Oracle® Communications
Evolved Communications Application Server

Installation Guide

Release 7.0

E51170-02

August 2015

ORACLE®

Oracle Communications Evolved Communications Application Server Installation Guide, Release 7.0

E51170-02

Contents

5   Installing OCECAS

6   Creating and Configuring OCECAS Domains

7   OCECAS Post-Installation Tasks

8 Patching OCECAS

9 Troubleshooting an OCECAS Installation

10 Uninstalling OCECAS

Preface

This guide describes the system requirements and procedures for installing Oracle Communications Evolved Communications Application Server (OCECAS).

Audience

This document is for system administrators who install and configure OCECAS. The person installing the software should be familiar with the following:

- Operating system commands

- Network management

- Oracle database installation, configuration and administration

- Oracle Coherence

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Accessing Oracle Communications Documentation

OCECAS documentation is available from the Oracle Documentation Web site:
http://docs.oracle.com.

Related Documents

Refer to these additional documents for related information on OCECAS:

- *Oracle Communications Evolved Communications Application Server Release Notes*

- *Oracle Communications Evolved Communications Application Server Concepts*

- *Oracle Communications Evolved Communications Application Server System Administrator's Guide*

- *Oracle Communications Evolved Communications Application Server Operator's Guide*
- *Oracle Communications Evolved Communications Application Server Security Guide*
- *Oracle Communications Evolved Communications Application Server Compliance Guide*
- *Oracle Communications Evolved Communications Application Server RESTful API Reference*
- *Oracle Fusion Middleware 12c Documentation Library*
- *Oracle Database Installation Guide 12c Release 1 (12.1) for Linux*
- *Oracle Database Administrator's Guide 12c Release 1 (12.1)*

1

OCECAS Installation Overview

This chapter describes the general process for installing and configuring Oracle Communications Evolved Communications Application Server (OCECAS). Subsequent chapters describe installation steps in detail.

For more information about OCECAS, see *Oracle Communications Evolved Communications Application Server Concepts*.

Overview of Installed Components

During the installation process, you install and configure the following components:

- Oracle database software

- Either the Oracle NoSQL database software or the Oracle NoSQL client driver

- Java Development Kit (JDK) software

- Web browser

- The OCECAS software, which includes:

  - Oracle WebLogic Server, which is the platform container

  - Oracle Coherence software

  - Parts of the Oracle Communications Converged Application Server software that are necessary for OCECAS

- (Optional) OpenLDAP software

- (Optional) Session Border Controller software

- (Optional) Core Session Manager software

To view the supported software versions, see "OCECAS System Requirements".

Overview of the OCECAS Installation

The process of installing the OCECAS software includes the following tasks:

1. Plan your installation:

   - Determine the scale of your implementation, for example, a small test system or a large production system

   - Determine how many physical machines you need, and which software components to install on each machine

- Plan the system topology, for example, how the system components connect to each other over the network

2. Review system requirements, including:

   - Hardware requirements, such as disk space

   - System software requirements, such as operating system (OS) versions and OS patch requirements, and Java Virtual Machine (JVM) process requirements (such as memory settings)

   - Information requirements, such as IP addresses and host names

3. Perform pre-installation tasks, such as installing the database software and the JDK

4. Install OCECAS on your machines in the following order:

   a. On the machine that hosts your UDR domain

   b. On the machines that host your runtime domains

   c. On the machine that hosts your management domain

5. Create your OCECAS database and schema

6. Configure your OCECAS domains in the following order:

   a. Management domain

   b. Runtime domains

   c. UDR domain

7. Perform post-installation tasks, such as:

   - Install the NoSQL database or NoSQL client driver software

   - Create users for the Session Design Center (SDC) GUI

   - Perform additional domain configuration tasks

8. Troubleshoot any installation issues

Ensuring a Successful Installation

The OCECAS installation must be performed by qualified personnel. You must be familiar with the software requirements and the operating systems on which you are installing the software.

Follow these guidelines:

- As you install each component, such as the JDK, verify that the component installed successfully before continuing the installation process.

- Pay close attention to the system requirements. Before you begin installing the software, make sure that your system has the required base software. In addition, make sure that you know all of the required configuration values, such as host names and port numbers.

- As you create new configuration values, write them down. In some cases, you need to re-enter configuration values later in the procedure.

Directory Placeholders Used in This Guide

Table 1–1 lists placeholders that are used in this guide to refer to the directories that contain OCECAS system components.

Table 1–1   Directory Placeholders

Placeholder	Directory
Central_inventory_location	The directory in which the Oracle inventory file lives. The Oracle inventory lists all Oracle software installed on a machine. The Oracle installer creates this directory upon the first Oracle product installation.
DB_Oracle_home	The directory in which the Oracle database software is installed.
Domain_home	The directory in which the OCECAS domain resides (*Ocecas_home***/user_projects/domains/***domain_name*).
Ocecas_home	The directory in which to install the OCECAS software. This directory is created during product installation. This directory also serves as a repository for common files that are used by Oracle products installed on the same machine. These common files: ■ Facilitate checking of cross-product dependencies during installation ■ Facilitate patch installation
temp_dir	A temporary directory into which you download the OCECAS software.

2

Planning Your OCECAS Installation

This chapter provides information about planning your Oracle Communications Evolved Communications Application Server (OCECAS) installation.

About Planning Your OCECAS Installation

When planning an OCECAS installation, consider how many physical servers can handle your subscriber base and how many OCECAS nodes to include in your cluster.

Oracle recommends that your production pipeline has a testing, staging, and production system, with each one on a different machine.

The difference between an OCECAS development system and an OCECAS production system is only the number of machines in the system. You install the same components in a test system that you install in a production system.

See "OCECAS System Requirements" for information about required hardware and software.

Your OCECAS installation must also include an ECAS subscriber server (ESS) to store some subscriber information and some internal data. For details on planning your subscriber stores, see "About Managing and Using Subscriber Data" in *Enhanced Communications Application Server Concepts*.

Planning Your Installation

The following section describes the recommended OCECAS installation topologies.

Understanding Installation Topologies

Figure 2–1 shows a simple OCECAS installation topology that consists of one machine with three domains: a management domain, a single runtime domain, and an UDR domain. This topology is useful for demonstration or evaluation purposes, or in cases with limited resources (that is, limited CPU and memory).

Figure 2–1   Simple OCECAS Installation Topology
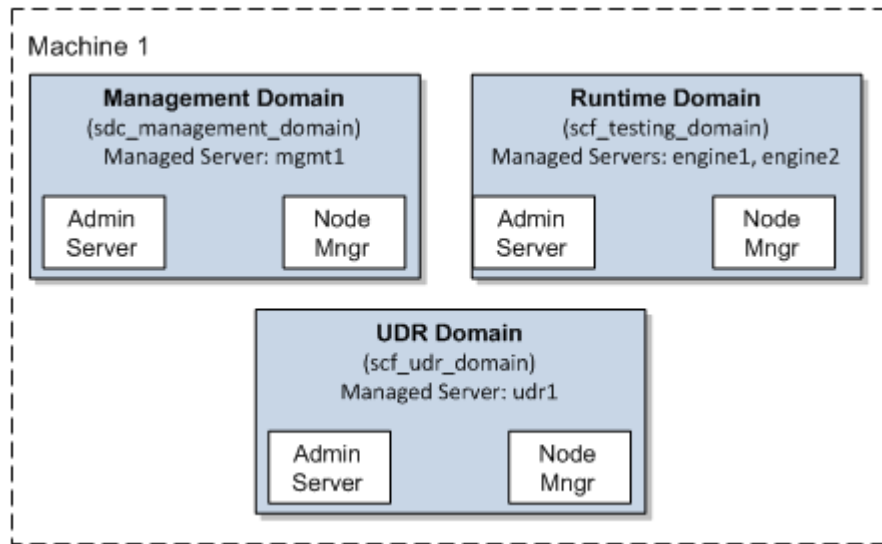
While a simple OCECAS topology is sufficient for development and Proof of Concept (PoC) installations, production systems must be robust and fault-tolerant.

Figure 2–2 shows a fault-tolerant OCECAS installation topology. In this topology, multiple machines are used to host clustered resources.

Figure 2–2   Fault-Tolerant OCECAS Installation Topology
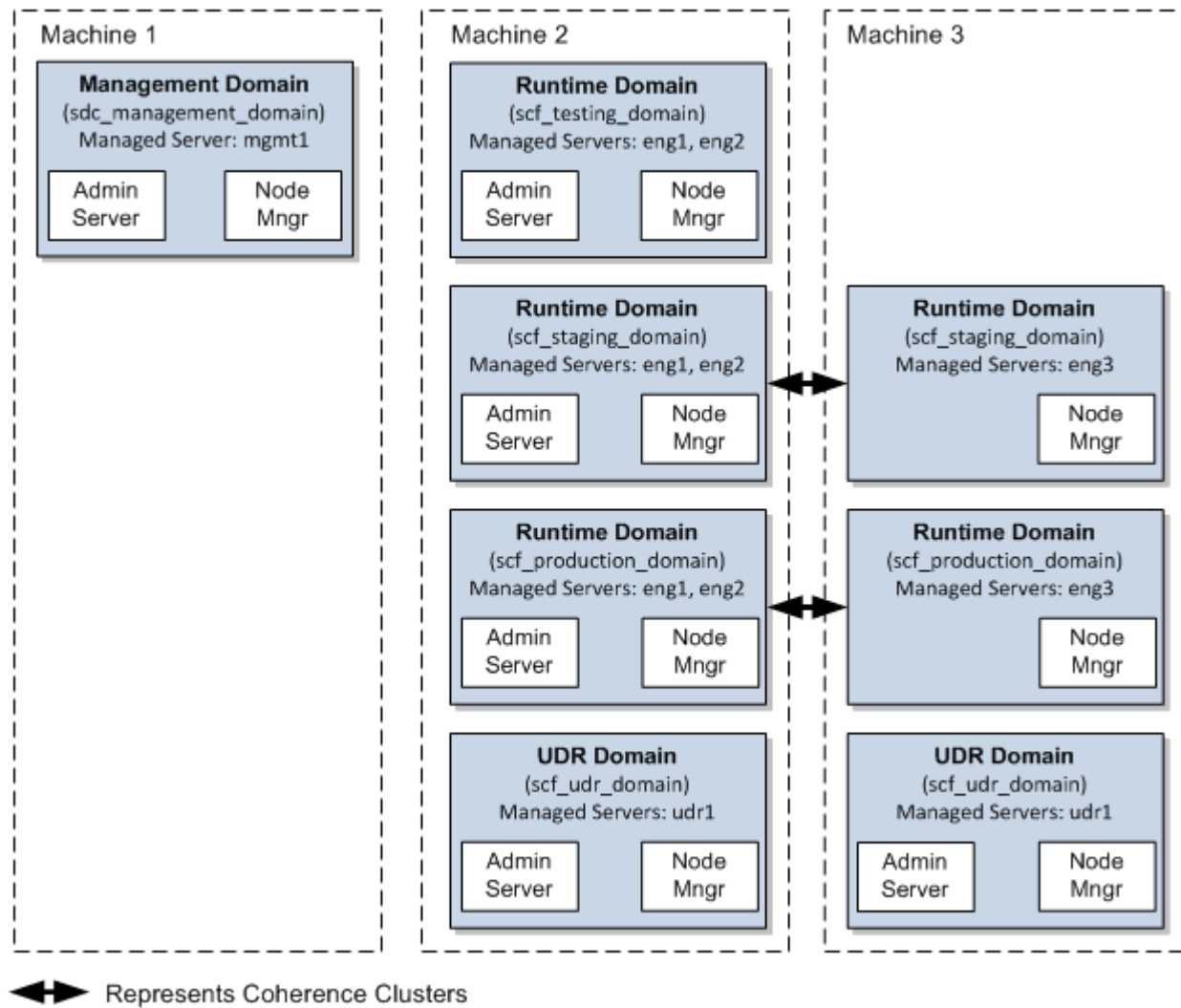
Each element in this topology illustration is described in Table 2–1.

Table 2–1   Description of the Elements in the OCECAS Standard Installation Topology

Element	Description and Links to Additional Documentation
OCECAS Domain	A logically related group of Java components (in this case, the Administration Server, managed servers, and other related software components).
	For more information, see "Understanding Domains" in *Oracle Fusion Middleware Understanding Oracle WebLogic Server*.
Administration Server	The central control entity of a domain, which maintains the domain's configuration objects and distributes configuration changes to managed servers.
	For more information, see "Administration Server" in *Oracle Fusion Middleware Understanding Oracle WebLogic Server*.

