to work. Here are the steps to follow to load the definition file.

16.3.1.1 Step 1: Load Configuration Change Console Dictionary File

Follow these steps to load the Configuration Change Console Dictionary file:

1. Start the Peregrine Service Center 6.1 client and log in as a user that has permission to customize Peregrine such as the default falcon user.
2. Backup the following components that will be modified by loading the custom dictionary file.
   - Format: *cm3r.assess.default.g*
   - Format: *cm3r.plan.default.g*
   - Format Control: *cm3r.assess.default*
   - Format Control: *cm3r.plan.default*
   - DBDICT: *cm3r*
3. In the main navigation pane, scroll down to the Toolkit section and click the **Database Manager** icon.
4. The *Database Manager* window will display. Click the down arrow icon in the upper right hand corner. Select **Import/Load** from the resulting drop-down menu.

5. The *ServiceCenter File Load/Import* screen will display. Click the folder icon at the end of the **File Name** field.
6. In the Open window, navigate to the folder containing the *ServiceCenter61-adapter-Generic-Additions.unl* file. Select the file and click **Open**.
7. Select **winnt** from the file type drop-down menu.
8. Click on the Load FG button in the upper left hand corner to start the import. The load status will display at the top of the window. Once finished the file name and path will display as "loaded".
9. Repeat steps 4 through 8 to import the *ServiceCenter61-adapter-Generic-Modifications.unl* file.

16.3.1.2 Step 2: Enable External Web Services Access

In order to access Peregrine Service Center data through web services, the Configuration Change Console requires settings on certain external access records to be modified. Please follow these steps to ensure that the integration functions properly.

1. In the Peregrine Service Center client, return to the main navigation menu by clicking the **Back** icon in the upper left hand corner.
2. From the main navigation pane scroll down to the *Utilities* section and click the **Tools** icon.
3. Scroll down to the section titled *Web Services* and click the **External Access** icon. The *External Access Definition* screen will open.
4. You will be adding a number of services. For each definition 1 through 9 listed below:
   a. Enter the listed Name information in the **Name** field and press **Enter**.
   b. Verify that the **Service Name** and **Object Name** match those listed below.
   c. Click the **Add** icon, followed by the **OK** icon in the upper left-hand corner of the screen.

Definition 1
Name: ActiveR
Service Name: ActiveRWS
Object Name: ActiveR

Definition 2
Name: ActiveRAssignedCategoryListDetails
Service Name: ActiveRWS
Object Name: ARCategoryDetails

Definition 3
Name: ActiveRDetectedDetail
Service Name: ActiveRWS
ObjectName: ActiveRDetectedDetail

Definition 4
Name: cm3tcategory
ServiceName: ActiveRWS
ObjectName: cm3tcategory

Definition 5
Name: cm3tcategory

ServiceName: ActiveRWS
ObjectName: cm3tcategory

> **Note:** For this definition you will also need to click the **DataPolicy** tab, and enter false in the exclude column for the values in the list below:

Field NameExclude
company false
description false
name false
phases false

Definition 6
Name: cm3rsubcat
ServiceName: ActiveRWS
ObjectName: cm3rsubcat

> **Note:** For this definition you will also need to click the **DataPolicy** tab, and enter false in the exclude column for the values in the list below:

Field NameExclude
category false
company false
description false
subcategory false
sysmodcount false
sysmoduser false

Definition 7
Name: eventout
ServiceName: ActiveRWS
ObjectName: eventout

> **Note:** For this definition you will also need to click the **DataPolicy** tab, and enter false in the exclude column for the values in the list below:

Field NameExclude
evfields false
evnumber false
evsepchar false
evstatus false
evsysseq false
evtype false
evuser false

Definition 8
Name: operator
ServiceName: ActiveRWS

ObjectN: operator

> **Note:** For this definition you will also need to click the **DataPolicy** tab. For the corresponding Field names, enter **false** in the Exclude column. All other rows within the column should have true entered.

i.department
ii.Full.name
iii.name
iv.User.role

> **Note:** For this definition you will also need to click the **DataPolicy** tab, and enter false in the exclude column for the values in the list below:

Field Name Exclude
department false
full.name false
name false
user.role false

Definition 9
Note: This definition should already exist in a customer's Peregrine system.
Name: cm3r
ServiceName: ActiveRWS
ObjectName: Change

> **Note:** For this definition you will also need to click the **DataPolicy** tab, and enter false in the exclude column for the values in the list below:

Field Name Exclude
contact.first.name false
contact.last.name false
header,assign.dept false
header,coordinator false
header,planned.end false
header,planned.start false

5. For definitions 1,2,3,and 7, map the following allowed actions:
   - delete->delete
   - add->create
   - save->update
6. Once finished, click the **Back** button twice to return to the main navigation window.

