

# Oracle® Communications Converged Application Server Installation Guide



Release 8.3

G47662-03

May 2026

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## About this Guide

---

### 1 Components

---

Overview of the Converged Application Server Installation Procedure	1
Ensuring a Successful Installation	2
Placeholders Used in This Guide	2

### 2 Planning Your Installation

---

Understanding Installation Topologies	1
About Converged Application Server Coherence Planning	3
About Installing a Secure System	3

### 3 System Requirements

---

Software Requirements	1
Database Software	1
Middleware Software	1
Virtualization Software	1
About SIP Clients	2
About Critical Patch Updates	2
Hardware Requirements	2
Information Requirements	3

### 4 Pre-Installation Tasks

---

Pre-Installation Tasks for All Converged Application Server Systems	1
General Pre-Installation Tasks	1
Choosing an Installation Directory	1
Installing the Java Development Kit	2

<b>5</b>	<b>Installing Converged Application Server</b>	
	About the GUI Installation and Silent Installation	1
	Installing Converged Application Server Using the GUI Installation	1
	Installing Converged Application Server Using the Silent Installation	3
	About the Response File	3
	Returning Exit Codes to the Console	4
	Running the Installer in Silent Mode	5
<b>6</b>	<b>Creating and Configuring Domains</b>	
	About Domains and Domain Configuration	1
	About Converged Application Server Domain Types	1
	Creating a Converged Application Server Domain	3
	Preconfiguration Steps for Replicated Domains	3
	Starting the Configuration Wizard	4
	Creating a Converged Application Server Domain in Graphical Mode	5
	Configuration Type Screen	5
	Templates Screen	5
	Administrator Account Screen	5
	Domain Mode and JDK Screen	6
	Advanced Configuration Screen	6
	Configuration Summary Screen	10
	Configuration Progress Screen	10
	End Of Configuration Screen	10
	Extend an Existing Non-Diameter Domain	10
	Starting the Servers in Converged Application Server	11
	Starting the Administration Server	11
	Starting the Node Manager	12
	Starting the Managed Servers	12
<b>7</b>	<b>Post-Installation Tasks</b>	
	Overview of Converged Application Server Post-Installation Tasks	1
	Apply Patches	1
	Enabling DNS Server Lookup	1
	Configuring SSL Host Name Verification	2
	Configuring the Coherence Security Framework	2
<b>8</b>	<b>Installing Infrastructure Components</b>	
	Install the Media Flow Engine	1
	Configuring the Media Flow Engine	2

Install the RTP Proxy	3
KVM Configuration	4
Install RTP Proxy	9
Configuring the RTP Proxy	11
Install the Intelligent AI Connector	12

## 9 Migrating or Upgrading

---

About Migrating or Upgrading Converged Application Server	1
High Availability	1
Migrating or Upgrading Converged Application Server	1
Verifying Your Domain Administration Settings	1

## 10 Patching

---

About Converged Application Server Patch Releases	1
Types of Patch Releases	1
About Patch Content	1
About Patch Management In Clustered Environments	2
About OPatch	2
Preinstallation Tasks for OPatch	2
Verifying the Oracle Universal Installer Inventory	2
Creating a Backup of Your Current Converged Application Server Installation	3
Checking Your Environment Variables	3
Installing Converged Application Server Patches	4
Installing the Priority Call Handling Patch	4
Troubleshooting	5
Dealing with Conflicts When You Run the Apply Command	6
Uninstalling the Patch	6
OPatch Utility Reference	6

## 11 Troubleshooting

---

About Troubleshooting Converged Application Server Installations	1
About Converged Application Server Installation Log Files	1
Changing the Installer Logging Level	1
About Domain Configuration Log Files	2
AIC Troubleshooting	3

## 12 Uninstalling

---

Uninstalling Converged Application Server Components in GUI Mode	1
--	---



# About this Guide

**Table 1** Revision History

Date	Description
March 2026	<ul style="list-style-type: none"><li data-bbox="922 579 1110 604">• Initial release</li></ul>
May 2026	<ul style="list-style-type: none"><li data-bbox="922 621 1349 646">• Updates for Intelligent AI Connector</li></ul>

# 1

## Components

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

- Java Development Kit (JDK) software
- The Converged Application Server software, which includes:
  - Oracle WebLogic Server, which is the platform container
  - Oracle Coherence software

## Overview of the Converged Application Server Installation Procedure

The process for installing Converged Application Server is similar to the process for installing WebLogic Server:

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. System requirements include:
  - 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 assigning IP addresses to network assets and installing the JDK.
4. Install Converged Application Server.

When you install Converged Application Server, WebLogic Server and Oracle Coherence are also installed.
5. Configure a Converged Application Server domain.
6. Perform post-installation tasks.
7. Troubleshoot any installation issues.

## Ensuring a Successful Installation

The Converged Application Server installation should be performed only by qualified personnel. You must be familiar with WebLogic Server and the supported operating systems. You should be experienced with installing Java-related packages.

Follow these guidelines:

- As you install each component, 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. You re-enter these configuration values later in the procedure.

## Placeholders Used in This Guide

Placeholders are used in this guide to refer to the directories that contain Converged Application Server system components.

**Table 1-1 Directory Placeholders**

Placeholder	Directory
<i>Central_inventory_location</i>	The directory in which the Oracle inventory file lives. The Oracle inventory lists all Oracle software installed on a machine. This directory is created by the Oracle installer upon the first Oracle product installation.
<i>Domain_home</i>	The directory in which the Converged Application Server domain resides, located in <i>Oracle_Home/user_projects/domains</i> .
<i>Oracle_Home</i>	The directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Converged Application Server and WebLogic Server. The files in the <i>Oracle_Home</i> directory are essential to ensuring that software operates correctly on your system. They: <ul style="list-style-type: none"> <li>• Facilitate checking of cross-product dependencies during installation</li> <li>• Facilitate Service Pack installation</li> </ul>
<i>temp_dir</i>	A temporary directory into which you extract the installation images for Converged Application Server. Referenced when extracting installation files and other utilities.
<i>occas_home</i>	The directory in which the Converged Application Server software is installed. By default, this is a subdirectory of <i>Oracle_Home</i> ; for example, <i>Oracle_Home/occas</i>

# 2

## Planning Your Installation

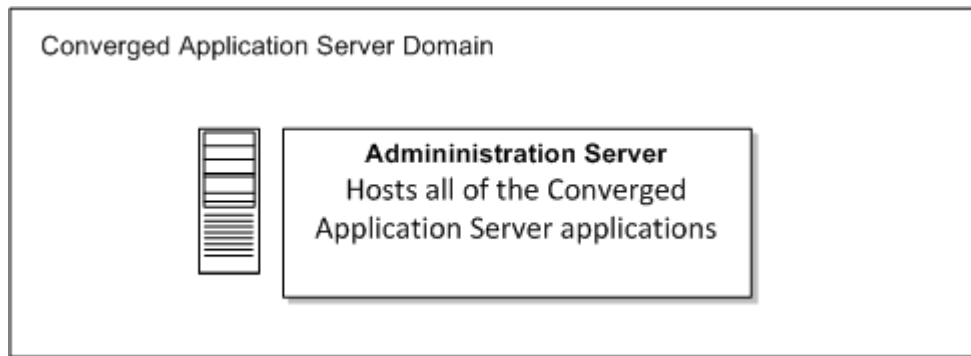
When planning a Converged Application Server installation, consider how many physical servers can handle your subscriber base and how many signaling and media server nodes to include in your cluster.

The difference between a Converged Application Server development system and a Converged Application Server production system is only the number of machines in the system. Install the same components in a development system as installed in a production system.

## Understanding Installation Topologies

A basic Converged Application Server installation topology consists of a domain with a single Administration Server. The Administration Server hosts all of the Converged Application Server applications on a single machine.

**Figure 2-1 Basic Converged Application Server Topology**



While a simple single host configuration is sufficient for development and Proof of Concept (PoC) installations, production systems must be robust and fault-tolerant.

In a fault-tolerant topology, the Administration Server is installed on a separate machine from the independent managed servers, each of which hosts a dedicated instance of Converged Application Server. The managed servers can be separated geographically for extra fault tolerance, and more engines can be added as required.