Table 2–1   (Cont.) Description of the Elements in the OCECAS Standard Installation

Element	Description and Links to Additional Documentation
Cluster	A collection of multiple OCECAS instances running simultaneously and working together. For more information, see "Managed Servers and Managed Server Clusters" in *Oracle Fusion Middleware Understanding Oracle WebLogic Server*.
Node Manager	Node Manager is a WebLogic Server utility that enables you to start, shut down, and restart Administration Server and managed server instances from a remote location. Although Node Manager is optional, it is recommended if your WebLogic Server environment hosts applications with high availability requirements. For more information, see "Running Node Manager as a Startup Service" in *Oracle Fusion Middleware Understanding Oracle WebLogic Server*.
Machine	A logical representation of the computer that hosts one or more WebLogic Server instances (servers). Machines are also the logical glue between OCECAS managed servers and the Node Manager; to start or stop a managed server with Node Manager, the managed server must be associated with a machine.
Managed Server	The host for your applications, application components, Web services, and their associated resources. For more information, see "Managed Servers and Managed Server Clusters" in *Understanding Oracle WebLogic Server*.

OCECAS Coherence Planning

OCECAS nodes are based on Oracle Coherence. Decide how to configure Oracle Coherence settings for your OCECAS topology, for example, how many nodes to add to the cluster when a node failure occurs. For more information, see "Configuring and Managing Coherence Clusters" in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

About the OCECAS Domains

An OCECAS implementation requires a set of WebLogic domains. Together they comprise a deployment pipeline that you use to develop, stage, and finally deploy multimedia services for your subscribers to use. For more information, see "About Change Management and the Production Pipeline" in *Evolved Communications Application Server Concepts*.

If you are creating a test, demonstration, or evaluation implementation, you can install these domains, or a combination of them, on the same physical or virtual system. A production implementation normally requires a separate WebLogic machine for each domain. Each OCECAS implementation requires these domains:

- **Management Domain**

  You use the management domain to administer all other domains. You run the Session Design Center (SDC) GUI on this domain. You must install the Oracle database software and run the **root.sh** script on the same machine that hosts this domain.

- **Testing Domain** (Runtime Domain)

You use the testing domain to develop new services and implementation changes. You create a testing domain by using the runtime domain template. You can cluster this domain across multiple WebLogic machines, if required.

Each runtime domain requires access to a UDR component. The UDR component can be co-located with the runtime domain, located in another runtime domain, or deployed into a domain of its own.

- **Staging Domain** (Runtime Domain)

  You use the staging domain to test the changes you created in the testing domain. You create a staging domain by using the runtime domain template.

  Each runtime domain requires access to a UDR component. The UDR component can be co-located with the runtime domain, located in another runtime domain, or deployed into a domain of its own.

- **Production Domain** (Runtime Domain)

  Your subscribers access services on the production domain. On clustered systems, one production domain spans two clustered WebLogic machines with the UDR domain on a separate machine.

  Each runtime domain requires access to a UDR component. The UDR component can be co-located with the runtime domain, located in another runtime domain, or deployed into a domain of its own.

- (Optional) **UDR Domain**

  You use the User Data Repository (UDR) domain to store some subscriber data in an ECAS subscriber server (ESS). You create a UDR domain by using the UDR domain template.

  An ESS is required, but it does not have to be in a dedicated UDR domain. You can also store it in a runtime domain, or on its own. See "About Managing and Using Subscriber Data" in *Enhanced Communications Application Server Concepts* for more information.

Table 2–2 describes each OCECAS domain.

Table 2–2   Domains Required by OCECAS

Domain Type	Domain Template to Use	Default Name and Location
Management Domain	Management Domain	*Ocecas_home*/**user_projects/domains/sdc_management_domain**
Testing Domain	Runtime Domain	*Ocecas_home*/**user_projects/domains/scf_testing_domain** (required; see "Configuration Type Screen")
Staging Domain	Runtime Domain	*Ocecas_home*/**user_projects/domains/scf_staging_domain** (required; see "Configuration Type Screen")
Production Domain	Runtime Domain	*Ocecas_home*/**user_projects/domains/scf_production_domain** (required; see "Configuration Type Screen")
UDR domain	UDR Domain	*Ocecas_home*/**user_projects/domains/scf_udr_domain**

Understanding Port Numbering

For a production OCECAS implementation, you must change the default port numbers. See "Securing Ports" in *Evolved Communications Application Server Security Guide* for a list of the default port numbers and their security implications.

For a test and evaluation system, you can use the default port numbers if you install each domain on its own system. However, you will probably install more than one domain on a single system. In that case, ensure that the various ports for each domain are unique within that system. This includes:

- Administration Server listening ports

- Administration Server SSL ports

- Node Manager Ports

- Management Server mgmt1 listening ports

- Management Server SSL listening ports

- Runtime Domain engine listening ports

- Runtime Domain engine SIP channel ports

- Runtime Domain engine SIPs channel ports

- Runtime Domain cluster unicast ports

Domain Support File Locations

The domain template JARs for these domain types are located in the *Ocecas_home*/**wlserver/common/templates/wls** directory.

The domain configuration scripts and property files are located in the *Ocecas_home*/**wlserver/common/templates/scripts/wlst** directory.

About Installing a Secure System

In a production system, ensure that communication between components and access to the system servers are secure. For information about choices for installing a secure system, see "Performing a Secure OCECAS Installation" in *Evolved Communications Application Server Security Guide*.

3

OCECAS System Requirements

This chapter describes the software, hardware, and information requirements for Oracle Communications Evolved Communications Application Server (OCECAS).

Software Requirements

OCECAS is supported for production use on the operating system, hardware, and Java Virtual Machine (JVM) combinations shown in Table 3–1.

> **Note:** OCECAS does not support any OpenJDK.

Table 3–1 OCECAS Supported Software

Operating System	Hardware Architectures	JDK	Additional Information
Oracle Enterprise Linux Release 6.5 (64 bits)	x86-32	Oracle JDK 1.8.0_31 (64 bits) and later security patch versions	NA

Database Software

Table 3–2 shows the databases that OCECAS supports.

Table 3–2 Supported Databases

Database Software	Notes
Oracle 12*c* Release 12.1.0.1.0 Standard Edition	NA
Oracle NoSQL Database, Community Edition 12*c*R1 (12.1.3.0.14)	NA
Oracle NoSQL Database, Client Driver 12.1.3.0.14	NA

LDAP Software

Table 3–3 shows the LDAP authentication software that OCECAS supports.

Table 3–3 Supported LDAP Software

LDAP Software	Notes
OpenLDAP Version 2.4.40	NA

Middleware Software

Table 3–4 shows the middleware software that OCECAS supports.

Table 3–4   Supported Middleware Software

Middleware Software	Notes
WebLogic Server Version 12.1.3.0.0	NA
Oracle Coherence 12.1.3.0.0	NA

Web Browsers

Table 3–5 shows the web browsers that OCECAS supports.

Table 3–5   Supported Web Browsers

Web Browser	Notes
Firefox 35.0.1	NA
Chrome 40.0	NA

About Critical Patch Updates

OCECAS is supported on all Oracle Critical Patch Updates. Install all critical patch updates as soon as possible.

To download Critical Patch Updates, find out about security alerts, and enable email notifications about Critical Patch Updates, see the Security topic on Oracle Technology Network:

http://www.oracle.com/technetwork/topics/security/whatsnew/index.html

Hardware Requirements

This section describes the required hardware for OCECAS.

The number and configuration of the computers that you employ for your OCECAS installation depend on the scale and the deployment type you plan according to your charging requirements. Work with your performance team to determine your sizing requirements.

OCECAS has similar requirements to Oracle WebLogic Server. The following items are required in addition to the basic WebLogic Server requirements:

- Gigabit Ethernet connections are required for all production deployments.
- Dual network interface cards (NICs) are required to provide failover capabilities in a production environment.
- Extra RAM is required to support the throughput requirements of most production installations.
- A load balancer is required for production installations.

Information Requirements

Table 3–6 shows the information you provide during the OCECAS installation process.

> **Note:** For production systems, reference fully qualified domain names (FQDN) for systems instead of **localhost** for listener addresses.

Table 3–6   Required Information

Information Type	Description	Default Value
Host name or IP address	The network names or IP addresses of the machines on which you are going to install the software.	Current host name or IP address
Directory	The directory on each machine that serves as your *Ocecas_home* directory.	NA
Password	A password for the administrative user. The password must have a minimum of eight characters, at least one of which is non-alphabetic.	NA

4

OCECAS Pre-Installation Tasks

This chapter describes tasks you must complete before installing Oracle Communications Evolved Communications Application Server (OCECAS).

About Pre-Installation Tasks

You must perform certain tasks before installing OCECAS. Pre-installation tasks are broken down into the following categories:

- Tasks that are not specific to OCECAS but that are required for a functioning installation. See "General Pre-Installation Tasks".

- Tasks that you must perform before you install OCECAS. See "OCECAS Pre-Installation Tasks".

General Pre-Installation Tasks

Before continuing, complete the following general pre-installation tasks:

- Allocate IP addresses for OCECAS interfaces, including:
    - Public-facing external interfaces
    - Internal-facing interfaces
    - Intra-system interfaces for private signaling between OCECAS nodes
    - If required by your organization, a separate systems management interface
- Determine which logical interfaces map to which physical interfaces on each server.
- Have access to a Domain Name Service (DNS) and Network Time Protocol (NTP) server.
- Optionally assign fully qualified domain names to each server.
- Make a note of any required static routes.

OCECAS Pre-Installation Tasks

Before you install the OCECAS software, perform the following pre-installation tasks on each physical or virtual machine:

- Create a user account for installing the OCECAS software. See "Creating a UNIX User for Installing OCECAS".

- Install the JDK software. See "Installing a Java Development Kit".

- Install the Oracle database software. See "Installing the Oracle Database Software".

- If LDAP authentication is required, install the OpenLDAP software. See "Installing the OpenLDAP Software".

- Choose a directory for installing all Oracle software. See "Choosing an Installation Directory".

Creating a UNIX User for Installing OCECAS

You create a UNIX user to:

- Install the Oracle database software.

  For more information, see "Installing the Oracle Database Software".

- Run the **root.sh** script for creating your OCECAS database and schema.

  For more information, see "About the OCECAS Database Creation Script".

- Install the OCECAS software.

  For more information, see "Installing OCECAS in GUI Mode".

- Create the OCECAS domains.

  For more information, see "Starting the Domain Configuration Wizard".

Although you can use any UNIX user with sufficient privileges, this guide assumes that the user is named **ocecas** and is a member of the **dba** group.

To create a UNIX user for installing OCECAS:

1. Log into your system as user **root**.

2. Create a directory for storing the OCECAS software. For example:

   mkdir -p *Ocecas_home*

3. Create a user named **ocecas** that has a home directory of *Ocecas_home* and a default login shell of bash. For example:

   /usr/sbin/useradd -d *Ocecas_home* **-s /bin/bash ocecas passwd ocecas**

4. Change the user and group ownership to **ocecas** for the *Ocecas_home* directory and all of its files and subdirectories. For example:

   chown -R ocecas:ocecas *Ocecas_home*

Installing a Java Development Kit

Install Oracle Java Development Kit (JDK) plus the latest security update on each physical machine or VM in your OCECAS system. For a list of supported software versions, see "Software Requirements".

To install and configure your JDK:

1. Download the JDK from the Java SE Development Kit Downloads page at:

   http://www.oracle.com/technetwork/java/javase/downloads/

2. Install the JDK per instructions provided with it.

3. Add the JDK **bin** directory to the beginning of the **PATH** variable definition. For example:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```

```
export PATH
```

4. Check that your system is using the correct version of the JDK by entering the following command:

   java -version

Installing the Oracle Database Software

Install the Oracle 12*c* database software as the user **ocecas**. Install the software either:

- On the machine that hosts your management domain

- On a machine that is connected by Transparent Network Substrate (TNS) or Java Database Connectivity (JDBC) to the machine that hosts your management domain

To download the software, go to the Oracle Database Software Downloads page at:

http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html

> **Note:** Do not create a database. During OCECAS installation, you run the **root.sh** script, which automatically creates the OCECAS database instance and schema for you.

For more information about:

- Supported database software versions, see "Database Software".

- The **root.sh** script, see "About the OCECAS Database Creation Script".

Installing the OpenLDAP Software

If your system requires LDAP authentication, you must install the OpenLDAP software on each physical machine in your OCECAS system.

To see the list of supported OpenLDAP software versions, see "LDAP Software".

To install the OpenLDAP software:

1. Download the OpenLDAP software from the OpenLDAP software web site:

   http://www.openldap.org/software/download/

2. Unpack the archive file by entering the following command:

   tar xfz openldap-*n.n.nn***.tgz**

   The **openldap-***n.n.nn* subdirectory is created, where *n.n.nn* is the OpenLDAP software version number. For example, **openldap-2.4.40**.

3. Go to the **openldap-***n.n.nn* subdirectory.

4. Configure the software by using the OpenLDAP **configure** script. See "Building and Installing OpenLDAP Software" in *OpenLDAP Software 2.4 Administrator's Guide*.