16.3.1.3 Step 3: Database Dictionary Modifications

Use the following steps to modify the Database Dictionary:

1. In the Peregrine Service Center client, enter **dbdict** in the Command field, located below the file drop-down menu in the upper left-hand corner. Click the **Execute Command** icon. The Database Dictionary screen will display.
2. In the File Name field enter **cm3r**. Click the **Search** button.
3. In the Field table, highlight the **Number** entry and click the **Edit** icon in the upper left hand corner.
4. In the resulting window click the **Create Alias** button.
5. Change the value in the Name field from number.alias to **vj.number.1**. Click the OK icon in the upper left-hand corner.
6. Repeat steps 3 - 5, this time entering **vj.number.2** in the name field for step 5.
7. Click the **OK** icon in the upper left-hand corner of the file screen. The configuration is now complete.

16.3.1.4 Step 4: Creating Macros

Use the following steps to create macros:

1. In the Peregrine Service Center client, return to the main navigation menu by clicking the **Back** icon in the upper left hand corner.
2. From the main navigation pane scroll down to the *Utilities* section and click the **Tools** icon.
3. Scroll down to the section titled Tools and click the **Macros** icon. The *Available Macros* screen will display.
4. You will need to create two macros. For each of the two definitions below:
   a. Click the **Add** button on the left side of the *Available Macros* screen.
   b. Fill in the values for **Macro Name**, **Applies When**, **Macro Type**, and **Macro Condition** with the appropriate values. Note that the macro condition will need to be customized depending on your installed Peregrine customizations.
   c. Click the **Set Parameters** button. The *Editing Macro Parameters* screen will display.
   d. Fill in the value for **Application to Call**, then add the appropriate parameter-value pairs in the table below.
   e. Click **Save** to close the *Editing Macro Parameters* screen.
   f. Click the green check button to save the macro.

Definition 1
Macro Name: ARcm3rout Closed Change Requests
Applies When: Change Requests are Saved
Macro Type: Call A RAD Routine
Macro Condition: *category in $L.new="RFC - Advanced" and priority in $L.new~="1" and current.phase in $L.new~="4.implement"*

Set Parameters Section:
Application to Call: script.execute

Parameters	Values
file	$L.new
name	ARCustomClosedEventUpdate

Definition 2
Macro Name: ARcm3rout Open Change Requests
Applies When: Change Requests are Saved
Macro Type: Call A RAD Routine
Macro Condition: *category in $L.new="RFC - Advanced" and (priority in $L.new="1" or current.phase in $L.new="4.implement") and current.phase in $L.new~="5.accept"*

Set Parameters Section:
Application to Call: script.execute

Parameters	Values
file	$L.new
name	ARCustomClosedEventUpdate

16.3.1.5 Step 4: Editing the Event.out Format Control

The Configuration Change Console agent needs to update the "status" field in the Event Output Queue. In order for this to be possible, settings must be changed for the event.out format control. Please follow these steps to complete these changes.

1. In the Peregrine Service Center client, return to the main navigation menu by clicking on the **Main Menu** tab.
2. From the main navigation pane scroll down to the Utilities section and click the **Tools** icon.
3. Scroll down to the section titled Tools and click the **Format Control** icon. The *Search Format Control Records* screen will display.
4. In the Name field type `event.out` and click the **Search** button.
5. In the record for *event.out*, click the **Privileges** button.
6. In the Function/Condition table, set the values for *Add and Update* to **true**.
7. Click the **OK** button to save the record.
8. Click the **Back** button to close the form.

16.4 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 Remedy integration, for example, only the Windows agent can integrate with Remedy. If you are connecting to a Remedy server on another host, you can proxy the integration through a Windows host. For Peregrine, the operating system on which Peregrine is installed does not matter since the integration is web services based.

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.

16.5 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:  Oracle EM CCC Structure of Management Information
--
-- Copyright (c) 2002-2009 by Oracle, Inc.
-- All rights reserved.
--
-- ****************************************************************
--

AR-SMI DEFINITIONS ::= BEGIN

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

activer MODULE-IDENTITY
        LAST-UPDATED "200903040000Z"
        ORGANIZATION "Oracle, Inc."
        CONTACT-INFO
                        "Oracle
                        Support

                Postal: 500 Oracle Parkway
                        Redwood Shores, CA 94065
                        USA

                   Tel: +1 800 ORACLE1

                E-mail: oraclesales_us@oracle.com"
        DESCRIPTION
                "The Structure of Management Information for
                Oracle EM CCC."
        REVISION      "200903040000Z "
```

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

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

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

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

activerNotifications OBJECT-IDENTITY
        STATUS  current
        DESCRIPTION
                "activerNotifications is the main subtree for notifications
                (traps) sent by Oracle CCC software."
        ::= { activer 5 }

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

activerModules OBJECT-IDENTITY
        STATUS  current
        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 Oracle CCC-assigned
                OID subtree for use with Policy Management."
         ::= { activer 8 }
activerExperiment OBJECT-IDENTITY
```