Figure 2-2 Fault-Tolerant Converged Application Server Topology

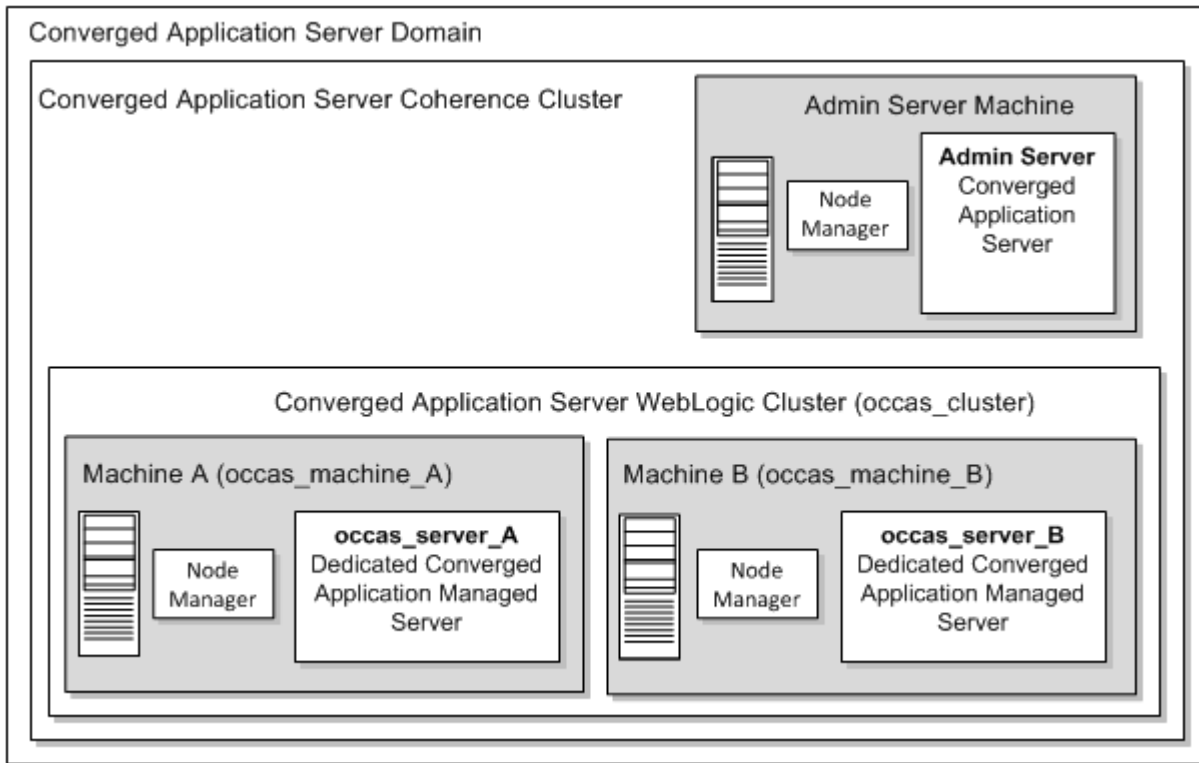


Table 2-1 Elements in the Installation Topology

Element	Description and Links to Additional Documentation
Converged Application Server Domain	A group of logically related Java components (in this case, the Administration Server, managed servers, and other related software components). For more information, see <a href="#">"Understanding Domains"</a> in <i>Understanding Oracle WebLogic Server</i> .
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 <a href="#">"Administration Server"</a> in <i>Understanding Oracle WebLogic Server</i> .
Cluster	A collection of multiple Converged Application Server instances running simultaneously and working together. For more information, see <a href="#">"Managed Servers and Managed Server Clusters"</a> in <i>Understanding Oracle WebLogic Server</i> .
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, Oracle recommends it if your WebLogic Server environment hosts applications with high availability requirements.
Machine	A logical representation of the computer that hosts one or more WebLogic Server instances (servers). Machines are also the logical glue between Converged Application Server 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.

**Table 2-1 (Cont.) Elements in the Installation Topology**

Element	Description and Links to Additional Documentation
Managed Server	The host for your applications, application components, Web services, and their associated resources. For more information, see " <a href="#">Managed Servers and Managed Server Clusters</a> " in <i>Understanding Oracle WebLogic Server</i> .

## About Converged Application Server Coherence Planning

Converged Application Server nodes are based on Oracle Coherence. For optimal performance, determine how to configure Oracle Coherence settings for your Converged Application Server topology. For example, determine the number of servers needed in the cluster and the number of machines deployed to ensure that there are enough servers to accommodate any type of failure, such as server processes, machines, and so on. For more information, see "[Configuring and Managing Coherence Clusters](#)" in *Administering Clusters for Oracle WebLogic Server*.

## 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 *Converged Application Server Security Guide*.

# 3

## System Requirements

This chapter describes the software, hardware, and information requirements for Oracle Communications Converged Application Server.

### Software Requirements

Converged Application Server is supported on the following operating systems, hardware architectures, and JDKs.

Converged Application Server does not support any Open Java Development Kit (OpenJDK).

**Table 3-1 Supported Software**

Components	Operating System	Hardware Architectures	JDK	Additional Information
Converged Application Server 8.3	Oracle Linux 9.6+ or later	x86-64	JDK 17 or JDK 21	Certified on native or VM
Intelligent AI Connector	Oracle Linux 9.6+ or later	x86-64	JDK 25	Certified on native or VM

### Database Software

The Converged Application Server supports any JDBC Type 4 compliant driver.

See [JDBC Data Sources](#) in the *What's New in Oracle WebLogic Server*.

### Middleware Software

Converged Application Server supports the following middleware software.

**Table 3-2 Supported Middleware Software**

Middleware Software	Notes
Oracle WebLogic Server 14.1.2	Oracle WebLogic Server is bundled with the Converged Application Server installer.
Oracle Coherence 14.1.2	Oracle Coherence is bundled with the Converged Application Server installer.

### Virtualization Software

Converged Application Server is supported on the following virtualization software:

- Kernel-based Virtual Machine (KVM) 0.12
- Oracle OVM 3
- VMware ESXi 8

## About SIP Clients

Any standards-compliant Session Initiation Protocol (SIP) User Agent can be used.

## About Critical Patch Updates

Converged Application Server is supported on all Oracle Critical Patch Updates. Install all Critical Patch Updates as soon as possible.

### Warning

The Converged Application Server ships with both Oracle WebLogic Server and Oracle Coherence. Customers must install all Critical Patch Updates for Oracle WebLogic Server and Oracle Coherence.

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

<https://www.oracle.com/security-alerts/>

## Hardware Requirements

The number and configuration of the computers that you employ for your Converged Application Server system depend on the scale and the deployment type you plan. Work with your performance team to determine your sizing requirements.

Converged Application Server 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 between engine servers for most 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.

**Table 3-3 Minimum System Requirements**

Resource	Minimum	Recommended
RAM	8 GB	16 GB or higher
CPU	8 cores	16 cores or higher
Disk space	150 GB	300 GB+
Network	1 Gbps Ethernet	Dedicated production network

**Table 3-4 Network Interface (NIC) Requirements**

Component	Minimum NICs	Recommended NICs	Purpose
Converged Application Server Node	1 NIC	3 NICs	1st NIC for REST/control traffic. 2nd NIC for SIP Signalling traffic. 3rd NIC for dedicated Coherence communication (Optional)
Intelligent AI Connector	1 NIC	2 NICs (dedicated)	One for REST/control traffic, one for media.

## Information Requirements

Installing Converged Application Server requires the following information.

**Table 3-5 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 <i>Oracle_Home</i> directory. It is the directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Converged Application Server and WebLogic Server.	NA
Directory	The directories on each machine in which to install Converged Application Server and WebLogic Server software. By default, these are subdirectories of <i>Oracle_Home</i> .	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

## Pre-Installation Tasks

This chapter describes tasks you must complete before installing Oracle Communications Converged Application Server.

### Pre-Installation Tasks for All Converged Application Server Systems

Before installing the Converged Application Server software, complete the following pre-installation tasks:

- Perform general pre-installation tasks. See "[General Pre-Installation Tasks](#)".
- Choose your Oracle home directory. See "[Choosing an Installation Directory](#)".
- Install JDK on all machines in your Converged Application Server system. See "[Installing the Java Development Kit](#)".

### General Pre-Installation Tasks

Complete the following general pre-installation tasks:

- Allocate IP addresses for Converged Application Server interfaces, including:
  - Public-facing external interfaces
  - Internal-facing interfaces
  - Intra-system interfaces for private signaling between Converged Application Server 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) servers.
- Optionally assign fully qualified domain names to each server.
- Make a note of any required static routes.

### Choosing an Installation Directory

When you install Converged Application Server, you are prompted to specify a *Oracle\_Home* directory. This directory serves as a repository for common files that are used by multiple Fusion Middleware products installed on the same machine. For this reason, the *Oracle\_Home* directory can be considered a central support directory for all of the Fusion Middleware products installed on your system.

The files in the *Oracle\_Home* directory are essential to ensuring that Converged Application Server and WebLogic Server operate correctly on your system. They facilitate checking of cross-product dependencies during installation.

For more information about selecting an installation directory, see *Installing and Configuring Oracle WebLogic Server and Coherence*.

## Installing the Java Development Kit

Install Oracle Java Development Kit (JDK) plus the latest security update on each physical machine or VM in your Converged Application Server system. For a list of supported versions, see [Software Requirements](#).

To install and configure your JDK:

1. Download the JDK from the Java SE Development Kit Downloads page at: <https://www.oracle.com/java/technologies/downloads/#java17>
2. Install the JDK per instructions provided with it.
3. Add the JDK **bin** directory to the beginning of the **PATH** variable definition on the target system. For example:

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

# 5

## Installing Converged Application Server

This chapter describes how to install the Oracle Communications Converged software.