5. Build dependencies by entering the following command:

   make depend

6. Build and compile the OpenLDAP software by entering the following command:

```
make
```

7. Run the test suite to verify the build by entering the following command:

```
make test
```

8. As a super user, install the OpenLDAP software by entering the following command:

```
su root -c 'make install'
```

For more information about:

- Installing and using the OpenLDAP software, see *OpenLDAP Software 2.4 Administrator's Guide*.

- Configuring LDAP authentication, see "Managing User Entities" in *Evolved Communications Application Server System Administrator's Guide*.

Choosing an Installation Directory

When you install OCECAS, you are prompted to specify an Oracle Home directory. This is the directory in which you install the OCECAS software. This directory also serves as a repository for common files that are used by multiple Oracle products installed on the same machine.

The files in the *Ocecas_home* directory are essential to ensuring that OCECAS, WebLogic Server, and Oracle Coherence operate correctly on your system. They facilitate checking of cross-product dependencies during installation.

For more information about selecting an installation directory, see "Understanding the Oracle WebLogic Server and Coherence Directory Structure" in *Installing and Configuring Oracle WebLogic Server and Coherence*.

Next Steps

After you complete the pre-installation tasks, install OCECAS. See "Installing OCECAS" for instructions.

5

Installing OCECAS

This chapter describes how to run the Oracle Communications Evolved Communications Application Server (OCECAS) installation program.

Before you install OCECAS, complete all pre-installation tasks described in "OCECAS Pre-Installation Tasks".

Overview of OCECAS Installation Tasks

After you complete all pre-installation tasks, install OCECAS by performing the following:

1. Install OCECAS on the machine that will host your *UDR domain*.

2. Install OCECAS on the machines that will host your *runtime domains*.

3. Install OCECAS on the machine that will host your *management domain*.

4. Create your OCECAS database and schema by running the **root.sh** script on the machine that will host your management domain.

You can run the OCECAS installer in GUI mode or silent mode. Silent mode enables you to perform a non-interactive installation of OCECAS. Use silent mode to install OCECAS quickly on multiple systems.

For installation instructions, see the following sections:

- Installing OCECAS in GUI Mode

- Installing OCECAS in Silent Mode

Installing OCECAS in GUI Mode

To run the installation program in GUI mode, the console attached to the machine on which you are installing the software must support a Java-based GUI.

To install OCECAS:

1. Log in to the machine on which you want to install OCECAS.

2. If you plan to create a domain immediately after installing OCECAS, ensure that the Oracle database listener is running.

    To start the Oracle database listener, enter the following command:

    *DB_Oracle_home***/bin/lsnrctl start**

where *DB_Oracle_home* is the directory in which you installed the Oracle database software. For more information about starting the listener, see "Listener Control Utility" in *Oracle Database Net Services Reference*.

3. Download the OCECAS software from the Oracle software delivery website at:

   http://edelivery.oracle.com

4. Go to the directory where you downloaded the installation program and unzip the archive.

5. Launch the installation program by entering the following command from the JDK directory on your system:

   java -jar ocecas_generic.jar

   The installation program starts.

   If no other Oracle products are installed on the system, the Installation Inventory screen appears. Specify the location where you want to create your central inventory. Make sure that the operating system group name selected on this screen has write permissions to the central inventory location.

   For more information about the central inventory, see "Understanding the Oracle Central Inventory" in *Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

   If an Installation Inventory exists, the Installation Welcome screen appears.

6. Click **Next**.

   The Installation Location screen appears.

7. Enter or browse to the directory in which to install the OCECAS software and then click **Next**.

   The Installation Type screen appears.

8. Select **Evolved Communications Application Server Installation**, and then click **Next**.

   The Prerequisite Checks screen appears.

9. The screen automatically tests your system to ensure that it meets all operating system and JDK software requirements:

   - A green check mark indicates that your system passed the prerequisite check.

   - A red circle indicates a problem. The bottom of the screen shows a short error message to help you troubleshoot the problem. Fix the error and click **Rerun** to perform the prerequisite checks again. To continue the installation without fixing the problem, click **Skip**.

10. Click **Next**.

    The Security Updates screen appears.

11. If you already have a My Oracle Support account, use this screen to indicate how you would prefer to receive security updates: through email or through My Oracle Support.

    If you do not have a My Oracle Support account and are sure that you want to skip this step, clear the check box and verify your selection in the follow-up dialog box.

12. Click **Next**.

The Installation Summary screen appears.

13. Verify the installation options you selected. If you want to save these options to a response file, click **Save Response File** and provide a location and name for the response file. Response files can be used later in a silent installation.

> **Note:** If you only want to save a response file, you can exit the installation now.

14. Click **Install** to start the installation.

The Installation Progress screen appears, and a progress bar indicates the status of the installation process.

> **Note:** After the installation begins, if you click **Cancel**, the installation process stops but the files that are already copied are not removed.

15. Click **Next**.

The Installation Instructions screen appears.

16. If you are installing OCECAS on a machine that will host a runtime or UDR domain, click **Next** and proceed to step 17.

If you are installing OCECAS on a machine that will host the management domain, open a command window and perform the following steps:

a. Log in as the **ocecas** user. See "Creating a UNIX User for Installing OCECAS".

b. Ensure that ORACLE_BASE and ORACLE_HOME are not defined in your environment.

c. Enter the following command to create the OCECAS database and schema:

```
./root.sh -d install
```

The script displays a series of prompts.

> **Note:**
>
> ■ Do not run **root.sh** in a shell spawned as a sub-process; otherwise, the script will hang.
>
> ■ For more information about the **root.sh** script, see "About the OCECAS Database Creation Script"

d. At each prompt, answer the question and then press Enter. Table 5–1 describes each prompt.

Table 5–1   Root.sh Script Prompts

Prompt	Description
UNIX_USER	Enter the name of the user you used to install the Oracle database software.
UNIX_GROUP	Enter the name of the group to which the UNIX user belongs. The default Oracle database group name is **dba**.
ORACLE_BASE	Enter the base directory of the Oracle database installation. The Oracle base directory is the initial portion of the installation path in a standard Oracle database installation. For example, **/u01/app/oracle**.
ORACLE_HOME	Enter the complete path to the Oracle database installation. For example, if ORACLE_BASE is **/u01/app/oracle**, ORACLE_HOME would be **/u01/app/oracle/product/12.1.0/dbhome**.
sdc User Password	Enter a password for the **sdc** user. The **sdc** user is the owner of the database that this script creates, and is used by OCECAS for all database operations. You will be prompted to enter this password twice.
SYS User Password	Enter the password for the Oracle database **SYS** user. The SYS user is an administrative user and is the owner of all database objects. For more information about the Oracle database **SYS** user, see "Administrative User Accounts" in *Oracle Database Administrator's Guide*. You will be prompted to enter this password twice.
SYSTEM User Password	Enter the password for the Oracle database **SYSTEM** user. The Oracle database **SYSTEM** user is the master database administrator user with access to all of the database objects. For more information about the Oracle database **SYSTEM** user, see "Administrative User Accounts" in *Oracle Database Administrator's Guide*. You will be prompted to enter this password twice.
SDC_ADMIN User Password	Enter a password for the **SDC_ADMIN** user. You will be prompted to enter this password twice.

    e.   Return to the GUI installer screen and click **Next**.

17. In the Installation Complete screen, perform one of the following:

- Select the **Automatically Launch the Configuration Wizard** check box on this screen. After you click **Finish** to close the installer, the configuration wizard is started and you can begin to configure your domain. If you choose to do this, proceed to "Creating Domains Using the Graphical Domain Configuration Wizard".

- Deselect the **Automatically Launch the Configuration Wizard** check box on this screen. After you click **Finish** to close the installer, manually start the configuration wizard to begin configuring your domain. If you choose to do this, proceed to "Starting the Domain Configuration Wizard".

Installing OCECAS in Silent Mode

Silent mode is a way of setting installation options once and then using those settings to duplicate the installation on many machines. The installation program reads your settings from a Response File that you create prior to beginning the installation. The installation program does not display any options during the installation process.

For general information about silent installation for Oracle products, see "Running the Installation Program in Silent Mode" in *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server.*

About the Response File

The entries in the Response File (**response.rsp**) correspond to the prompts that you would see if you used GUI mode.

Incorrect entries in **response.rsp** can cause installation failures. To help you determine the cause of a failure, Oracle recommends that you create a log file when you start the installation.

The following shows a sample version of a **response.rsp** file. Your input may be slightly different, depending on your installation.

```
[ENGINE]

#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

#The oracle home location. This can be an existing Oracle Home or a new Oracle
Home
ORACLE_HOME=Ocecas_home

#Set this variable value to the Installation Type selected. e.g. Session Design
and Control.
INSTALL_TYPE=Evolved Communications Application Server

#Provide the My Oracle Support Username. If you wish to ignore Oracle
Configuration Manager configuration provide empty string for user name.
MYORACLESUPPORT_USERNAME=

#Provide the My Oracle Support Password
MYORACLESUPPORT_PASSWORD=<SECURE VALUE>

#Set this to true if you wish to decline the security updates. Setting this to
true and providing empty string for My Oracle Support username
will ignore the Oracle Configuration Manager configuration
DECLINE_SECURITY_UPDATES=true

#Set this to true if My Oracle Support Password is specified
SECURITY_UPDATES_VIA_MYORACLESUPPORT=false

#Provide the Proxy Host
PROXY_HOST=

#Provide the Proxy Port
PROXY_PORT=

#Provide the Proxy Username
PROXY_USER=

#Provide the Proxy Password
PROXY_PWD=<SECURE VALUE>

#Type String (URL format) Indicates the OCM Repeater URL which should be of the
format [scheme[Http/Https]]://[repeater host]:[repeater port]
```

```
COLLECTOR_SUPPORTHUB_URL=
```

See *Oracle WebLogic Server Installation Guide* for more information.

Returning Exit Codes to the Console

The silent installation program generates exit codes that indicate the success or failure of the installation. Table 5–2 describes these exit codes:

Table 5–2   Installation Program Exit Codes

Code	Description
0	Installation completed successfully.
-1	Installation failed due to a fatal error.
-2	Installation failed due to an internal XML parsing error.

If you start the silent installation process from a script, you can have these exit codes displayed to the console. Example 5–1 shows a sample command file that runs the installation while in silent mode and echoes the exit codes to the console from which the script is executed.

Example 5–1   Return Exit Codes

```
rem Execute the installer in silent mode
@echo off
java -jar ocecas_generic.jar -silent -responseFile=/home/use/bin/response.rsp
-log=logfilename

@rem Return an exit code to indicate success or failure of installation
set exit_code=%ERRORLEVEL%

@echo.
@echo Exitcode=%exit_code%
@echo.
@echo Exit Code Key
@echo ---------------
@echo  0=Installation completed successfully
@echo -1=Installation failed due to a fatal error
@echo -2=Installation failed due to an internal XML parsing error
@echo.
```

Running the Installer in Silent Mode

To install OCECAS in silent mode:

1. Log in to the target system.

2. Download the OCECAS software from the Oracle software delivery website at:

   http://edelivery.oracle.com

3. Create a response file, as described in "About the Response File".

4. Go to the directory where you downloaded the OCECAS software.

5. Start the installer by entering the following command:

   java -jar ocecas_generic.jar -silent -responseFile *ResponseFile*

The OCECAS Installer checks for all required software and writes errors to a log file if it detects any missing or unavailable components, or if there are any connectivity-related issues.

6. If you are installing OCECAS on the machine that will host the management domain, perform the following additional steps:

a. When prompted, run the **root.sh** script from the *Ocecas_home* directory:

```
root.sh -d install -u unixUser -g dbGroup -b oracleBaseDir -h DB_Oracle_
home -i dbInstance
```

For more information about the script and its parameters, see "About the OCECAS Database Creation Script".

b. When prompted, enter passwords for the **sdc** user, **SYS** user, **SYSTEM** user, and **SDC_ADMIN** user.

c. When the **root.sh** script completes, ensure that the Oracle TNSListener has started by entering the following command:

```
DB_Oracle_home/bin/lsnrctl start
```

7. Check whether the installer completed successfully by retrieving the exit codes, as described in "Returning Exit Codes to the Console".

About the OCECAS Database Creation Script

During the OCECAS installation process, you must run the **root.sh** script on the machine that hosts the management domain.

The script creates the following:

- An Oracle database instance named **SDC**.

- The OCECAS database schema.

- A database user named **sdc**. This account is used to access the data in the SDC database.

- A database administrative user named **SDC_ADMIN**. This user owns the database schema and has administrator privileges.

Script Syntax and Options

The **root.sh** script is located in *Ocecas_home* and uses the following syntax:

```
root.sh -d install| remove -u unixUser -g dbGroup -b oracleBaseDir -h DB_Oracle_
home -i dbInstance
```

The script accepts a number of command-line arguments. If you do not include any arguments, the script prompts for the required values. The script automatically prompts you for passwords for the **sdc**, **sdc_admin**, **SYS**, and **SYSTEM** user accounts.

Table 5–3 describes the command-line options for **root.sh** in detail.