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

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

END


AR-NOTIF.mib
-- ****************************************************************
-- AR-NOTIF.my:  Oracle EM CCC Notification Definition File
----
-- Copyright (c) 2002-2009 by Oracle, 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 "200903040000Z "
        ORGANIZATION "Oracle, Inc."
        CONTACT-INFO
                        "Oracle
                        Support

                Postal: 500 Oracle Parkway
                        Redwood Shores, CA 94065
                        USA

                   Tel: +1 800 ORACLE1

                E-mail: oraclesales_us@oracle.com"
        DESCRIPTION
                "The Definition of Notification sent by
                Oracle EM CCC."
        REVISION      "200903040000Z "
        DESCRIPTION
                "Initial version of this MIB module."
        ::= { activerModules 1 }   -- assigned by IANA
```

```
occNotifMIBObjects      OBJECT IDENTIFIER ::= { arNotif 1 }
occNotifConformance     OBJECT IDENTIFIER ::= { arNotif 2 }
occNotifInfo            OBJECT IDENTIFIER ::= { occNotifMIBObjects 1 }
occNotifNotification    OBJECT IDENTIFIER ::= { occNotifMIBObjects 2 }

-- Notification information objects

occNotifInfoMessage     OBJECT-TYPE
        SYNTAX          OCTET STRING (SIZE (0..256))
MAX-ACCESS    read-only
        STATUS        current
        DESCRIPTION
                "The text of the notification message generated by the
                Oracle EM CCC server."
        ::= { occNotifInfo 1 }

-- Notifications

occNotifNotificationSent        NOTIFICATION-TYPE
        OBJECTS         { occNotifInfoMessage }
        STATUS          current
        DESCRIPTION
                "This notification is generated by the CCC 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 Server, Data Center 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 that is used for the silent agent installation process:

```
#    Configuration Change Console Basic Silent Agent
#    Installation Configuration
#
#    This file should only be used to automate the agent installation
#    This file must be named to match the installer file name.
#    For example, if the installation file is agent-win32.exe,
#    this file should be agent-win32.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\:\\oracle\\ConfigurationChangeConsoleAgent

#  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\:\\\\oracle\\\\ConfigurationChangeConsoleAgent

# Which jre should this installation use... typical installs will use the user_
install_dir\jre
JAVA_HOME= C\:\\oracle\\ConfigurationChangeConsoleAgent\\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_PROVIDER_URL=t3s://host1:sslport1,host2:sslport2,host3:sslport3

#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/ConfigChangeConsole/Agent/bin
EXTRA_LD_LIBRARY_PATH=/tmp/ConfigChangeConsole/lib

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

C

Configuring an Oracle Database For Real-Time Monitoring

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 *
DatabaseName
DBUserName
HostName
LoginSid
NTDomainName
ObjectName
ObjectType
OwnerName
ServerName
TextData
Application Name
ObjectName
ObjectType
OwnerName
ServerName

TextData *
Application Name *
NTUserName *
LoginName*
SPID*
StartTime*

7. Click **Run**

E

User Permissions for Database Snapshot Monitoring

This section documents the permission requirements for the database snapshot monitoring capability. 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 9i/10g/11g

If you are running an Oracle 9i, 10g, or 11g 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 configuration file. Typically you should never need to change any values to these settings. They are documented here only for reference and possible problem resolution. The configuration file is located at:

<agent install directory>/config/probe.properties

After making any changes to this property file, the agent must be stopped and restarted for the changes to take affect.

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://host1:port1,host2:port2,….	This is the URL the agent uses to connect to the server(s) for communication. This is set by the installer and under normal operations does not need to be changed. If you are running a non-clustered environment, there will only be one host and one secure port (443 by default). If you are in a clustered environment, list each host and secure port separated by a comma.
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.

Table F–1 (Cont.) Agent Configuration File Parameters

Parameter	Suggested Value
archive.enabled=false	Enable or disable saving a copy of the XML messages that will be sent to the 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

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 G–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.
systemlanguage	'en'	The default language the system will use for non-UI based actions such as pre-generated reports or notifications. You can change this if you want the default language to be different. This will not affect the UI language which is set through the user's browser settings.

Table G–1 (Cont.) Server Properties Stored In Repository

Property Name	Default Value	Description
systemlocale	'US'	The default locale the system will use for non-UI based actions such as pre-generated reports or notifications. You can change this if you want the default locale to be different. This will not affect the UI locale which is set through the user's browser settings.