Before you install Converged Application Server, complete all pre-installation tasks described in "[Pre-Installation Tasks](#)".

### About the GUI Installation and Silent Installation

You can install Converged Application Server by using the GUI installation or the silent installation. The silent installation enables you to perform a non-interactive installation of Converged Application Server. You can use the silent installation to install Converged Application Server quickly on multiple systems.

For installation instructions, see the following sections:

- [Installing Converged Application Server Using the GUI Installation](#)
- [Installing Converged Application Server Using the Silent Installation](#)

### Installing Converged Application Server Using the GUI Installation

To run the installation program in graphical mode, the console attached to the machine on which you are installing the software must support a Java-based GUI. All consoles for Windows systems support Java-based GUIs, but not all consoles for Linux systems do.

To install Converged Application Server:

1. Log in to the target machine.
2. Download the Converged Application Server software from the Oracle software delivery website at:  
<http://edelivery.oracle.com>
3. Go to the directory where you downloaded the installation ZIP file and extract **occas\_generic.jar**.
4. Launch the installation program by entering the following command from the JDK directory on your system:

```
java -jar occas_generic.jar
```

The installation program starts.

If no other Oracle products are installed on the system, the Installation Inventory Setup 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.

If an Installation Inventory exists, the Converged Application Server Installation Welcome screen appears.

5. Click **Next**.

The Auto Updates screen appears.

6. If you already have an Oracle Technical Support account, use this screen to indicate how you would prefer to receive product and security updates. Either enter your account details or select **Skip Auto Updates**, then click **Next**.

The Installation Location screen appears.

7. Use this screen to specify the location of your Oracle home directory. Click **Next**.

The Installation Type screen appears.

8. Select one of the following options:
  - **Converged Application Server Installation:** This option includes everything you need to install, configure, and run Converged Application Server.
  - **Complete Installation:** In addition to the Converged Application Server software, this option also includes example converged applications. The examples are installed in your *Oracle\_Home/occas/samples/sipserver/examples* directory. *Oracle\_Home* is the directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Converged Application Server and WebLogic Server. For more information about the examples, see *Converged Application Server Developer's Guide*. Click **Next**.

The Prerequisite Checks screen appears.

9. This screen verifies that your system meets the minimum requirements. If there are any warnings or errors, make sure that your environment meets all of the prerequisites. See [System Requirements](#) for more information.

Click **Next**.

The Installation Summary screen appears.

10. Use this screen to 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, exit the installer now.

For more information about silent installation, see "[Installing Converged Application Server Using the Silent Installation](#)".

11. Review the selections you have made, and click **Install**. The Installation Progress screen appears and the installation begins.

#### Note

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

12. When the installation completes, click **Next**. The Installation Complete screen appears.

The next step is to launch the configuration wizard to create your WebLogic Server domain. There are two ways to launch the configuration wizard:

- Select **Automatically Launch the Configuration Wizard** on this screen. After you click **Finish** to close the installer, the configuration wizard starts and you can begin to configure your domain. Proceed to "[Creating a Converged Application Server Domain](#)".
- Do not select **Automatically Launch the Configuration Wizard** on this screen. After you click **Finish** to close the installer, manually start the configuration wizard to begin configuring your domain. Proceed to "[Starting the Configuration Wizard](#)".

#### Note

You must install the latest patches before you can use the Remote Console to configure your Converged Application Server.

## Installing Converged Application Server Using the Silent Installation

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 before you begin installation. The installation program does not display any options during the installation process.

#### Note

You must install the latest patches before you can use the Remote Console to configure the Converged Application 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]

#Set this to true if you wish to skip software updates
DECLINE_AUTO_UPDATES=true

#My Oracle Support User Name
MOS_USERNAME=

#My Oracle Support Password
```

```

MOS_PASSWORD=<SECURE VALUE>

#If the Software updates are already downloaded and available on your local system, then
specify the path to the directory where these patches are available and set
SPECIFY_DOWNLOAD_LOCATION to true
AUTO_UPDATES_LOCATION=

#Proxy Server Name to connect to My Oracle Support
SOFTWARE_UPDATES_PROXY_SERVER=

#Proxy Server Port
SOFTWARE_UPDATES_PROXY_PORT=

#Proxy Server Username
SOFTWARE_UPDATES_PROXY_USER=

#Proxy Server Password
SOFTWARE_UPDATES_PROXY_PASSWORD=<SECURE VALUE>

#The oracle home location. This can be an existing Oracle Home or a new Oracle Home
ORACLE_HOME=/home/sdp/occas8

#The federated oracle home locations. This should be an existing Oracle Home. Multiple
values can be provided as comma separated values
FEDERATED_ORACLE_HOMES=

#Set this variable value to the Installation Type selected. e.g. Converged Application
Server, Complete with Examples.
INSTALL_TYPE=Converged Application Server

```

## Returning Exit Codes to the Console

The silent installation program generates exit codes that indicate the success or failure of the installation.

**Table 5-1 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 WebLogic Platform 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

```

#!/bin/bash

# Execute the installer in silent mode
java -jar occas_generic.jar -silent -responseFile /home/user/bin/response.rsp

exit_code=$?

echo "exit code = ${exit_code}"

```

```
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'
```

## Running the Installer in Silent Mode

To perform a silent installation:

1. Log in to the target system.
2. Download the Converged Application Server 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 Converged Application Server software.
5. Start the installer by entering the following command:

```
java -jar occas_generic.jar -silent -responseFile ResponseFile
```

The 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. Check whether the installer completed successfully by retrieving the exit codes, as described in "[Returning Exit Codes to the Console](#)".

# 6

## Creating and Configuring Domains

This chapter describes the steps required to create your Oracle Communications Converged Application Server domain.

Before continuing in this chapter, you need to understand the following:

- WebLogic Server domains and clustering. See "[Understanding Oracle WebLogic Server Domains](#)" in *Understanding Domain Configuration for Oracle WebLogic Server*.
- The domain topologies available for use with Converged Application Server. See [Understanding Installation Topologies](#).

### About Domains and Domain Configuration

You must configure the domains of all servers in your Converged Application Server system. You can configure your domains by:

- Using the WebLogic Server Configuration Wizard to configure each server in your installation.
- You can scale your domain horizontally, with managed servers and engines. Start by configuring the domain on the Administration Server and then using the **pack** and **unpack** commands provided by Oracle WebLogic Server to package the configuration data for copying to all the other servers. The Converged Application Server installer puts the **pack** and **unpack** commands in the `Oracle_Home/wlserver/common/bin` directory. `Oracle_Home` is the directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Converged Application Server and WebLogic Server. The pack and unpack commands do not copy security files. Security files need to be provisioned manually after unpacking a domain configuration on the target system with the necessary certificates and security files.

For more information about packing and unpacking configurations, see [Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands](#).

- Using the WebLogic Scripting Tool (WLST) to configure each domain. The WLST scripting environment is based on the Java scripting interpreter, Jython. See [Oracle Fusion Middleware Understanding the WebLogic Scripting Tool](#) for more information.

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*.

### About Converged Application Server Domain Types

Converged Application Server ships with default domain configuration templates for each type of deployment that Converged Application Server supports. You use one of these templates to configure your domain. These templates contain the basic configurations for setting up domains, but you may need to adjust some aspects of the domain during the domain configuration process.

- **Converged Application Server - Basic Domain**

The Basic Domain template enables you to create a simple Converged Application Server domain. This domain configuration can be used during development where it is more convenient to deploy and test applications on a single server. The Basic Domain topology can also be used in deployments that do not have high-availability and scalability requirements.

This domain template is specified in **oracle.communications.occas.basic.template.jar**.

The domain configuration script for this domain type is **occas-basic.py**, which you can find in *Oracle\_Home/occas/common/templates/scripts/wlst*.

- **Converged Application Server - Basic Intelligent Media Connector Domain**

The Basic Intelligent Media Connector Domain template enables you to create a simple Converged Application Server domain that supports the Intelligent Media Connector. This domain configuration can be used during development where it is more convenient to deploy and test applications on a single server. This domain can also be used in deployments that do not have high-availability and scalability requirements.

This domain template is specified in

**oracle.communications.occas.basic.intelligentmediaconnector.template.jar**.

The domain configuration script for this domain type is **occas-media-connector-basic.py**, which you can find in *Oracle\_Home/occas/common/templates/scripts/wlst*.

- **Converged Application Server - Replicated Domain**

The Replicated Domain template enables you to create a replicated Converged Application Server domain. The Replicated Domain topology is designed for use with SIP applications that require high levels of scalability, availability, and performance.

This domain template is specified in

**oracle.communications.occas.combined.coherence.template.jar**.

The domain configuration script for this domain type is **occas-replicated.py**, which you can find in *Oracle\_Home/occas/common/templates/scripts/wlst*.

- **Converged Application Server - Replicated Intelligent Media Connector Domain**

The Replicated Intelligent Media Connector Domain template enables you to create a replicated Converged Application Server domain that supports the Intelligent Media Connector. This domain is designed for use with SIP applications that require high levels of scalability, availability, and performance.

This domain template is specified in

**oracle.communications.occas.replicated.intelligentmediaconnector.template.jar**.

The domain configuration script for this domain type is **occas-media-connector-replicated.py**, which you can find in *Oracle\_Home/occas/common/templates/scripts/wlst*.

- **Converged Application Server - Dynamic Cluster Replicated Domain**

The Dynamic Domain template enables you to create a dynamically scaled Converged Application Server domain. The Dynamic Domain topology is designed for use with SIP applications that require high levels of scalability, availability, and performance in a private or public cloud.

This domain template is specified in

**oracle.communications.occas.combined.coherence.dynamicserver.template.jar**.

The domain configuration script for this domain type is **occas-replicated-dynamiccluster.py**, and the associated properties file is *occas-replicated-dynamiccluster.properties*, which you can find in *Oracle\_Home/occas/common/templates/scripts/wlst*.

- **Converged Application Server - Diameter Domain**

The Diameter Domain template enables you to create a simple Diameter Converged Application Server domain, complete with a Home Subscriber Server (HSS), HSS client, and relay servers. The Diameter Domain topology supports the Diameter protocol over the TCP, TLS, and SCTP transport protocols.

### Note

The Diameter Domain is not available through the Graphical Mode Domain Configuration Wizard. To configure the Diameter Domain graphically with the Domain Configuration Wizard, you need to choose one of the custom templates below.

You install and configure the Diameter Domain manually. For instructions, see "Configuring Diameter Client Nodes and Relay Agents" in *Converged Application Server Administrator's Guide*.

These domain templates are specified in `Oracle_Home/wlserver/common/templates/wls/`

- **diameterdomain.jar**: enables you to configure hss, hssclient and relay servers.
- **diameterextension.jar**: enables you to add diameter protocol support to existing domains.

The domain template JAR files for these domain types are located in the directory `Oracle_Home/wlserver/common/templates/wls/`.

The domain configuration scripts and property files are located in the directory `Oracle_Home/occs/common/templates/scripts/wlst/`.

To add Diameter support, extend an existing domain with Diameter components. The domain extension template is `Oracle_Home/wlserver/common/templates/wls/diameterextension.jar`.

## Creating a Converged Application Server Domain

To create a Converged Application Server domain:

1. If you are creating a replicated domain, perform the required preconfiguration steps.
2. Start the Configuration Wizard.  
`Oracle_Home/oracle_common/common/bin/config.sh`
3. Answer the questions in each screen of the Configuration Wizard.

For more information about creating a WebLogic Server domain by using the Configuration Wizard, see "[Creating a WebLogic Domain](#)" in *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

## Preconfiguration Steps for Replicated Domains

If you are creating a Converged Application Server replicated domain, perform the following configuration steps:

- Specify an explicit listener address for each machine in your cluster. This enables your machines to communicate with each other when the Coherence Cluster uses the default cluster mode.

If you do not want to specify an explicit listen address for each machine, change the Coherence cluster mode either to unicast addressing by using the Well Known Address (WKA) feature or to multicast addressing.

- Keep the directory structures the same on each machine in the cluster to simplify deployment.
- Install the Converged Application Server 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:

```
rm -rf Domain_home/servers/
```

*Domain\_home* is the directory in which the Converged Application Server domain resides, located in *Oracle\_Home/user\_projects/domains*.

For more information, see the following:

- ["Configuring and Managing Coherence Clusters"](#) in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.
- ["Introduction to Coherence Clusters"](#) in *Oracle Fusion Middleware Developing Applications with Oracle Coherence*.
- ["Relationship Between Coherence and WebLogic Server Clusters"](#) in *Oracle Fusion Middleware Understanding Oracle WebLogic Server*.

## Starting the Configuration Wizard

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

To start the Configuration Wizard manually:

1. Enable graphical login on the target system by enabling VNC (or another similar tool).
2. Log in to the target system.
3. Go to the *Oracle\_Home/oracle\_common/common/bin* directory.
4. At a command prompt, enter:

```
sh config.sh
```

The Configuration Wizard starts and the Configuration Type screen appears. Go to ["Creating a Converged Application Server Domain in Graphical Mode"](#) and follow the steps for configuring the domain.

## Creating a Converged Application Server Domain in Graphical Mode

The Configuration Wizard displays a sequence of screens in the order listed below. The screens that you see depend on the type of product configuration template that you use. To configure your domain, answer the questions on the following screens.

### 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.  
Oracle recommends that you create your domain outside of the *Oracle\_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 options on the Configuration Type screen, see [Configuration Type](#) in *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 one of the following Converged Application Server configuration templates:
  - **Converged Application Server - Basic Domain**
  - **Converged Application Server - Replicated Domain**
  - **Converged Application Server - Basic Intelligent Media Connector Domain**
  - **Converged Application Server - Replicated Intelligent Media Connector Domain**
  - **Converged Application Server - Replicated Dynamic Cluster Domain**
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.  
  
This user name is used for booting and connecting to the Administration Server. For setup and testing, Oracle recommends that you use **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 need this information later to start and access the Administration Server.
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 *Performance and Tuning for Oracle WebLogic Server*.
2. In the **Enable or Disable Default Ports for Your Domains**, select whether or not your instance listens on SSL ports.  
By default, Development mode listens on non-SSL ports and Production listens on SSL ports.
3. 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 Converged Application Server. You can specify a different JDK.
4. Click **Next**.  
The Advanced Configuration screen appears. (See "[Advanced Configuration Screen](#)").

## 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**.

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
2. Click **Next**.

### 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.
4. To enable the SSL listen port, select the **Enable SSL** check box and enter the port number to use for secure requests. The default port number is **7002**.
5. 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.
  - **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 Remote 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. To enable the SSL listen port, select the **Enable SSL** check box and enter the port number to use for secure requests.  
Do not enable SSL unless you have a trusted key.
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**.

### Server Templates Screen

In the Server Templates Screen:

1. Click Add to add a new server record.
2. Enter a name, for the server record, specify a listen port and an SSL listen port, and specify whether SSL is enabled.
3. Click **Next**.

To delete a server record, select a row and click the **Delete** button.

To discard all changes you've made, click the **Discard Changes** button.

### Dynamic Servers Screen

Use the Dynamic Servers screen to configure however many dynamic servers that you need. Configuring dynamic clusters is an optional configuration.

If you want to configure a dynamic cluster for your domain:

1. In the **Dynamic Cluster** column, enable the dynamic cluster checkbox for your domain.  
Notice that a new row is added to the table of dynamic clusters.
2. In the **Cluster Name** column, enter a name for your dynamic server.
3. In the **Server Name Prefix** column, enter the server name prefix.
4. From the **Server Template** column, select a server template that you created on the previous screen.
5. In the **Dynamic Cluster Size** column, enter the size of the dynamic cluster.
6. In the **Machine Name Match Expression** column, enter the regular expression to match the dynamic cluster with the machine.

7. If the machine names are calculated dynamically according to the **Machine Name Match Expression**, select the checkbox in the **Calculated Machine Names** column.
8. If the listen ports are calculated dynamically according to the port defined on the server template, select the checkbox in the **Calculated Listen Ports** column.
9. Click **Next**.

For more information, see the discussion about administering clusters and creating dynamic clusters in your Oracle WebLogic Server documentation.

### Assign Servers to Clusters Screen

In the Assign Servers to Clusters screen:

1. In the **Servers** pane, select one or more managed servers.
2. In the **Clusters** pane, select the cluster to which you want to assign the managed servers.
3. Click the right arrow button.
4. 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 Converged Application Server 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.

1. In the Machines screen, select the **Unix Machine** tab.
2. To add machines to your Converged Application Server 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**.

### For Windows

1. In the Machines screen, select the **Machine** tab.
2. To add machines to your Converged Application Server 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. In the **Node Manager Listen Address** list, select the address that Node Manager uses to listen for connection requests.
5. In the **Node Manager Listen Port** list, select the port that Node Manager uses to listen for connection requests.
6. Click **Next**.

### Services Targeting Screen

Target services for deployment on 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**.

## 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**.

## End Of Configuration Screen

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

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

## Extend an Existing Non-Diameter Domain

When extending an existing non-diameter domain, add a custom-resource to config.xml.

There are two ways to extend a non-diameter domain: using the Configuration Wizard or editing the config.xml file.

1. Extend the non-Diameter domain with the Configuration Wizard.

- a. Start the Configuration Wizard.  

```
cd Oracle/Middleware/Oracle_Home/oracle_common/common/bin
sh config.sh
```
  - b. Select **Update an existing domain**.
  - c. Select **Update Domain Using Custom Template** and browse to the `diameterextension.jar` file.  

The `diameterextension.jar` file is located in *Oracle\_Home/wls/***common/templates/wls/**.
  - d. Select **Next** and complete the upgrade.
2. Extend the non-Diameter domain by editing the `config.xml` file.
    - Add a custom-resource like the following.

**Note**

The target property is environment specific.