Table 5–3   root.sh Command Line Options

Command Flag	Description
-d install | **remove**	When set to **install**, the script creates an OCECAS Oracle instance. When set to **remove**, the script removes the OCECAS Oracle instance.
-u *unixUser*	The name of the UNIX user you used to install OCECAS and the Oracle database software. See "Creating a UNIX User for Installing OCECAS".
-g *dbGroup*	The name of the group to which the UNIX user belongs, for example, **dba**.
-b *oracleBaseDir*	The base directory of the Oracle database software. The Oracle base directory is the initial portion of the installation path that terminates before **/product/12.1.0/dbhome** in a standard Oracle database software installation.
-h *DB_Oracle_home*	The complete path to the Oracle database installation, for example, *oracleBaseDir***/product/12.1.0/dbhome**.
-i *dbInstance*	The database instance number.

Troubleshooting root.sh

If **root.sh** fails with any errors, you can find logs at *Ocecas_home***/wlserver/csp/installation/scripts/logs/install.log**.

Next Steps

Now that OCECAS is installed, you need to create and configure the domains it requires. See "Creating and Configuring OCECAS Domains" for instructions.

6

Creating and Configuring OCECAS Domains

This chapter describes the steps required to create your Oracle Communications Evolved Communications Application Server (OCECAS) domains. You do this after the OCECAS software has been successfully installed.

Before continuing in this chapter, you must understand the following:

- WebLogic Server domains and clustering. See "Understanding Oracle WebLogic Server Domains" and "Understanding WebLogic Server Clustering" in *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server*.

- The domain topologies available for use with OCECAS, see "Understanding Installation Topologies".

Overview of OCECAS Domain Creation Tasks

Create your OCECAS domains in the following order:

1. Management domain

2. Runtime domains

3. (Optional) UDR domain

For instructions for creating your domain, see "Creating Domains Using the Graphical Domain Configuration Wizard".

About Domains and Domain Configuration

You must configure the domains of all servers in your OCECAS system. You configure your domains by using the WebLogic Server Domain Configuration Wizard.

After you configure a domain by using the Domain Configuration Wizard, you can package the domain configuration data and copy it to other servers. Use the **pack** and **unpack** commands provided by Oracle WebLogic Server to package the configuration data for copying to all the other servers. The OCECAS installer copies the **pack** and **unpack** commands to the *Ocecas_home*/**wlserver/common/bin** directory. For more information about packing and unpacking configurations, see *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

For more information about other methods available for domain creation, see "Additional Tools for Creating, Extending, and Managing WebLogic Domains" in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Recommendations and Requirements for Replicated Domains

If you are replicating a testing, deployment, or production domain, use the following guidelines for ease of deployment:

- Keep the directory structures the same on each machine in the cluster to simplify deployment.

- Install the OCECAS binaries on each machine in the cluster.

- Install any required patches manually on each machine in the cluster; they are not distributed automatically.

- Create the replicated domain on your Administration Server, and copy that domain to each of your cluster machines.

> **Note:** If the Administration Server is already started before you copy its domain to the cluster servers, delete the existing domains on each cluster server with this command:
>
> ```
> rm -rf Domain_home/servers/
> ```

Creating Domains Using the Graphical Domain Configuration Wizard

The general process for creating domains is:

1. Create your management domain.

2. Create the *Domain_home* directory (*Ocecas_home*/**user_projects/domains/***domain_name*) for your runtime domains.

   where *domain_name* is the name of the directory in which to install your domain files. For replication to work properly, your runtime domains must have *domain_name* set to one of the following:

   - For the testing domain: **scf_testing_domain**

   - For the staging domain: **scf_staging_domain**

   - For the production domain: **scf_production_domain**

3. Create your runtime domains.

4. (Optional) Create your UDR domain.

Starting the Domain Configuration Wizard

If you selected the **Automatically Launch the Configuration Wizard** check box during OCECAS installation, the Domain Configuration Wizard starts automatically.

To start the Domain Configuration Wizard manually:

1. Log in to the target machine as user **ocecas**. For more information, see "Creating a UNIX User for Installing OCECAS".

2. Go to the *Ocecas_home*/**wlserver/common/bin** directory.

3. Enter the following command:

   ./config.sh

Configuring Domains Using the GUI Configuration Wizard

The Domain Configuration Wizard screens prompt you to enter specific information about your system and configuration. For information about responding to the prompts during installation, see the following sections:

- Configuration Type Screen

- Templates Screen

- Administrator Account Screen

- Domain Mode and JDK Screen

- JDBC Data Sources Screen

- JDBC Data Sources Test Screen

- Advanced Configuration Screen

- Configuration Summary Screen

- Configuration Progress Screen

- Configuration Success Screen

Configuration Type Screen

In the Configuration Type screen:

1. Select **Create a new domain**.

2. In the **Domain Location** field, specify your *Domain_home* directory. This directory must be empty.

   For runtime domains, override the default domain name (base_domain) with one of the following names. These names allow replication to work properly in an OCECAS system with Coherence Clusters.

   - For the testing domain: **scf_testing_domain**

   - For the staging domain: **scf_staging_domain**

   - For the production domain: **scf_production_domain**

   Oracle recommends that you create your domain outside of the *Ocecas_home* directory. This directory structure helps you avoid issues when you upgrade or reinstall your software.

3. Click **Next**.

   The Templates screen appears.

For more information about:

- The *Domain_home* directory, see "Choosing a Domain Home" in *Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware*.

- Other options on the Configuration Type screen, see "Configuration Type" in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Templates Screen

In the Templates screen:

1. Select **Create Domain Using Product Templates**.

   This option offers you a set of domain templates. See "About Domains and Domain Configuration" for a description of the different templates.

2. In the **Available Templates** area, select only *one* of the following OCECAS configuration templates:

   - To create a runtime domain, select **Oracle Communications SCF Runtime Domain - 7.0.0.0**

   - To create a UDR domain, select **Oracle Communications SCF UDR Domain - 7.0.0.0**

   - To create a management domain, select **Oracle Communications SDC Management Domain - 7.0.0.0**

   > **Note:** You can configure only one OCECAS domain at a time.

   ---

3. Click **Next**.

   The Administrator Account screen appears.

   For more information about the options on the Templates screen, see "Templates" in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Administrator Account Screen

In the Administrator Account screen:

1. In the **Name** field, enter the user name for the domain's default WebLogic Administrator account. The default is **weblogic**.

   User names are case-sensitive. Do not use commas or any characters in the following comma-separated list:

   `\t, < >, #, |, &, ?, ( ), { }`

2. In the **Password** field, enter the main administrator password.

   The password is case-sensitive and must contain a minimum of eight characters, at least one of which is not alphabetic.

3. In the **Confirm Password** field, re-enter your password.

4. Write down the user name and password. You will need this information later.

5. Click **Next**.

   The Domain Mode and JDK screen appears.

Domain Mode and JDK Screen

In the Domain Mode and JDK screen:

1. In the **Domain Mode** area, select the appropriate startup mode for your installation:

   - **Development Mode**

   - **Production Mode**

     Production mode gives your environment a higher degree of security, requiring a user name and password to start the Administration Server.

   For more information about startup modes, see "Development vs. Production Mode Default Tuning Values" in *Oracle Fusion Middleware Performance and Tuning for Oracle WebLogic Server*.

2. In the **JDK** area, select the JDK to use for the domain.

By default, the installer selects the JDK that was used when you installed OCECAS. Alternatively, you can specify a different JDK.

3. Click **Next**.

The JDBC Data Sources screen appears.

JDBC Data Sources Screen

In the JDBC Data Sources screen:

1. In the table, select the data source that you want to configure.

The fields at the top of the screen become editable. Most of the fields are pre-populated with information about the data source that was created by the **root.sh** script, and you should not change them.

2. In the **Driver** field, select the driver for your database type from the list.

3. In the **Host Name** field, enter the name of the machine that is hosting your OCECAS database. The default is **localhost**.

4. In the **Password** field, enter the **sdc** user password. The **root.sh** script prompted you for this password during the OCECAS installation process.

5. Accept the default values for all other fields.

6. Click **Next**.

The JDBC Data Sources Test screen appears.

JDBC Data Sources Test Screen

The JDBC Data Sources Test screen automatically tests your data source configurations:

- A green check mark displayed in the **Status** column indicates that the configuration is valid.

- A red circle displayed in the **Status** column indicates a problem.

  The bottom of the screen shows a short error message to help you troubleshoot the problem. Common data source problems include the database or the TNSListener not having been started. Fix the error and click **Test Selected Connections** to test your data source configurations again.

Click **Next** when you are ready to proceed to the next screen.

The Advanced Configuration screen appears.

Advanced Configuration Screen

The Advanced Configuration screen allows you to perform advanced configuration on the listed items. If you approve of the current settings, keep all of the check boxes deselected and click **Next**.

> **Note:** If multiple domains are installed on the same host, you must modify the default Administration Server and Node Manager settings to ensure that their port numbers are unique across all domains on the host.

In the Advanced Configuration screen:

1. Select one or more of the following check boxes.

   ■ Administration Server

   ■ Node Manager

   ■ Managed Servers, Clusters and Coherence

   ■ Deployments and Services

   ■ JMS File Store

2. Click **Next**.

The screens that appear next depend on the check boxes that you selected (see Table 6–1).

Table 6–1   Screens Displayed for Advanced Configuration

Check Box Selected	Screens Displayed
Administration Server	Administration Server Screen
Node Manager	Node Manager Screen
Managed Servers, Clusters and Coherence	Managed Servers Screen Clusters Screen Coherence Clusters Screen Machines Screen Assign Servers to Machines
Deployments and Services	Deployments Targeting Screen Services Targeting Screen
JMS File Store	JMS File Stores Screen

Administration Server Screen

In the Administration Server screen:

1. In the **Server Name** field, enter the name of your Administration Server.

2. In the **Listen Address** list, select an explicit listener address for your Administration Server. Using an explicit listener address enables your machines to communicate with each other when the Coherence Cluster uses the default cluster mode.

3. In the **Listen Port** field, enter a port number to use as a listening port for the Administration Server. If you have multiple domains on the machine, you must assign a unique port number for each domain.

4. Select the **Enable SSL** check box.

5. In the **SSL Listen Port** field, enter the port number to use for secure requests. The default is **7002**.

6. Click **Next**.

Node Manager Screen

In the Node Manager screen:

1. In the **Node Manager Type** area, select one of the following:

   ■ **Per Domain Default Location**. If you select this option, the Node Manager home is predefined within the domain as *DomainName*/**nodemanager** and you

cannot edit the Node Manager home. The Node Manager for each domain can have a different configuration, as determined by the files in this directory. This is the default.

- **Per Domain Custom Location**. If you select this option, the Node Manager configuration files are created in a specific location for this domain. Specify the directory in the **Node Manager Home** field, or click **Browse** to navigate to the location. The specified directory must be empty. The **nodemanager.properties** and **nodemanager.domains** files are created in this directory.

- **Manual Node Manager Setup**. If you select this option, Node Manager configuration for the domain is skipped. You must manually create and update the Node Manager configuration for the domain.

2. In the **Node Manager Credentials** area, enter the user name and password that is used to start the specified Node Manager.

3. Click **Next**.

Managed Servers Screen

Add or change connection information for your managed servers. You can add server instances now by clicking the **Add** or **Clone** buttons or add them later by using the Administration Console.

In the Managed Servers screen:

1. In the **Server Name** field, enter the name of the managed server.

2. In the **Listen Address** list, select an explicit listener address for your managed server. Using an explicit listener address enables your machines to communicate with each other when the Coherence Cluster uses the default cluster mode.

   The values for the listener address can include alphanumeric characters, dots [.], and dashes [-] only.

3. In the **Listen Port** field, enter a port number to use as a listening port for the managed server.

4. Select the **Enable SSL** check box and enter the port number to use for secure requests.

5. Click **Next**.

Clusters Screen

Clusters enable you to group managed servers such that they operate as a single unit for hosting applications and resources. You can add clusters by clicking the **Add** button.

In the Clusters screen:

1. In the **Cluster Name** field, enter the name of the cluster. The name of the cluster must be unique among all component names within the domain.

2. In the **Cluster Address** field, enter the addresses for identifying the managed servers in the clusters.

3. In the **Frontend Host** field, enter the IP address of the frontend host for the cluster.

4. In the **Frontend HTTP Port** field, enter the plain port (HTTP) of the frontend host for the cluster.

5. In the **Frontend HTTPS** field, enter the secure port (HTTPS) of the frontend host for the cluster.

6. Click **Next**.

Coherence Clusters Screen

In the Coherence Clusters screen:

1. In the **Cluster Name** field, enter the name of the Coherence cluster.

2. In the **Unicast Listen Port** field, enter the port number to use as the Coherence cluster unicast listen port.

3. Click **Next**.

Machines Screen

Add or change information about the machines in your OCECAS system. In the context of WebLogic Server, a machine is the logical representation of the system that hosts one or more WebLogic Server instances, for the purposes of starting and stopping remote servers using the Node Manager. In a domain, machine definitions identify a particular, physical piece of hardware and are used to associate a computer with the managed servers it hosts.

In the Machines screen:

1. Select the **Unix Machine** tab.

2. To add machines to your OCECAS system, click **Add**.

3. In the **Name** field, enter the name of the machine.

   The name does not have to match the network name for the machine. However, the name must be unique among all component names within the domain.

4. To enable a server running on this machine to bind to a UNIX group ID (GID) after it finishes all privileged startup actions, select the **Enable Post Bind GID** check box and enter the GID in the **Post Bind GID** field.

5. To enable a server running on this machine to bind to a UNIX user ID (UID) after it finishes all privileged startup actions, select the **Enable Post Bind UID** check box and enter the UID in the **Post Bind UID** field.

6. In the **Node Manager Listen Address** list, select the address that Node Manager uses to listen for connection requests.

7. In the **Node Manager Listen Port** list, select the port that Node Manager uses to listen for connection requests.

8. Click **Next**.

Assign Servers to Machines

Assign WebLogic Server instances to the machines that you defined in the previous screen.

In the Assign Servers to Machines screen:

1. In the **Servers** pane, select the WebLogic Server instance.

2. In the **Machines** pane, select the machine to which you want to assign a WebLogic Server instance.

3. Click the right arrow button.

4. Click **Next**.

Deployments Targeting Screen

Target applications and libraries for deployment on your server or cluster.

In the Deployments Targeting screen:

1. In the **Deployments** pane, select one or more applications to deploy.

2. In the **Targets** pane, select the cluster or server on which to deploy the application.

3. Click the right arrow button.

4. Click **Next**.

Services Targeting Screen

Target services for deployment on managed servers or clusters.

In the Services Targeting screen:

1. In the **Services** pane, select one or more services to deploy.

2. In the **Targets** pane, select the cluster or server on which to deploy the service.

3. Click the right arrow button.

4. Click **Next**.

JMS File Stores Screen

A JMS file store is a disk-based file in which persistent messages are stored.

In the JMS File Stores screen:

1. In the **Name** field, enter the name for the JMS file.

2. In the **Directory** field, enter the path of the directory in which to store the JMS file.

3. In the **Synchronous Write Policy** list, select how the file store writes data to the disk.

4. Click **Next**.

Configuration Summary Screen

The Configuration Summary screen lists the detailed configuration settings of your domain.

Click **Create** to accept the domain details and to start creating the domain.

Configuration Progress Screen

The Configuration Progress screen displays a progress bar that indicates the status of the configuration process.

After the domain is created successfully, click **Next**.

Configuration Success Screen

The Configuration Success screen displays the name of your domain, the path to the domain files, and the URL for accessing the Administration Console.

Click **Finish** to end your configuration session.

Next Steps

After you create your OCECAS domains, you must complete OCECAS post-installation tasks, such as:

- Performing post-configuration tasks for your management domain
- Performing post-configuration tasks for your runtime domains
- Performing post-configuration tasks for your UDR domains

See "OCECAS Post-Installation Tasks" for instructions.

7

OCECAS Post-Installation Tasks

This chapter provides instructions for Oracle Communications Evolved Communications Application Server (OCECAS) post-installation tasks.

Before continuing, complete the tasks in the following chapters:

- Installing OCECAS
- Creating and Configuring OCECAS Domains

Overview of OCECAS Post-Installation Tasks

After installing OCECAS and creating your domains, perform the following tasks:

1. Set up your OCECAS system for subscriber data. See "Setting up OCECAS for Subscriber Data".

2. Perform post-configuration tasks for your OCECAS domains:
   - Management domain. See "Post-Configuration Tasks for Your Management Domain".
   - Runtime domains. See "Post-Configuration Tasks for Your Runtime Domains".
   - UDR domains. See "Post-Configuration Tasks for Your UDR Domains".

3. Start your WebLogic Server administration and managed servers. See "Starting WebLogic Server Administration and Managed Servers".

4. Create users for the Session Design Center (SDC) GUI. See "Creating Users for the SDC GUI".

5. Configure authentication. See "Configuring Authentication".

6. Configure SSL host name verification. See "Configuring SSL Hostname Verification".

7. Configure the Coherence security framework. See "Configuring the Coherence Security Framework".

Setting up OCECAS for Subscriber Data

OCECAS can retrieve subscriber data from an ECAS subscriber server (ESS), a local NoSQL database often used in combination with a home subscriber server (HSS). Both can serve as subscriber data stores, and you may also use both and federate the data between them.

The instructions in this section apply whether you are using the UDR domain, or just adding the NoSQL database to a runtime domain.

These tasks are required to obtain data from the ESS NoSQL database:

- To install an OCECAS ESS by creating the NoSQL database in each runtime domain, see "Creating an ESS NoSQL Database".

- To install the NoSQL client driver in each domain, see "Installing the ESS NoSQL Client Driver".

For more information about:

- Using, changing, and provisioning the OCECAS data stores, see "Working with User Data Repositories" in *Evolved Communications Application Server Services Guide*.

- The NoSQL database software, see the Oracle NoSQL Database 12c Release1 web site:

  http://docs.oracle.com/cd/NOSQL/html/index.html

- Securing your NoSQL database, see "Securing the NoSQL Database" in *Evolved Communications Application Server Security Guide*.

- NoSQL databases, see *Oracle NoSQL Database Administrator's Guide 12c*.

Creating an ESS NoSQL Database

To store subscriber data in an ESS, create a NoSQL database on each machine that hosts an OCECAS runtime domain.

To see the list of supported NoSQL database software versions, see "Database Software".

To create a NoSQL database:

1. Log in to the target machine as the **ocecas** user. See "Creating a UNIX User for Installing OCECAS".

2. Download the Oracle NoSQL Database, Community Edition software from the Oracle Technology Network web site:

   http://www.oracle.com/technetwork/database/database-technologies/nosqld
   b/downloads/nosql-downloads-1876643.html

3. Go to the directory where you downloaded the software, and unpack the archive file by entering the following command:

   ```
   tar xfz kv-ce-3.0.14.gz
   ```

   The **kv-3.0.14** subdirectory is created.

4. Verify the installation by going to the **kv-3.0.14** directory and entering the following command:

   ```
   java -Xmx256m -Xms256m -jar lib/kvclient.jar
   ```

   If installation was successful, you see something similar to the following:

   ```
   12cR1.3.0.14 2013-11-11 12:09:35 UTC Build id: 912c25300b5e
   ```

5. For each runtime domain on your machine, copy the **kvclient.jar** file from the **kv-3.0.14/lib** directory to the *Domain_home*/**lib** directory:

   ```
   cp kv-3.0.14/lib/kvclient.jar Domain_home/lib
   ```

6. Create your NoSQL database by running **kvstore.jar**. For example, to create and run a NoSQL database for testing purposes, enter the following command:

```
nohup java -jar kv-3.0.14/lib/kvstore.jar kvlite -host Hostname -store spr.data
> nosql.log 2>&1 &
```

where *Hostname* is the name of the machine that is hosting your NoSQL database.

For more information, see "Installing Oracle NoSQL Database" in *Oracle NoSQL Database Administrator's Guide*.

Installing the ESS NoSQL Client Driver

To obtain subscriber data from your ESS, you must install the NoSQL Client driver on each machine that hosts an OCECAS runtime domain, and modify the UDR view to query data directly from your HSS.

For details about the default view that OCECAS uses to configure subscriber data, see "Understanding How OCECAS Stores Subscriber Data" in *Enhanced Communications Application Services Service Guide*.

To see the list of supported NoSQL software versions, see "Database Software".

To install a NoSQL client driver:

1. Log in to the target machine as the **ocecas** user. See "Creating a UNIX User for Installing OCECAS".

2. Download the Oracle NoSQL Client Driver software from the Oracle Help Center website:

   http://www.oracle.com/technetwork/database/database-technologies/nosqld
   b/downloads/index.html

3. Go to the directory where you downloaded the software, and unpack the archive file by entering the following command:

   tar xfz kv-client-3.0.14.gz

   The **kv-3.0.14** subdirectory is created.

4. Verify the installation by going to the **kv-3.0.14** directory and entering the following command:

   java -Xmx256m -Xms256m -jar lib/kvclient.jar

   If installation was successful, you see something similar to the following:

   ```
   12cR1.3.0.14 2013-11-11 12:09:35 UTC Build id: 912c25300b5e
   ```

5. For each domain on your machine, copy the **kvclient.jar** file from the **kv-3.0.14/lib** directory to the *Domain_home***/lib** directory:

   cp kv-3.0.14/lib/kvclient.jar *Domain_home*/lib

6. Modify the view to query data directly from your ESS NoSQL database.

Post-Configuration Tasks for Your Management Domain

You must perform post-configuration tasks on the machine that hosts your management domain, such as running the **setDomainEnv.sh** and **disableBasicAuth.py** scripts. These scripts automatically:

- Set your environment
- Disable basic authentication
- Create the **EvolvedCommunicationUsers** group. All user accounts that you create for the SDC GUI must belong to this group.

To configure your management domain:

1. Log in to the machine that hosts the management domain.

2. Go to the *Domain_home* directory.

3. Enter the following command:

   `. bin/setDomainEnv.sh`

4. Enter one of the following commands:

   - For t3s connections:

     `java -Dweblogic.security.TrustKeyStore=DemoTrust`
     `-Dweblogic.security.SSL.protocolVersion=TLS1 weblogic.WLST`
     `bin/disableBasicAuth.py` *`admin_username`* **`'`***`admin_password`***`'`**
     `t3s://`*`hostname:admin_SSL_port domain_name`*

   - For t3 connections:

     `java weblogic.WLST bin/disableBasicAuth.py` *`admin_username`*
     `'admin_password'` **`t3://`***`hostname:admin_listen_port domain_name`*

   where:

   - *hostname* specifies the host name or IP address of the machine that hosts the management domain.
   - *admin_listen_port* references the Administration Server plain listen port.
   - *admin_SSL_port* specifies the number for the Administration Server SSL listen port. You configured the SSL port number in the "Administrator Account Screen".
   - *domain_name* specifies the name of your management domain. You specified the domain name in the "Configuration Type Screen" of the Domain Configuration Wizard.

Post-Configuration Tasks for Your Runtime Domains

You must perform the following configuration tasks on the machine that hosts your testing, staging, and production domains:

- Configure your runtime domains to communicate with the UDR
- Configure the JMS Store-and-Forward system

Configuring Communication Between Your Runtime Domains and the UDR

These instructions explain how to configure communication between a runtime domain and the default NoSQL database as an ESS.

To configure communication between a runtime domain and the default NoSQL ESS:

1. Log in to the target machine.

2. Go to the *Domain_home*/**lib** directory.

3. Create a link to the NoSQL **kvclient jar** file. For example:

```
ln -s NoSQL_home/lib/kvclient.jar ./kvclient.jar
```

where *NoSQL_home* is the directory in which you installed the NoSQL client driver or installed the NoSQL database software. See "Setting up OCECAS for Subscriber Data" for more information.

4. Go to the *Domain_home*/**config/custom** directory.

5. Open the **csp.xml** file in a text editor.

6. Configure an `<adapter>` element to specify the ESS NoSQL database. The default database name is nosql1, and is of type **NoSQLProvicerFactory**. You can use these default values or change them for your implementation.

   - `<name>` is set to a name for the database.

   - `<helper-host>` is set to the host IP address and port number for your NoSQL database.

   - `<store-name>` is set to **spr.data**.

```
<adapters>
    <no-sql-adapter>
      <name>nosql1</name>
      <helper-host>IP_address:port_no</helper-host>
      <store-name>spr.data</store-name>
    </no-sql-adapter>
  </adapters>
```

7. Save and close the file.

8. Restart this domain to make your changes take effect.

> **Note:** Your ESS requires more configuration to work. For details, see "Advanced Configuration of Your ESS Subscriber Data Store" in *Enhanced Communications Application Server Operator's Guide*.

Configuring the JMS Store-and-Forward System on Your Runtime Domains

You must configure a JMS Store-and-Forward (SAF) system for each runtime domain, which includes creating the following:

- A Store-and-Forward (SAF) agent

- A persistent store for each SCF engine in your domain

- A JMS module, which includes:

  – A connection factory resource

  – An SAF remote context

  – An SAF imported destination

  – A subdeployment

The following instructions assume that your OCECAS system contains two SCF engines (**engine1** and **engine2**) and that your management domain's SDC server is listening on SSL port **6002**.

To configure the JMS SAF system:

1. Start your OCECAS servers if they are not already running. See "Starting WebLogic Server Administration and Managed Servers" for more information.

2. Navigate to the Administration Console and log in with your administrator user name and password:

   ```
   http://hostname:port/console
   ```

   where *hostname* is the name of your OCECAS server and *port* is the Administration Console access port number.

3. Create the persistent stores by performing the following steps:

   a. In the Domain Structure pane on the left side, expand **Services** and then click **Persistent Stores**.