```
<custom-resource>
  <name>ProfileService</name>
  <target>hssclient</target>
  <deployment-order>300</deployment-order>
  <descriptor-file-name>custom/profile.xml</descriptor-file-name>
  <resource-
class>com.bea.wcp.profile.descriptor.resource.ProfileServiceResource</
resource-class>
  <descriptor-bean-
class>com.bea.wcp.profile.descriptor.beans.ProfileServiceBean
  </descriptor-bean-class>
</custom-resource>
```

## Starting the Servers in Converged Application Server

To access the tools for managing your domain, start the necessary servers:

- [Starting the Administration Server](#)
- [Starting the Node Manager](#)
- [Starting the Managed Servers](#)

## Starting the Administration Server

To start the Administration Server:

1. Go to the `Domain_home/bin` directory.
2. Enter the following command:  

```
./startWebLogic.sh
```
3. If you selected 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*.

## Starting the Node Manager

To start Node Manager:

1. Go to the `Domain_home/bin` directory.
2. Enter the following command:

```
./startNodeManager.sh
```

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 the Managed Servers

Before starting your managed servers 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 you want to start.
- `admin_server_url` is the full URL of the Administration Server.

The following shows sample commands for starting `occas_server_1` and `occas_server_2`:

```
./startManagedWebLogic.sh occas_server_1 t3://host.example.com:7001 &  
./startManagedWebLogic.sh occas_server_2 t3://host.example.com:7001 &
```

For more information about starting managed servers, see [Starting and Stopping Managed Servers](#) in *Administering Server Startup and Shutdown for Oracle WebLogic Server*.

# 7

## Post-Installation Tasks

This chapter provides instructions for Oracle Communications Converged Application Server post-installation tasks.

Before continuing, complete the tasks in the following chapters:

- [Installing Converged Application Server](#)
- [Creating and Configuring Domains](#)

## Overview of Converged Application Server Post-Installation Tasks

After installing Converged Application Server, complete the following post-installation tasks:

- [Apply Patches](#)
- [Enabling DNS Server Lookup](#)
- [Configuring Converged Application Server Authentication](#)
- [Configuring the Coherence Security Framework](#)

Before continuing, start the servers in your Converged Application Server system. See "[Starting the Servers in Converged Application Server](#)" for more information.

### Apply Patches

At regular intervals, search for and apply patches for Converged Application Server and for Oracle WebLogic Server.

For more information about patching Converged Application Server, see "[Patching](#)".

For more information about patching Oracle WebLogic Server, see your WebLogic Server documentation.

#### Note

You must install the latest patches before you can use the Remote Console to configure the Converged Application Server.

### Enabling DNS Server Lookup

You must enable DNS server lookup on your Converged Application Server system to ensure that the **maddr** parameter in SIP headers is processed properly.

To enable DNS server lookup:

1. Start your Converged Application Server servers if they are not already running. See "[Starting the Servers in Converged Application Server](#)" for more information.

2. From the **Edit Tree** of the Remote Console, select **Custom Resources**, and then **sipserver**, and then **Sip Server**.
3. Scroll down and select the **Enable DNS Server Lookup** option.
4. Click **Save**, and then the shopping cart, and then **Commit Changes**.

## Configuring SSL Host Name Verification

If your Converged Application Server system supports Secure Socket Layer (SSL), disable host name verification.

To disable SSL host name verification:

1. From the **Edit Tree** of the Remote Console, click **Environment**, and then **Servers**.
2. For each server in the **Servers** table, do the following:
  - a. Click the name of the server, and then click the **Security** tab, and then click the **SSL** subtab.
  - b. Click **Show Advanced Fields**.
  - c. Enable the **Disable Hostname Verification** option.
  - d. Click **Save**, click the shopping cart, and then click **Commit Changes**.

## 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*.

# 8

## Installing Infrastructure Components

If you installed the basic or replicated Intelligent Media Connector domain, you must also install the Media Flow Engine and the RTP Proxy on a separate physical or virtual machine. The Converged Application Server download includes the Media Flow Engine tarball and the RTP Proxy tarball.

1. Install the Media Flow Engine.
2. Install the RTP Proxy.
3. Install the Intelligent AI Connector.

### Install the Media Flow Engine

Install the Media Flow Engine on a separate machine from your Converged Application Server.

The IP address must be reachable by both the RTP Proxy and the Converged Application Server.

#### Note

Oracle recommends using two separate IP addresses: one for control traffic from the Converged Application Server, the other for receiving RTP packets from the RTP Proxy.

1. Download the Media Flow Engine installer tarball.
2. Set the `JAVA_HOME` variable to the path of your JDK 25. Then update your `PATH` variable to include the bin directory of your new `JAVA_HOME`.

```
export JAVA_HOME=/usr/lib/jvm/jdk-25.0.2-oracle-x64
export PATH="$JAVA_HOME/bin:$PATH"
```

3. Extract the Media Flow Engine file.

```
tar xf media-flow-engine-8.3.0.0.0.tar.gz
```

4. Navigate to the `media-flow-engine-8.3.0.0.0-MFE/MFE_HOME/config` directory and update the two IP address parameters in the `application.yaml` file to match the IP address of the server where you will deploy the MFE.
  - `application.ip-address` – The IP address which Converged Application Server uses to communicate with the Media Flow Engine over HTTP or HTTPS. When configuring **Media Flow Engines** in the Remote Console, use this IP address for the **Management IP** field.

- **Gst.Ip-address** – The internal IP address used for receiving RTP packets from the RTP Proxy.

```
application:
  media-session:
    base-path: /media/v1/session
    ip-address: "127.0.0.1"
  custom-metrics:
    endpoint-path: /metrics
```

```
Gst:
  Ip-address: "127.0.0.1"
```

5. Navigate to the `media-flow-engine-8.3.0.0.0-MFE/MFE_HOME/bin` directory.

```
cd ../bin
```

6. Start the MFE.

```
sh startMFE.sh
```

To verify the MFE has started, open a browser and navigate to `http://<IP address>:9090/metrics`. The Converged Application Server uses port 9090 for health checks.

## Configuring the Media Flow Engine

After installing the Media Flow Engine (MFE), follow one of these procedures to identify the MFE to your Converged Application Server.

### Remote Console

You may use the Remote Console to identify the MFE to your Converged Application Server instance.

1. From the Edit Tree, select **Custom Resources**, and then **IntelligentMediaConnector**, and then **Media Connector Configurations**, and then **Media Flow Engines**.
2. Click **New**.
3. Enter the following required fields:
  - **Server Name** – Enter a name for this server, such as MFE-1.
  - **Management IP** – Enter the management IP address for this server. This IP address is the same identified in the `application.ip-address` parameter of the `application.yaml` file.
  - **Management TLS Port** – Enter the port that the Media Flow Engine will use for HTTPS management traffic. This value must match the value of `server.https-port` in the `application.yaml` file.
  - **Management Non-TLS Port** – Enter the port that the Media Flow Engine will use for HTTP management traffic. This value must match the value of `server.http-port` in the `application.yaml` file of the MFE.
4. To enable TLS, move the **SSL/TLS Enabled** slider to the right.

**Note**

If you enable TLS, you must create a keystore and update the `JAVA_OPTIONS` variable to point to your keystore.

```
JAVA_OPTIONS="${SAVE_JAVA_OPTIONS} \  
-Djavax.net.ssl.trustStore=${ORACLE_HOME}/client-truststore.jks \  
-Djavax.net.ssl.trustStorePassword=changeit \  
-Djavax.net.ssl.trustStoreType=JKS"
```

See the [keytool documentation](#) for instructions on creating a keystore.

5. Select **Create**.
6. Select the shopping cart and then **Commit Changes**.

**REST APIs**

You may use the REST API to identify the MFE to your Converged Application Server instance.

Send a POST request to the endpoint `/management/weblogic/latest/edit/customResources/IntelligentMediaConnector/customResource/mediaFlowEngines/`.

```
curl -X POST \  
--user <ADMIN_USERNAME>:<ADMIN_PASSWORD> \  
-H 'X-Requested-By:MyClient' \  
-H 'Accept:application/json' \  
-H 'Content-Type:application/json' \  
-d @mfe.json \  
"http://10.0.0.1:7001/management/weblogic/latest/edit/customResources/  
IntelligentMediaConnector/customResource/mediaFlowEngines/"
```

The contents of the `mfe.json` file sent in the request must contain the parameters shown below. Modify the values to match with your deployment. Note that 8443 is the default TLS port for the MFE and 8080 is the default non-TLS port for the MFE.