      The Summary of Persistent Stores page appears.

   b. In the **Persistent Stores** table, click **New** and then click **Create FileStore**.

      The Create a New File Store page appears.

   c. In the **Name** field, enter **scfEdrSafPersistentStore-Engine1**.

   d. From the **Target** list, select **engine1**.

   e. In the **Directory** field, enter *Domain_home***/saf_edr/engine1/jmsStore**.

   f. Click **OK**.

   g. In the **Persistent Stores** table, click **New** and then click **Create FileStore**.

      The Create a New File Store page appears.

   h. In the **Name** field, enter **scfEdrSafPersistentStore-Engine2**.

   i. From the **Target** list, select **engine2**.

   j. In the **Directory** field, enter *Domain_home***/saf_edr/engine2/jmsStore**.

   k. Click **OK**.

4. Create the JMS module by performing the following steps:

   a. In the Domain Structure pane on the left side, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

      The Summary of JMS Modules page appears.

   b. Click **New**.

      The Create JMS System Module page appears.

   c. In the **Name** field, enter **scfEdrGeneration**.

   d. In the **Descriptor File Name** field, enter **/jms/scfedrgeneration-jms.xml**.

   e. Click **Next**.

   f. Select the **BEA_ENGINE_TIER_CLUST** check box.

   g. Select the **All servers in the cluster** option.

   h. Click **Next**.

   i. Select the **Would you like to add resources to this JMS system module?** check box.

   j. Click **Finish**.

      You are returned to the Settings for scfEdrGeneration page.

5. Create the Connection Factory by performing the following steps:

   a. In the **Summary of Resources** table, click **New**.

     The Create a New JMS System Module Resource page appears.

   b. Select the **Connection Factory** option, and then click **Next**.

   c. In the **Name** field, enter **scfEdrGeneration_CFactory**.

   d. In the **JNDI** field, enter **/scf/jms/edr/qcon/edr_cf**.

   e. Click **Next**.

   f. Select the **BEA_ENGINE_TIER_CLUST** check box.

   g. Select the **All servers in the cluster** option.

   h. Click **Finish**.

     You are returned to the Settings for scfEdrGeneration page.

6. Create the SAF remote context:

   a. In the **Summary of Resources** table, click **New**.

     The Create a New JMS System Module Resource page appears.

   b. Select the **Remote SAF Context** option, and then click **Next**.

   c. In the **Name** field, enter **/scfEdrSafRemoteContext**.

   d. In the **URL** field, enter **t3s://**_hostname_**:6002**.

   e. In the **User Name** field, enter the user name used to log in to the remote resource.

   f. In the **Password** field, enter the password used to log in to the remote resource.

   g. Click **OK**.

     You are returned to the Settings for scfEdrGeneration page.

7. Create the SAF imported destination:

   a. In the **Summary of Resources** table, click **New**.

     The Create a New JMS System Module Resource page appears.

   b. Select the **SAF Imported Destinations** option, and then click **Next**.

   c. In the **Name** field, enter **scfEdrSafRemoteImportedDestination**.

   d. In the **JNDI Prefix** field, enter **/scf/jms/saf/importedDestination**.

   e. In the **Remote SAF Context** field, enter **scfEdrSafRemoteContext**.

   f. Click **Next**.

   g. Select the **BEA_ENGINE_TIER_CLUST** check box.

   h. Select the **All servers in the cluster** option.

   i. Click **Finish**.

     You are returned to the Settings for scfEdrGeneration page.

   j. In the **Summary of Resources** table, click **scfEdrSafRemoteImportedDestination**.

     The Settings for scfEdrSafRemoteImportedDestination page appears.

     k.   Click the **Configuration** tab, and then click the **Queues** subtab.

     l.   Click **New**.

        The Create a New SAF Queue page appears.

     m. In the **Name** field, enter **scfEdrGenerationSAF_Q**.

     n. In the **Remote JNDI Name** field, enter **/jms/edr/edr_q/Local**.

     o. Click **OK**.

        You are returned to the Settings for scfEdrGenerationSAF_Q page.

     p. In the **SAF Queues** table, click **scfEdrGenerationSAF_Q**.

     q. In the Local JNDI Name field, enter **/Local**.

     r. Click **Save**.

        You are returned to the Settings for scfEdrGenerationSAF_Q page.

8. Create the SAF agents by performing the following steps:

     a. In the Domain Structure pane on the left side, expand **Services**, then expand **Messaging**, and then click **Store-and-Forward Agents**.

        The Summary of Store-and-Forward Agents page appears.

     b. Click **New**.

        The Create a New Store-and-Forward Agents page appears.

     c. In the **Name** field, enter **scfEdrSafAgent-Engine1**.

     d. From the **Persistent Store** list, select **scfEdrSafPersistentStore-Engine1**.

     e. From the **Agent Type** list, select **sending-only**.

     f. Click **Next**.

     g. From the **Target** list, select **engine1**.

     h. Click **Finish**.

        You are returned to the Summary of Store-and-Forward Agents page.

     i. In the **Name** field, enter **scfEdrSafAgent-Engine2**.

     j. From the **Persistent Store** list, select **scfEdrSafPersistentStore-Engine2**.

     k. From the **Agent Type** list, select **sending-only**.

     l. Click **Next**.

     m. From the **Target** list, select **engine2**.

     n. Click **Finish**.

9. Create a subdeployment by performing the following steps:

     a. In the Domain Structure pane on the left side, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

        The Summary of JMS Modules page appears.

     b. In the JMS Modules table, click **scfEdrGeneration**.

        The Settings for sdcEdrGeneration page appears.

     c. Click the **Subdeployments** tab.

     d. Click **New**.

The Create a New Subdeployment page appears.

e. In the **Subdeployment Name** field, enter **scfEdrGeneration_SD**.

f. Click **Next**.

g. Select the **scfEdrSafAgent-Engine1** and **scfEdrSafAgent-Engine2** check boxes.

h. Click **Finish**.

Post-Configuration Tasks for Your UDR Domains

You must perform the following configuration tasks on the machine that hosts your UDR domains:

- Disable basic authentication
- Configure your UDR domains to communicate with the UDR
- Configure the JMS Store-and-Forward system

Disabling Basic Authentication

You must run the **setDomainEnv.sh** and **disableBasicAuth.py** scripts, which automatically:

- Disable basic authentication
- Create the **EvolvedCommunicationUsers** group. All user accounts that you create for the SDC GUI must belong to this group.

To disable basic authentication and create the **EvolvedCommunicationUsers** group:

1. Log in to the machine that hosts the UDR domain.

2. Go to the *Domain_home* directory.

3. Enter the following command:

```
. bin/setDomainEnv.sh
```

4. Enter one of the following commands:

- For t3s connections:

  ```
  java -Dweblogic.security.TrustKeyStore=DemoTrust
  -Dweblogic.security.SSL.protocolVersion=TLS1 weblogic.WLST
  bin/disableBasicAuth.py admin_username 'admin_password'
  t3s://hostname:admin_SSL_port domain_name
  ```

- For t3 connections:

  ```
  java weblogic.WLST bin/disableBasicAuth.py admin_username
  'admin_password' t3://hostname:admin_listen_port domain_name
  ```

where:

- *hostname* specifies the host name or IP address of the machine that hosts the UDR domain.
- *admin_listen_port* references the Administration Server plain listen port.
- *admin_SSL_port* specifies the number for the Administration Server SSL listen port. You configured the SSL port number in the "Administrator Account Screen".

- *domain_name* specifies the name of your UDR domain. You specified the domain name in the "Configuration Type Screen" of the Domain Configuration Wizard.

Configuring Communication Between Your UDR Domain and the UDR

To configure communication:

1. Log in to the target machine.

2. Go to the *Domain_home*/**lib** directory.

3. Create a link to the NoSQL **kvclient jar** file. For example:

```
ln -s NoSQL_home/lib/kvclient.jar ./kvclient.jar
```

where *NoSQL_home* is the directory in which you installed the NoSQL client driver or installed the NoSQL database software. See "Setting up OCECAS for Subscriber Data" for more information.

4. Go to the *Domain_home*/**config/custom** directory.

5. Open the **csp.xml** file in a text editor.

6. Ensure that the following elements are set correctly:

    - **name** is set to the correct name.

    - **helper-host** is set to the correct host IP address and port number for your NoSQL database.

    - **store-name** is set to **spr.data**.

```
<adapters>
    <no-sql-adapter>
      <name>nosql1</name>
      <helper-host>IP_address:port_no</helper-host>
      <store-name>spr.data</store-name>
    </no-sql-adapter>
  </adapters>
```

7. Save and close the file.

Configuring the JMS Store-and-Forward System on Your UDR Domains

You must configure a JMS SAF system for each UDR domain, which includes creating the following:

- An SAF agent
- A persistent store for each SCF engine in your domain
- A JMS module, which includes:
    - A connection factory resource
    - An SAF remote context
    - An SAF imported destination
    - A subdeployment

The following instructions assume that your OCECAS system only contains the default UDR (**udr1**)) and that your management domain's SDC server is listening on SSL port **6002**.

To configure the JMS SAF system:

1. Start your OCECAS servers if they are not already running. See "Starting WebLogic Server Administration and Managed Servers" for more information.

2. Navigate to the Administration Console and log in with your administrator user name and password:

   ```
   http://hostname:port/console
   ```

   where *hostname* is the name of your OCECAS server and *port* is the Administration Console access port number.

3. Create the persistent stores by performing the following steps:

   a. In the Domain Structure pane on the left side, expand **Services** and then click **Persistent Stores**.

      The Summary of Persistent Stores page appears.

   b. In the **Persistent Stores** table, click **New** and then click **Create FileStore**.

      The Create a New File Store page appears.

   c. In the **Name** field, enter **udrEdrSafPersistentStore-udr1**.

   d. From the **Target** list, select **udr1**.

   e. In the **Directory** field, enter *Domain_home***/saf_edr/udr1/jmsStore**.

   f. Click **OK**.

4. Create the JMS module by performing the following steps:

   a. In the Domain Structure pane on the left side, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

      The Summary of JMS Modules page appears.

   b. Click **New**.

      The Create JMS System Module page appears.

   c. In the **Name** field, enter **udrEdrGeneration**.

   d. In the **Descriptor File Name** field, enter **/jms/udredrgeneration-jms.xml**.

   e. Click **Next**.

   f. Select the **BEA_UDR_TIER_CLUST** check box.

   g. Select the **All servers in the cluster** option.

   h. Click **Next**.

   i. Select the **Would you like to add resources to this JMS system module?** check box.

   j. Click **Finish**.

      You are returned to the Settings for udrEdrGeneration page.

5. Create the Connection Factory by performing the following steps:

   a. In the **Summary of Resources** table, click **New**.

      The Create a New JMS System Module Resource page appears.

   b. Select the **Connection Factory** option, and then click **Next**.

   c. In the **Name** field, enter **udrEdrGeneration_CFactory**.

    d. In the **JNDI** field, enter **/jms/edr/qcon/edr_cf**.

    e. Click **Next**.

    f. Select the **BEA_ENGINE_TIER_CLUST** check box.

    g. Select the **All servers in the cluster** option.

    h. Click **Finish**.

       You are returned to the Settings for udrEdrGeneration page.

6. Create the SAF remote context:

    a. In the **Summary of Resources** table, click **New**.

       The Create a New JMS System Module Resource page appears.

    b. Select the **Remote SAF Context** option, and then click **Next**.

    c. In the **Name** field, enter **udrEdrSafRemoteContext**.

    d. In the **URL** field, enter **t3s://***hostname***:6002**.

    e. In the **User Name** field, enter the user name used to log in to the remote resource.

    f. In the **Password** field, enter the password used to log in to the remote resource.

    g. Click **OK**.

       You are returned to the Settings for udrEdrGeneration page.

7. Create the SAF imported destination:

    a. In the **Summary of Resources** table, click **New**.

       The Create a New JMS System Module Resource page appears.

    b. Select the **SAF Imported Destinations** option, and then click **Next**.

    c. In the **Name** field, enter **udrEdrSafRemoteImportedDestination**.

    d. In the **JNDI Prefix** field, enter **/jms/edr/edr_q/Local**.

    e. In the **Remote SAF Context** field, enter **udrEdrSafRemoteContext**.

    f. Click **Next**.

    g. Select the **BEA_ENGINE_TIER_CLUST** check box.

    h. Select the **All servers in the cluster** option.

    i. Click **Finish**.

       You are returned to the Settings for udrEdrGeneration page.

    j. In the **Summary of Resources** table, click **udrEdrSafRemoteImportedDestination**.

       The Settings for udrEdrSafRemoteImportedDestination page appears.

    k. Click the **Configuration** tab, and then click the **Queues** subtab.

    l. Click **New**.

       The Create a New SAF Queue page appears.

    m. In the **Name** field, enter **udrEdrGenerationSAF_Q**.

    n. In the **Remote JNDI Name** field, enter **/jms/edr/edr_q/Local**.

    o. Click **OK**.

8. Create the SAF agents by performing the following steps:

    a. In the Domain Structure pane on the left side, expand **Services**, then expand **Messaging**, and then click **Store-and-Forward Agents**.

       The Summary of Store-and-Forward Agents page appears.

    b. Click **New**.

       The Create a New Store-and-Forward Agents page appears.

    c. In the **Name** field, enter **scfEdrSafAgent-Engine1**.

    d. From the **Persistent Store** list, select **udrEdrSafPersistentStore-udr1**.

    e. From the **Agent Type** list, select **sending-only**.

    f. Click **Next**.

    g. From the **Target** list, select **udr1**.

    h. Click **Finish**.

9. Create a subdeployment by performing the following steps:

    a. In the Domain Structure pane on the left side, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

       The Summary of JMS Modules page appears.

    b. In the JMS Modules table, click **scfEdrGeneration**.

       The Settings for sdcEdrGeneration page appears.

    c. Click the **Subdeployments** tab.

    d. Click **New**.

       The Create a New Subdeployment page appears.

    e. In the **Subdeployment Name** field, enter **scfEdrGeneration_SD**.

    f. Click **Next**.

    g. Select the **scfEdrSafAgent-Engine1** and **scfEdrSafAgent-Engine2** check boxes.

    h. Click **Finish**.

Starting WebLogic Server Administration and Managed Servers

After installing and configuring the domains, start the necessary servers on each domain:

- Starting the Administration Server
- Starting Node Manager
- Starting Your Managed Servers

Starting the Administration Server

To start the Administration Server:

1. Log in to the target system.

2. Go to the *Domain_home*/**bin** directory.

3. Enter the following command:

   `./startWebLogic.sh`

4. If your domain uses a production startup mode, you are prompted for the login credentials of the Administrator user.

   You can create a boot identity file to bypass the need to provide a user name and password when starting the Administration Server in production mode. For more information, see "Creating a Boot Identity File for an Administration Server" in *Oracle Fusion Middleware Administering Server Startup and Shutdown for Oracle WebLogic Server*.

For more information about starting the Administration Server, see "Starting and Stopping Administration Server" in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

Starting Node Manager

To start Node Manager:

1. Log in to the target system.

2. Go to the *Domain_home*/**bin** directory.

3. Enter the following command:

   `nohup ./startNodeManager.sh > nm.out&`

Oracle recommends that you install Node Manager to run as a startup service, which allows Node Manager to start up automatically each time the system restarts. For more information about installing a per domain Node Manager service, see "Running Node Manager as a Startup Service" in *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

Starting Your Managed Servers

Before starting a managed server for the first time, copy the *Domain_home*/**security/SerializedSystemIni.dat** file from the Administration Server to the same directory on each managed server.

To start a managed server:

1. Log in to the target system.

2. Go to the *Domain_home*/**bin** directory.

3. Enter the following command:

   `./startManagedWebLogic.sh` *managed_server_name admin_server_url*

   where:

   - *managed_server_name* is the name of the managed server that you want to start.
   - *admin_server_url* is the full URL of the Administration Server, as provided on the Configuration Success screen.

For more information about starting managed servers, see "Starting and Stopping Managed Servers" in *Administering Oracle Fusion Middleware*.

Creating Users for the SDC GUI

You must create at least one user for logging in to the SDC GUI, but you can create more users to meet system requirements.

For more information about the SDC GUI, see "About the Session Design Center" in *Evolved Communication Application Server Concepts*.

To create a user for the SDC GUI:

1. Log in to the machine that hosts the management domain.

2. Ensure that your Administration Server has been started.

3. Navigate to the Administration Console and log in with your administrator user name and password:

   http://_hostname_**:**_port_**/console**

   where *hostname* is the IP address or name of the machine that hosts your management domain and *port* is the Administration Console access port number for your management domain.

4. In the Domain Structure pane on the left side, click **Security Realms**.

   The Summary of Security Realms page appears.

5. In the **Realms** table, click **myRealm**.

   The Settings for myrealm page appears.

6. Click the **Users and Groups** tab, and then click the **Users** subtab.

7. Click **New**.

   The Create a New User page appears.

8. In the **Name** field, enter the user name for accessing the SDC GUI.

9. In the **Password** and **Confirm Password** fields, enter the password for the SDC GUI user.

10. Click **OK**.

11. In the **Users** table, click the SDC GUI user name that you created in step 8.

    The Settings for *UserName* page appears.

12. Click the **Groups** tab.

13. In the **Available** pane, select **EvolvedCommunicationUsers**.

14. Click the right arrow button to move **EvolvedCommunicationUsers** to the **Chosen** pane.

15. Click **Save**.

16. Restart the Administration Server to make your changes take effect.

Configuring Authentication

Configure OCECAS to provide authentication through an LDAP server or Oracle Identity Manager (OIM). For more information, see "Managing User Entities" in *Evolved Communications Application Server System Administrator's Guide*.

Configuring SSL Hostname Verification

If your installation is configured to use Secure Socket Layer (SSL) support, set the host name verification to **None** by using the WebLogic Server Administration Console.

To configure SSL host name verification:

1. Start your OCECAS Administration Server if it is not already running.

2. Navigate to the WebLogic Server Administration Console, and log in with your administrator user name and password:

   ```
   http://hostname:port/console
   ```

   where *hostname* is the name of your OCECAS server and *port* is the Administration Console access port number.

3. In the Domain Structure pane, expand **Environment**, and then click **Servers**.

4. In the Summary of Servers pane, click the **Configuration** tab.

5. For each of your servers in the **Servers** table, do the following:

   a. Click the server name in the table, for example, **AdminServer**.

   b. In the Settings for *ServerName* pane, click the **SSL** tab.

   c. Expand the **Advanced** settings at the bottom of the pane.

   d. From the **Hostname Verification** list, select **None**.

   e. Click **Save**.

No restart is required after making this change.

Configuring the Coherence Security Framework

If you created a clustered domain, enable the Coherence Security Framework. For instructions, see "Enabling the Oracle Coherence Security Framework" in *Securing Oracle Coherence*.

Next Steps

If you encountered any configuration issues, see "Troubleshooting an OCECAS Installation".

8

Patching OCECAS

This chapter describes how to apply patches to your Oracle Communications Evolved Communications Application Server (OCECAS) system.

About OCECAS Patch Releases

You can develop and maintain a strategy to handle the installation of patch releases so that your customers experience a seamless transition.

Types of Patch Releases

Oracle Communications distributes the following types of OCECAS patches to resolve issues, to resolve any perceived vulnerability in the software, or to improve its overall performance:

- **Patch Set**. A Patch Set is the most comprehensive patch release. It contains the accumulated resolutions and updates in OCECAS from the time of the last general release up to the current Patch Set release. Oracle recommends that you stay up-to-date by installing Patch Sets as soon as they become available.

  OCECAS 7.0 Patch Sets use the release numbering scheme 7.0.0.x, where x is the Patch Set number. For example, the first Patch Set for OCECAS 7.0 would be Evolved Communications Application Server 7.0.0.1.

- **Debug patch**. A debug patch is used to troubleshoot an ongoing issue in your OCECAS system. A debug patch represents a concerted attempt by you and Oracle Technical Support to fix an issue in your OCECAS system. Oracle Technical Support uses debug patches as a tool to extract better data from your OCECAS system as a way of resolving the issue. Therefore, the debug patch may not resolve the issue, and more patches may be required.

  Because debug patches address a single issue, OCECAS numbers them as v1, v2, v3, and so on. Each subsequent version replaces the prior version of the debug patch.

- **Temporary fix**. Temporary fixes are tailored to solve an issue in your OCECAS system. They are urgent, time-sensitive, or critical corrections that solve an issue you are experiencing. You may have to install more patches to make the temporary fix work.

  Because each temporary fix addresses a single issue, OCECAS numbers the fixes as v1, v2, v3, and so on. Each subsequent version replaces the prior version of the temporary fix.

About Patch Content

By default, every patch contains the following items:

- A README file

  The README file for a patch release describes how to install the patch. Additionally, in case you encounter problems while applying the patch, the README describes how you can revert to your current setup by rolling back the patch.

- Software updates to OCECAS

  These updates consist of fixes or debug changes.

At times, the patch includes a subdirectory named **custom**, which contains the following items:

- Additional documentation resources

  For example, the patch may contain the description of a specific fix detailing what configuration settings are required to utilize the fix.

- Manual patching steps

  The patch may target a resource you have modified, such as startup scripts.

About Patch Management In Clustered Environments

If your OCECAS system operates in a clustered environment, review the README file that accompanies the patch. Ensure that you apply the patch to all of the servers. Then, perform a rolling restart unless otherwise stated in the README file.

About OPatch

OPatch is an Oracle-supplied Java-based utility that supports the following tasks:

- Applying a patch
- Rolling back a patch to a previous version
- Listing the installed patches
- Detecting a conflict when applying a patch after previous patches have been applied. It also suggests the best options to resolve a conflict

OPatch requires installation of the Oracle Universal Installer software. It is platform-independent and runs on all supported operating systems.

For more information, see "About OPatch" in *Oracle Fusion Middleware Patching with OPatch*.

Preinstallation Tasks for OPatch

Complete the following tasks before you use OPatch for the first time on your system:

1. Checking Your Environment Variables
2. Verifying the Oracle Universal Installer Inventory
3. Creating a Backup of Your Current OCECAS Installation

For more information about the prerequisite checks for OPatch, see *Oracle Universal Installer and OPatch User's Guide*.

For the latest information about the OPatch utility, the JRE versions, or the Java commands for Linux, or to check for updates and get the latest versions, go to My Oracle Support at:

https://support.oracle.com/

Checking Your Environment Variables

The patch installation process uses the OPatch and ZIP software. Ensure that your system can find and use the software by setting your PATH environment variable to include:

- The *Ocecas_home*/**OPatch** directory

- The ZIP software directory

To confirm that your system can find the OPatch and ZIP software, enter the following at a command prompt:

```
which opatch
which unzip
```

Verifying the Oracle Universal Installer Inventory

To apply patches successfully, OPatch needs access to a valid version of Oracle Universal Installer, a valid Oracle Inventory directory (oraInventory), and a valid version of OPatch. Validate the versions on your system by entering the following command:

opatch lsinventory -oh *Ocecas_home*

This command displays your system's OPatch and Oracle Universal Installer versions and directories, and lists the patches currently installed in *Ocecas_home*. For example, the following shows a sample of the information displayed at the beginning of the output:

```
Oracle Interim Patch Installer version 13.2.0.0.0
Copyright (c) 2015, Oracle Corporation. All rights reserved.

Oracle Home           : Ocecas_home
Central Inventory     : /export/oraInventory
   from               : Ocecas_home/oraInst.loc
OPatch version        : 13.2.0.0.0
OUI Version           : 13.2.0.0.0
Log file location     : Ocecas_home/cfgtoollogs/opatch/opatch2015-6-16_11-16-55AM_
1.log
```

For more information, see "OPatch Utility Reference".

> **Caution:** If the **lsinventory** command errors out, do not proceed further with the patch attempt. Contact Oracle Technical Support to validate and verify the inventory setup.

Creating a Backup of Your Current OCECAS Installation

Before you start any patch operation, back up the contents of the *Ocecas_home* directory. You can back up the contents of *Ocecas_home* by using your preferred method. Use any of the following methods to compress the *Ocecas_home* contents:

- zip

- cp -r

- tar

- cpio

Installing OCECAS Patches

To install an OCECAS patch:

1. Log in to the target system.

2. Download the patch from the My Oracle Support website to a temporary directory:

    https://support.oracle.com/

    The patch archive (*PatchName*.**zip**) is downloaded to your temporary directory.

3. Determine whether you need to stop all servers in your OCECAS system by checking the patch README file.

    The README file explicitly states whether the patch requires you to stop your servers before installing the patch.

4. Create a directory for storing the unpacked patch contents. This document and the patch README file refer to this directory as the *Patch_top* directory.

    > **Note:** Ensure that the *PatchName*.**zip** file is not located inside the *Patch_top* directory.

5. Go to the directory where you downloaded the patch and unpack the patch archive (*PatchName*.**zip**) into the *Patch_top* directory.

    The *PatchName* subdirectory is created.

6. Go to the *Patch_top*/*PatchName* directory.

7. Run the OPatch utility by entering the following at a command prompt:

    opatch apply -oh *Ocecas_home*

    OPatch validates the patch and makes sure that there are no conflicts with the software already installed in *Ocecas_home* before applying the patch to your OCECAS system.

    For more information, see "OPatch Utility Reference" and "Dealing with Conflicts When You Run the Apply Command".

8. Verify that the patch installed successfully by running the following command:

    opatch lsinventory -oh *Ocecas_home*

    For more information, see "OPatch Utility Reference".

9. Determine whether you need to restart all servers in your OCECAS system or perform other tasks by checking the patch README file.

    The patch README file explicitly states whether the patch requires you to restart your servers or to perform other tasks after installing the patch.