```
{  
  "managementIP": "10.0.0.2",  
  "managementPort": 8443,  
  "sslEnabled": true,  
  "serverName": "MFE-3",  
  "secondaryPort": 8080  
}
```

## Install the RTP Proxy

After installing the Media Flow Engine, next install the RTP Proxy.

Before installing the RTP Proxy, verify your system matches the requirements.

Hypervisor	KVM/QEMU
Host OS	Oracle Linux 9 (UEK kernel recommended)

Guest OS	Oracle Linux 9 (x86_64)
Host NICs	Intel (E810/X710/XL710) or Mellanox/NVIDIA (ConnectX-5/6) with SR-IOV
Guest NICs	1 (virtio)
Access	Root access
vCPUs per VM	12 (16 recommended)
RAM per VM	16 - 48GB
Storage per VM	40GB
SR-IOV VFs per VM	2
Java	JDK 25

- NTP or chrony must be enabled on both the hosts and guests VMs.
- There must not be any layer 3 device between the active and standby RTP proxy nodes; L2 adjacency is required for VIP failover and gratuitous ARP propagation.

In failover scenarios, the standby node takes over the virtual IP and sends GARP (Gratuitous ARP) announcements. These GARP messages update the MAC/IP association of the VIP on the network, ensuring continuity of RTP stream delivery. Switches and connected infrastructure must not block or filter GARP messages, and should support fast MAC address table updates. Port security mechanisms (such as sticky MAC or dynamic ARP inspection) must allow legitimate MAC moves and GARP updates to prevent disruption during failover.

Receiver Side Scaling (RSS) must be enabled on every NIC to ensure performance.

## KVM Configuration

Complete the following steps to configure KVM for your RTP Proxies.

### BIOS/UEFI Settings

Depending on your hardware, some of these settings may not be available.

1. In the system's BIOS, set the CPU profile to "Performance".
2. Disable C3/C6 power states.
3. Enable Turbo.

### Tune the Kernel

The values for each setting must be customized for your CPU.

1. Disable IRQ balance.

```
sudo systemctl disable --now irqbalance
```

2. Add the following CPU parameters to grub.

**Table 8-1 Kernel Arguments**

Parameter	Purpose
isolcpus	Marks these CPUs as isolated from the scheduler's general load balancing
nohz_full	Puts those CPUs into full tickless mode to minimize scheduler timer interrupts
rcu_nocbs	Offloads RCU callbacks from those CPUs to housekeeping CPUs
intel_iommu	Enables Intel VT-d IOMMU for DMA isolation and for vfio-pci use
iommu	Enables pass-through mode for IOMMU on non-vfio devices to reduce overhead
tuned.non_isolcpus	Declares which CPUs are housekeeping (NOT isolated)
intel_pstate	Enables or disables the Intel P-state driver

The following command isolates Intel CPUs 2 through 47 and 50 through 97.

```
sudo grubby --update-kernel=ALL \
  --args="isolcpus=2-47,50-95 nohz_full=2-47,50-95 rcu_nocbs=2-47,50-95
intel_iommu=on iommu=pt tuned.non_isolcpus=00030000,00000003
intel_pstate=disable"
```

The following command isolates AMD CPUs 2 through 47 and 50 through 97

```
sudo grubby --update-kernel=ALL \
  --args="isolcpus=2-47,50-95 nohz_full=2-47,50-95 rcu_nocbs=2-47,50-95
amd_iommu=on iommu=pt tuned.non_isolcpus=00030000,00000003"
```

3. Once the appropriate kernel parameters have been set for your hardware, reboot the system.

Use this command to verify your kernel arguments:

```
cat /proc/cmdline
```

### Install KVM

1. Verify your CPU supports virtualization.

```
egrep -i 'vmx|svm' /proc/cpuinfo
```

2. Install virtualization software.

```
sudo dnf groupinstall "Virtualization Host"
```

3. Start the libvirtd service.

```
sudo systemctl enable --now libvirtd
```

## Manage Virtual Networks

1. Block the kernel from automatically loading the i40evf and iavf drivers.

```
echo "blacklist i40evf" | sudo tee -a /etc/modprobe.d/blacklist.conf
echo "blacklist iavf" | sudo tee -a /etc/modprobe.d/blacklist.conf
```

This allows the build-in driver `mlx5_core` to be used instead.

2. Customize the following script as appropriate to your network interfaces and requirements.

```
sudo bash -c 'cat > /etc/rc.d/rc.local << "EOF"
#!/usr/bin/env bash
# Create VFs
echo 2 > /sys/bus/pci/devices/0000:af:00.0/sriov_numvfs
echo 2 > /sys/bus/pci/devices/0000:af:00.1/sriov_numvfs
# Assign MACs
ip link set enp175s0f0 vf 0 mac ee:07:94:7a:a7:81
ip link set enp175s0f0 vf 1 mac ee:07:94:7a:a7:82
ip link set enp175s0f1 vf 0 mac 5a:b0:f8:ce:04:51
ip link set enp175s0f1 vf 1 mac 5a:b0:f8:ce:04:52
# Set trust and link state
ip link set enp175s0f0 vf 0 trust on
ip link set enp175s0f0 vf 1 trust on
ip link set enp175s0f1 vf 0 trust on
ip link set enp175s0f1 vf 1 trust on
ip link set enp175s0f0 vf 0 state auto
ip link set enp175s0f0 vf 1 state auto
ip link set enp175s0f1 vf 0 state auto
ip link set enp175s0f1 vf 1 state auto
# Optional: Disable spoof check for multi-mac
ip link set enp175s0f0 vf 0 spoof off
ip link set enp175s0f0 vf 1 spoof off
ip link set enp175s0f1 vf 0 spoof off
ip link set enp175s0f1 vf 1 spoof off
EOF
chmod +x /etc/rc.d/rc.local'
```

3. Reboot to apply the changes.

## Edit the Guest's Domain XML

The edits shown below are samples only. Do not reuse them without careful evaluation.

1. Use the command `lspci -D` to discover the Bus:Device:Function (BDF) values for your server.
2. Attach the VFs with VFIO.  
Edit the actual BDF values to match those of your server.

```
<hostdev mode='subsystem' type='pci' managed='yes'>
  <driver name='vfio' />
  <source>
    <address domain='0x0000' bus='0xaf' slot='0x02' function='0x0' />
  </source>
</hostdev>
```

```
<hostdev mode='subsystem' type='pci' managed='yes'>
  <driver name='vfio' />
  <source>
    <address domain='0x0000' bus='0xaf' slot='0x06' function='0x0' />
  </source>
</hostdev>
```

**3. Add a management interface.**

```
<interface type='bridge'>
  <mac address='52:54:00:22:9a:59' />
  <source bridge='br-mgmt0' />
  <model type='virtio' />
</interface>
```

**4. Define and pin the virtual CPUs to isolated NUMA-local CPUs of the host.**

```
<vcpu placement='static'>16</vcpu>
<cputune>
  <vcpupin vcpu='0' cpuset='2' />
  <vcpupin vcpu='1' cpuset='3' />
  ... (Repeat for all vCPUs) ...
  <emulatorpin cpuset='2-17' />
</cputune>
```

**5. Enable NUMA memory pinning.**

```
<numatune>
  <memory mode='strict' nodeset='0' />
</numatune>
```

**6. Enable hugepages-backed memory.**

```
<memoryBacking>
  <hugepages />
</memoryBacking>
```

## Start the Virtual Machine

**1. Define the virtual machine.**

```
virsh define vm.xml
```

**2. Start the virtual machine.**

```
virsh start <name>
```

**3. On the guest VM, enable console access from the KVM host.**

```
sudo systemctl enable --now serial-getty@ttyS0
```

**4. From the KVM host, connect to the virtual machine.**

```
virsh console <name>
```

## Prepare the Guest OS

These steps should be taken after you have connected to the guest VM.

### 1. Enable IOMMU.

```
sudo grubby --update-kernel=ALL --args="intel_iommu=on iommu=pt"
sudo reboot
```

### 2. Select the appropriate driver for your CPU.

**Table 8-2 List of Supported NIC and Their Drivers**

Vendor	Model/ Series	PF Driver	VF Driver	PF Usage	VF Usage	Notes
Intel	E810 (800 series)	ice	iavf	Keep on kernel (ice).	Recommended: vfio-pci	Enable IOMMU for vfio-pci. Bind VFs to vfio-pci for DPDK iaavf PMD.
Intel	X710/XL710 (700 series)	i40e	iavf (i40evf deprecated)	Keep on kernel (i40e).	Recommended: vfio-pci	Avoid i40evf (deprecated). Use iaavf + vfio-pci for VFs.
NVIDIA/Mellanox	ConnectX-5 / ConnectX-6	mlx5_core (eth: mlx5e)	mlx5_core (eth: mlx5e)	Do NOT use vfio-pci (keep on kernel)	Do NOT use vfio-pci (keep on kernel)	mlx5 PMD works with kernel mlx5_core + rdma-core/ DevX. Binding to vfio-pci breaks mlx5 PMD.

### 3. Set up hugepages.

The example below creates a 2GB hugepage that persists across reboots.

```
echo 2048 | sudo tee /proc/sys/vm/nr_hugepages
echo "vm.nr_hugepages = 2048" | sudo tee /etc/sysctl.d/99-hugepages.conf
sudo sysctl --system

sudo mkdir -p /dev/hugepages
echo "nodev /dev/hugepages hugetlbfs defaults 0 0" | sudo tee -a /etc/fstab
sudo mount -a
```

### 4. Apply the network-latency tuned profile.

```
sudo dnf install -y tuned-profiles-cpu-partitioning
sudo tuned-adm profile network-latency
```

5. Disable irqbalance.

```
sudo systemctl disable --now irqbalance
```

6. Install the following dependencies.

```
sudo dnf install libibverbs rdma-core librdmacm pciutils
```

7. Install the JDK 25.

```
sudo dnf install jdk-25-headless
```

## Install RTP Proxy

Install the RTP proxy.

### Active Node

Follow these steps to install the RTP Proxy on the primary node.

1. Download and extract the rtp-proxy-8.3.0.0.0.tar.gz file.

```
tar xvf rtp-proxy-8.3.0.0.0.tar.gz
```

This creates a directory called `ORACLE_HOME`.

2. Copy the contents to the `ORACLE_HOME` directory to your actual Oracle home directory.

```
cp -r ORACLE_HOME/* /scratch/occas/Oracle/Middleware/Oracle_Home/
```

3. Set the `RP_CONFIG_PATH` and `RP_LOG_PATH` variables.

```
export RP_CONFIG_PATH=/scratch/occas/Oracle/Middleware/Oracle_Home/config
export RP_LOG_PATH=/scratch/occas/Oracle/Middleware/Oracle_Home/log
```

4. Create the `config.json` file, the `log4j2.xml` file, and the `tangosol-coherence-override.xml` file.

```
cd $RP_CONFIG_PATH
mv config.json.sample config.json
mv log4j2.xml.sample log4j2.xml
mv tangosol-coherence-override.xml.sample tangosol-coherence-override.xml
```

5. Modify the `config.json` file to match the details of your environment. Pay attention to the following parameters:

- `Controller.main.server` – The IP address and port where you are running the RTP Proxy.
- `Controller.metrics.server` – The IP address and port that will serve up metrics.
- `Controller.vips` – The virtual IP addresses used by the RTP Proxy
- `Controller.tls.enabled` – Whether TLS is enabled (true) or disabled (false)
- `Datapath.spec.portConfig.ports` – Configure port information
- `Datapath.spec.domains` – Configure domains

- Datapath.spec.vipEndpoints – Set the IP address and port for the virtual IP endpoints
6. Add the active and standby RTP Proxy IP addresses to the `tangosol-coherence-override.xml` file.

```
<member-name system-property="coherence.member">RtpProxy1</member-name>
  <well-known-addresses>
    <address id="1"><ACTIVE_RTP_PROXY_IP></address>
    <address id="2"><STANDBY_RTP_PROXY_IP></address>
    <!-- Add as many WKA addresses as needed for your cluster -->
  </well-known-addresses>
<address system-property="coherence.localhost"><ACTIVE_RTP_PROXY_IP></address>
```

If your active node has the IP address of 10.1.1.1 and your standby the IP address of 10.2.2.2, your `tangosol-coherence-override.xml` file would contain the following:

```
<member-name system-property="coherence.member">RtpProxy1</member-name>
  <well-known-addresses>
    <address id="1">10.1.1.1</address>
    <address id="2">10.2.2.2</address>
    <!-- Add as many WKA addresses as needed for your cluster -->
  </well-known-addresses>
<address system-property="coherence.localhost">10.1.1.1</address>
```

7. Install the RTP proxy service.

```
cd $ORACLE_HOME/systemd
./install-systemd.sh
```

8. Start the service.

```
sudo systemctl enable --now rtp-proxy-datapath
sudo systemctl enable --now rtp-proxy-controller
```

See the `README.md` file for comprehensive details.

### Standby Node

When installing the RTP proxy service on the standby node, follow the steps for the primary node with these differences:

1. In the `config.json` file, set the IP address of the following parameters to the standby IP address:
  - `Controller.main.server.host`
  - `Controller.metrics.server.host`
2. In the `tangosol-coherence-override.xml` file, flip the `<address>` nodes so that the secondary node uses the ID attribute of 1 and the primary of 2. For example, if your active node has the IP address of 10.1.1.1 and your standby the IP address of 10.2.2.2, your `tangosol-coherence-override.xml` file would contain the following:

```
<member-name system-property="coherence.member">RtpProxy1</member-name>
  <well-known-addresses>
    <address id="1">10.2.2.2</address>
```

```
<address id="2">10.1.1.1</address>
<!-- Add as many WKA addresses as needed for your cluster -->
</well-known-addresses>
<address system-property="coherence.localhost">10.2.2.2</address>
```

## Configuring the RTP Proxy

After installing the RTP Proxy, follow one of these procedures to identify the RTP Proxy to your Converged Application Server.

### Remote Console

You may use the Remote Console to identify the RTP Proxy to your Converged Application Server instance.

1. From the Edit Tree, select **Custom Resources**, and then **IntelligentMediaConnector**, and then **Media Connector Configurations**, and then **RTP Proxies**.
2. Click **New**.
3. Enter the following required fields:
  - **Server Name** – Enter a name for this proxy, such as RTP-1.
  - **Management IP Address** – Enter the management IP address for this proxy. This IP address is the same identified in the `Controller.main.server.host` parameter of the `config.yaml` file.
  - **Management Port** – Enter the port that the RTP Proxy will use for HTTPS management traffic. This value must match the value of `Controller.main.server.httpsPort` in the `config.yaml` file.
  - **Secondary Port (Non-TLS)** – Enter the port that the RTP Proxy will use for HTTP management traffic. This value must match the value of `Controller.main.server.port` in the `config.yaml` file.
4. To enable TLS, move the **SSL/TLS Enabled** slider to the right.

#### Note

If you enable TLS, you must create a keystore and update the `JAVA_OPTIONS` variable to point to your keystore.

```
JAVA_OPTIONS="${SAVE_JAVA_OPTIONS} \  
-Djavax.net.ssl.trustStore=${ORACLE_HOME}/client-truststore.jks \  
-Djavax.net.ssl.trustStorePassword=changeit \  
-Djavax.net.ssl.trustStoreType=JKS"
```

See the [keytool documentation](#) for instructions on creating a keystore.

5. Select **Create**.
6. Select the shopping cart and then **Commit Changes**.

## REST APIs

You may use the REST API to identify the RTP Proxy to your Converged Application Server instance.

Send a POST request to the endpoint `/management/weblogic/latest/edit/customResources/IntelligentMediaConnector/customResource/mediaFlowEngines/`.

```
curl -X POST \  
  --user <ADMIN_USERNAME>:<ADMIN_PASSWORD> \  
  -H 'X-Requested-By:MyClient' \  
  -H 'Accept:application/json' \  
  -H 'Content-Type:application/json' \  
  -d @rtp.json \  
  "http://10.0.0.1:7001/management/weblogic/latest/edit/customResources/  
IntelligentMediaConnector/customResource/RTPProxys/"
```

The contents of the `rtp.json` file sent in the request must contain the parameters shown below. Modify the values to match with your deployment. Note that 8443 is the default TLS port for the RTP Proxy and 8080 is the default non-TLS port for the RTP Proxy.

```
{  
  "managementIP": "10.0.0.7",  
  "managementPort": 8443,  
  "rtpProxyName": "example.net",  
  "sslEnabled": false,  
  "secondaryPort": 8080  
}
```

# Install the Intelligent AI Connector

If you are using the Intelligent AI Connector (IAC), you must install either the Basic Intelligent Media Connector Domain or the Replicated Intelligent Media Connector Domain.

## Download Patchset 39305242

1. Log into My Oracle Support and select Patches.
2. Search for patch 39305242.
3. Download the file `p39305242_83000_Linux-x86-64.zip`.
4. Extract the zip file.

```
$ unzip p39305242_83000_Linux-x86-64.zip  
Archive:  p39305242_83000_Linux-x86-64.zip  
inflating: 38769006.zip  
inflating: IMCSampleApp-8.3.0.0.0.zip  
extracting: IntelligentAIConnector-8.3.0.0.0.tar.gz  
inflating: media-flow-engine-8.3.0.0.0.tar.gz  
inflating: README.txt  
inflating: rtp-proxy-8.3.0.0.0.tar.gz
```

### Install Patch 38769006

After extracting the patchset, install patch number 38769006.

1. Copy 38769006.zip to the OPatch directory.

```
cp 38769006.zip ~/Oracle/Middleware/Oracle_Home/OPatch/
```

2. Navigate to the OPatch directory.

```
cd ~/Oracle/Middleware/Oracle_Home/OPatch/
```

3. Install the patch.

```
./opatch apply 38769006.zip -silent
```

4. Verify the patch installed.