If you encounter any issues in any of these steps, see "Troubleshooting".

Troubleshooting

OPatch is reliable and protects *Ocecas_home* and the inventory. It can bring back the contents of the *Ocecas_home* directory to a stable state from patch application failures. It can also easily detect patch conflicts.

OPatch logs information to a **.log** file. Here is an example entry:

```
Log file location : /home/oracle_
TEST/product/11.1.0/db1/cfgtoollogs/opatch/opatch-yyyy_month_dd_HH-MM-SS-IST_
Wed.log
```

If you encountered errors while installing a patch and you need assistance from Oracle Technical Support, be sure to provide the associated log file together with the patch command you used to install the patch.

Handling Java Errors

When you run the OPatch utility, you may receive the following error message:

```
Exception in thread "main"
java.lang.UnsupportedClassVersionError:com/oracle/cie/gdr/external/InventoryExcept
ion : Unsupported major.minor
```

This occurs because OPatch cannot locate the correct version of the JDK. For supported JDK versions, see "Software Requirements". To fix this error, include the **-jre** option when you run the OPatch utility from the command line. For example, if the JDK files are located in *Path***/jre1.8.0_31**, enter the following command to apply a patch:

opatch apply -oh *Ocecas_home* **-jre** *Path***/jre1.8.0_31**

Handling OPatch and OUI Version Errors

When you run the OPatch utility, you may receive the following message:

```
OPatch Version : 13.2.0.0.0
OUI Version : 12.1.0.1.0
The OPatch version is not applicable for current OUI version.
```

This occurs because OPatch cannot locate the correct version of the OUI libraries. To fix this error, include the **-oui_loc** option when you run the OPatch utility from the command line. For example, if the OUI files are located in *Path***/oui**, enter the following command to apply a patch:

opatch apply -oh *Ocecas_home* **-oui_loc** *Path***/oui**

Dealing with Conflicts When You Run the Apply Command

When you run the OPatch **apply** command, you may encounter the following conflicts:

- Conflict with a patch already applied to the contents of the *Ocecas_home* directory.

  In this case, stop the patch installation and contact Oracle Technical Support.

- Conflicts with a subset patch already applied to the contents of the *Ocecas_home* directory.

  In this case, continue the installation, because the new patch contains all of the fixes from the existing patch. The subset patch is automatically rolled back before the installation of the new patch.

Uninstalling the Patch

If you experience any problems after installing a patch, remove the patch.

To uninstall the patch:

1. Stop all servers in your OCECAS system.

2. Roll back the patch with the following command:

   opatch -oh *Ocecas_home* **rollback -id** *PatchNumber*

   where *PatchNumber* is the patch number. For more information, see "OPatch Utility Reference".

If you need further assistance, contact Oracle Technical Support with the required information.

OPatch Utility Reference

By default, the OPatch utility is located in the *Ocecas_home***/OPatch** directory. The following shows the syntax for running the OPatch utility:

```
opatch [-help] [-jre JRE_home] [-oh Ocecas_home] [-oui_loc OUI_home] [-report]
command
```

where:

- **-help** lists the commands and options supported by the utility.

  Use the **-help** option together with a command to view detailed information for the OPatch command. For example:

  ```
  opatch apply -help
  ```

- **-jre** *JRE_home* specifies to use JRE from the specified directory.

- **-oh** *Ocecas_home* specifies to apply the patch to (or roll back the patch from) the product in the specified directory.

- **-oui_loc** *OUI_home* specifies the directory in which Oracle Universal Installer (OUI) resides. By default, the OCECAS installer copies the OUI files to *Ocecas_home***/oui**.

- **-report** prints the actions without executing the command.

- *command* is one of these OPatch commands:

  – **apply** [*PatchDirectory*]

    This command applies the patch from the specified directory to your product. If you do not run the utility from the directory in which the patch content resides (*PatchDirectory*), include the complete path to the directory.

  – **lsinventory**

    This command displays your system's OPatch and Oracle Universal Installer versions and directories, and lists the patches currently installed in *Ocecas_home*. The following shows sample output for the **lsinventory** command:

    ```
    --------------------------------------------------------------------
    Oracle Interim Patch Installer version 13.2.0.0.0
    Copyright (c) 2015, Oracle Corporation. All rights reserved.

    Oracle Home        : Ocecas_home
    ```

```
Central Inventory    : /export/oraInventory
   from              : Ocecas_home/oraInst.loc
OPatch version       : 13.2.0.0.0
OUI Version          : 13.2.0.0.0
Log file location    : Ocecas_home/cfgtoollogs/opatch/opatch2015-6-16_
11-16-55AM_1.log

OPatch detects the Oracle Home as "Ocecas_home"

-----------------------------------------------------------------------
Interim patches (1):

Patch  19836145     : applied on Tue Dec 16 10:51:13 CST 2014
Unique Patch ID      : 1418034883552
Patch description    : "[Patch Set v6.0.0.0.1] - Patch set zero"
   Created on 8 Dec 2015, 02:34:45 hrs PST8PDT
   Bugs fixed:
     123412
-----------------------------------------------------------------------
```

- **rollback -id** *PatchNumber*

  This command removes the specified patch from the product, where *PatchNumber* is the patch number.

  You can find the patch number by using the **lsinventory** command. For example, you would use the command **rollback -id 19836145** to roll back the patch shown in the following sample **lsinventory** output:

```
-----------------------------------------------------------------------
Interim patches (1) :

Patch  19836145     : applied on Tue Dec 16 10:51:13 CST 2014
Unique Patch ID: 1418034883552
Patch description:  "[Patch Set v6.0.0.0.1] - Patch set zero"
   Created on 8 Dec 2014, 02:34:45 hrs PST8PDT
   Bugs fixed:
     123412
-----------------------------------------------------------------------
```

For a full list of the OPatch commands and their descriptions, see "Common OPatch Commands When Patching an Oracle Fusion Middleware Oracle home" in *Oracle Fusion Middleware Patching with OPatch*.

9

Troubleshooting an OCECAS Installation

This chapter describes how to troubleshoot Oracle Communications Evolved Communications Application Server (OCECAS) installations.

Troubleshooting an OCECAS Installation

The OCECAS installer and the Domain Configuration Wizard write information to log files. You can check those log files for information about errors and actions performed during the installation.

About OCECAS Installation Log Files

The OCECAS installation log files can be found at *Central_inventory_location*/**oraInventory/logs**, where *Central_inventory_location* is the directory path to the **oraInventory** directory. If you do not know the location of your Oracle Inventory directory, you can find it in the *Ocecas_home*/**oraInst.loc** file.

The following install log files are written to the log directory:

- *date-time-stamp***install.log**

  This is the main log file.

- **install***date-time-stamp***.out**

  This log file contains the output and error streams during the installation.

- **installProfile***date-time-stamp***.log**

  This log file contains the overall statistics such as the time taken to complete the installation as well as configuration, memory, and CPU details.

- **oraInstall***date-time-stamp***.log**

  This log file contains the output stream of the copy session.

- **oraInstall***date-time-stamp***.err**

  This log file contains the error stream of the copy session.

Changing the Installer Logging Level

To change the logging level, use the **-logLevel** parameter from the command line when you start the installer. For example:

```
java -jar ocecas_generic.jar -logLevel info
```

The following shows valid values for **-logLevel** from most detailed to least detailed:

- **severe**

- **warning**

- **info**

- **config**

You can also specify logging details from detailed to least detailed in the following manner:

- **fine**

- **finer**

- **finest**

OCECAS Domain Configuration Log Files

If you encounter errors when configuring an OCECAS domain, you can start the Fusion Middleware Configuration Wizard with the appropriate logging options.

To enable domain configuration logging, go to *Ocecas_home*/**oracle_ common/common/bin** and start **config.sh** with the **-log** and **-log_priority** options:

./config.sh -log=_log_filename_ **-log_priority=**_log_level_

Table 9–1 lists the **-log** and **-log_priority** options.

Table 9–1   Configuration Wizard Log File Options

Parameter	Description
-log	Specify the location of your log file.
	If you specify a log file name, it is created in the same directory as the **config.sh** script unless you add a path component. Log files are otherwise created in *Ocecas_home*/**logs**.
	Other values that can be specified with **-log** are:
	■ **stdout**
	Writes the error message to the standard output stream.
	■ **stderr**
	Writes the error messages to the standard error stream.
	■ **disable**
	Disables default logging so that no log files are generated in *Ocecas_home*/**logs**.
-Log_priority	Specify the level of detail you want included in your logs.
	The following list shows the acceptable values:
	■ **OFF**
	■ **SEVERE**
	■ **WARNING**
	■ **INFO**
	■ **CONFIG**
	■ **FINE**
	■ **FINER**
	■ **FINEST**

10

Uninstalling OCECAS

This chapter describes how to uninstall Oracle Communications Evolved Communications Application Server (OCECAS) and its components.

Uninstalling OCECAS in GUI Mode

To uninstall OCECAS components in GUI mode, perform the following on each machine in your OCECAS system:

1. Log in to the target system.

2. Manually shut down all services and WebLogic Server.

3. Perform this step only on the machine that hosts your Management Domain:

   Go to the *Ocecas_home* directory, and enter the following command:

   `./root.sh -d remove`

4. Go to the *Ocecas_home*/**oui/bin** directory, and enter the following command:

   `./deinstall.sh`

5. If you have multiple Oracle products installed in your Oracle Inventory directory (oraInventory), the Distribution to Uninstall screen appears.

   Perform the following to specify the Oracle product to uninstall:

   a. From the **Select Distribution to Uninstall** list, select **Evolved Communications Application Server~7.0.0.0.0**.

   b. Click **Uninstall**.

6. From the Welcome screen, click **Next**.

   The Deinstallation Summary screen appears.

7. Verify that the list of feature sets to uninstall is correct.

   To save the information to a response file so you can uninstall the components later, click **Save Response File** and specify the name and location of the response file.

8. Click **Deinstall**.

   The Deinstallation Progress screen appears, and a progress bar indicates the status of the uninstallation process.

9. When the uninstallation process is complete, click **Next**.

   The Deinstallation Complete screen appears.

10. Click **Finish**.

The uninstaller exits.

Uninstalling OCECAS in Silent Mode

Use silent mode to uninstall duplicate installations on multiple machines. In silent mode, you create and use a **response_uninistall.rsp** configuration file, and then specify it as a parameter at the command line. The program does not display any options during the uninstallation process.

To uninstall OCECAS components in silent mode, perform the following on each machine in your OCECAS system:

1. Log in to the target system.

2. Manually shut down all services and WebLogic Server.

3. Create a text file.

4. Add the following contents to your text file:

```
[ENGINE]

#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

#This will be blank when there is nothing to be de-installed in distribution
level
SELECTED_DISTRIBUTION=Evolved Communications Application Server~7.0.0.0.0

#The oracle home location. This can be an existing Oracle Home or a new Oracle
Home
ORACLE_HOME=Ocecas_home
```

where SELECTED_DISTRIBUTION is set to the component to uninstall. This parameter is required only if multiple applications are installed in the Oracle Inventory directory (oraInventory). For OCECAS, set SELECTED_DISTRIBUTION to **Evolved Communications Application Server~7.0.0.0.0**.

5. Save the text file with the name **response_uninstall.rsp**.

6. Perform this step only on the machine that hosts your Management Domain:

Go to the *Ocecas_home* directory, and enter the following command:

./root.sh -d remove

7. Go to the *Ocecas_home*/**oui/bin** directory and enter the following in a command window:

./deinstall.sh -silent -responseFile *ResponseFile*

where *ResponseFile* is the full path and name of the **response_uninstall.rsp** file. For example, *Ocecas_home*/**oui/bin/response_uninstall.rsp**.

The uninstallation process completes with no prompts.

If the uninstallation procedure completes successfully, you see a response similar to the following:

```
Launcher log file is /tmp/OraInstall2015-11-06_01-46-10PM/launcher2015-11-06_
```

```
01-46-10PM.log.
Starting Oracle Universal Installer

Checking if CPU speed is above 300 MHz.   Actual 2893.030 MHz    Passed
Checking swap space: must be greater than 512 MB.   Actual 15826924 MB    Passed
Checking if this platform requires a 64-bit JVM.   Actual 64    Passed (64-bit not
required)
Checking temp space: must be greater than 300 MB.   Actual 136360 MB    Passed


Preparing to launch the Oracle Universal Installer from /tmp/OraInstall2014-11-06_
01-46-10PM
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option MaxPermSize=512m;
support was removed in 8.0
Log: /tmp/OraInstall2014-11-06_01-46-10PM/deinstall2014-11-06_01-46-10PM.log
Setting ORACLE_HOME to /home/oracle/
Copyright (c) 1996, 2015, Oracle and/or its affiliates. All rights reserved.
Starting silent deinstallation...
-----------20%----------40%----------60%----------80%--------100%

The uninstall of Oracle Communications Evolved Communications Application Server
7.0.0.0.0 completed successfully.
Logs successfully copied to /export/oraInventory/logs.
```