```
./opatch lsinventory
```

### Update Config XML

1. Navigate to the \$DOMAIN\_HOME/config directory.
2. Backup the existing config.xml file.
3. Add the following blocks before the <admin-server-name> element.  
For the **Basic Intelligent Media Connector Domain**

```
<custom-resource>
  <name>IntelligentAIConnector</name>
  <target>AdminServer</target>
  <descriptor-file-name>custom/aic-connector.xml</descriptor-file-name>
  <resource-
class>com.bea.wcp.aic.descriptor.resource.AIConnectorResource</resource-
class>
  <descriptor-bean-
class>com.bea.wcp.aic.descriptor.beans.AIConnectorBean</descriptor-bean-
class>
</custom-resource>
<custom-resource>
  <name>AICHealthMonitor</name>
  <target>AdminServer</target>
  <descriptor-file-name>custom/aic-connector.xml</descriptor-file-name>
  <resource-
class>com.oracle.occas.ags.aihm.descriptor.resource.AICHealthMonitorResourc
e</resource-class>
  <descriptor-bean-
class>com.bea.wcp.aic.descriptor.beans.AIConnectorBean</descriptor-bean-
class>
</custom-resource>
```

**For the Replicated Intelligent Media Connector Domain**

```

<custom-resource>
  <name>IntelligentAIConnector</name>
  <target>BEA_ENGINE_TIER_CLUST</target>
  <descriptor-file-name>custom/aic-connector.xml</descriptor-file-name>
  <resource-
class>com.bea.wcp.aic.descriptor.resource.AIConnectorResource</resource-
class>
  <descriptor-bean-
class>com.bea.wcp.aic.descriptor.beans.AIConnectorBean</descriptor-bean-
class>
</custom-resource>
<custom-resource>
  <name>IntelligentAIConnectorStorage</name>
  <target>BEA_ENGINE_TIER_CLUST</target>
  <descriptor-file-name>custom/coherence.xml</descriptor-file-name>
  <resource-
class>com.oracle.occas.ags.storage.descriptor.resource.AIGatewayStorageReso
urce</resource-class>
  <descriptor-bean-
class>com.bea.wcp.sip.management.descriptor.beans.CoherenceStorageBean</
descriptor-bean-class>
</custom-resource>
<custom-resource>
  <name>AICHealthMonitor</name>
  <target>BEA_ENGINE_TIER_CLUST</target>
  <descriptor-file-name>custom/aic-connector.xml</descriptor-file-name>
  <resource-
class>com.oracle.occas.ags.aihm.descriptor.resource.AICHealthMonitorResourc
e</resource-class>
  <descriptor-bean-
class>com.bea.wcp.aic.descriptor.beans.AIConnectorBean</descriptor-bean-
class>
</custom-resource>

```

**Add the aic-connector.xml**

1. Navigate to \$ORACLE\_HOME/OPatch.
2. Extract the patch.

```
unzip 38769006.zip
```

3. Copy the file.

```
cp 38769006/custom/aic_config/aic-connector.xml $DOMAIN_HOME/config/custom/
```

**Modify startWebLogic.sh**

If JWT authentication is enabled:

1. Copy the private\_aic.pem from the build package into the Oracle home directory

2. Add the following JVM parameters to the SAVE\_JAVA\_OPTIONS variable:

```
-Dmfe.config.file=${ORACLE_HOME}/mfe-app.properties
-Doracle.sdp.mgs.jwt.pem.path=${ORACLE_HOME}/private.pem
-Doracle.occas.ags.jwt.pem.path=${ORACLE_HOME}/private_aic.pem
-Daic.transcription.save=true
-Daic.transcription.dir=${ORACLE_HOME}/Transcriptions
```

3. Open the <DOMAIN\_HOME>/bin/setDomainEnv.sh file.
4. Replace the POST\_CLASSPATH if-else block with the following:

```
if [ "${POST_CLASSPATH}" != "" ] ; then
    POST_CLASSPATH="${ORCL_HOME}/occas/server/lib/platform/
oracle.sdp.occas.depended.jar${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/
server/lib/wlss-runtime-rest-proxy.jar${CLASSPATHSEP}${ORCL_HOME}/
wlserver/sip/server/lib/weblogic_sip.jar${CLASSPATHSEP}${ORCL_HOME}/
wlserver/sip/server/lib/media-gateway-storage.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/health-monitor.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/mediagateway-api.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/mgs-impl.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/media-control-api-impl.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/aic-health-monitor.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ai-gateway-storage.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ags-api.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ags-impl.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ai-service-api-impl.jar$
${CLASSPATHSEP}${POST_CLASSPATH}"
    export POST_CLASSPATH
else
    POST_CLASSPATH="${ORCL_HOME}/occas/server/lib/platform/
oracle.sdp.occas.depended.jar${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/
server/lib/wlss-runtime-rest-proxy.jar${CLASSPATHSEP}${ORCL_HOME}/
wlserver/sip/server/lib/weblogic_sip.jar${CLASSPATHSEP}${ORCL_HOME}/
wlserver/sip/server/lib/media-gateway-storage.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/health-monitor.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/mediagateway-api.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/mgs-impl.jar${CLASSPATHSEP}$
${ORCL_HOME}/wlserver/sip/server/lib/media-control-api-impl.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/aic-health-monitor.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ai-gateway-storage.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ags-api.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ags-impl.jar$
${CLASSPATHSEP}${ORCL_HOME}/wlserver/sip/server/lib/ai-service-api-impl.jar$
    export POST_CLASSPATH
fi
```

5. Restart the Admin and all Managed Servers.

## Download and Configure AIC

1. Download and extract the AIC package from the Oracle Software Delivery Cloud.

```
tar -xzvf IntelligentAIConnector-8.3.0.0.0.tar.gz
```

2. Navigate to the `config` directory.

```
cd IntelligentAIConnector-8.3.0.0.0-AIC/AIC_HOME/config/
```

3. Open the `application.yaml` file.
  - a. Set the `providers.oci.compartmentId` to your OCI compartment ID
  - b. Set the `providers.oci.region` to your OCI region.
  - c. Set `application.ip-address` to the management IP used by the REST/HTTP worker. This interface must have public network access, as IAC connects to OCI STT through this IP.
  - d. Set `application.udp.bind-address` to the private IP used for UDP media ingress. This address must be in the same subnet (L2 adjacency) as the RTPProxy and MFE to ensure proper audio packet delivery.
4. Modify the rest of the file as needed for your environment.
5. Start the AIC.

```
cd IntelligentAIConnector-8.3.0.0.0-AIC/AIC_HOME/bin  
./startAIC.sh
```

# 9

## Migrating or Upgrading

This chapter provides instructions for upgrading your Oracle Communications Converged Application Server system.

### About Migrating or Upgrading Converged Application Server

Because of architectural changes in the underlying WebLogic Server platform, there is no automated upgrade path. Instead, you must manually upgrade or migrate your Converged Application Server to the latest version.

### High Availability

During your upgrade and migration, you can introduce high availability (HA).

For information about HA environments, see "Failure Prevention and Automatic Recovery Features" in the *Converged Application Server Administrator's Guide*.

### Migrating or Upgrading Converged Application Server

To manually upgrade or migrate your Converged Application Server system:

1. Back up all of your old Converged Application Server domains.
2. Install Converged Application Server on any servers hosting the Administration Server or Managed Servers (engines). See [Installing Converged Application Server](#) and the [Cloud Deployment Guide](#).
3. Create your new Converged Application Server domains. See [Creating and Configuring Domains](#) for more information.
4. Copy the WAR or EAR files from your old domains into your new domains.
5. Verify the domain administration settings on your new Converged Application Server system. See [Verifying Your Domain Administration Settings](#).
6. Install and deploy your old applications to your new system.
7. Verify that the applications deployed on your new Converged Application Server system work as expected.

### Verifying Your Domain Administration Settings

In this section, the system you are upgrading from is called *old* (for example, your old system), and the system you are upgrading to is called *new* (for example, your new system).

1. Start your new Converged Application Server Administration Server.
2. Log in to the Remote Console.
3. Verify that your new domain configuration is correct. In particular, pay attention to the following settings:

- SSL is enabled/disabled consistently on every node machine
- All security authentication providers are listed and configured correctly
- Coherence security has been configured
- Work managers are configured correctly
- The application router is configured correctly
- The call state storage and data tier has been configured

# 10

## Patching

This chapter describes how to apply patches to your Oracle Communications Converged Application Server system.

### About Converged Application Server 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 patch releases for Converged Application Server 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 Converged Application Server 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. Converged Application Server 8.2 Patch Sets use the release numbering scheme 8.2.0.x.0, where x is the Patch Set number. For example, the first Patch Set for Converged Application Server 8.2 would be Converged Application Server 8.2.0.1.0.
- **Debug patch.** A debug patch is used to troubleshoot an ongoing issue in your Converged Application Server system. A debug patch represents a concerted attempt by you and Oracle Technical Support to fix an issue in your Converged Application Server system. Oracle Technical Support uses debug patches as a tool to extract better data from your Converged Application Server 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, Converged Application Server 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 Converged Application Server 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, Converged Application Server 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 Converged Application Server

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 Converged Application Server 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. [Verifying the Oracle Universal Installer Inventory](#)
2. [Creating a Backup of Your Current Converged Application Server Installation](#)
3. [Checking Your Environment Variables](#)

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 Linux, or to check for updates and get the latest versions, go to My Oracle Support at:

<https://support.oracle.com/>

## 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 using the following command:

```
opatch lsinventory
```

This command displays your system's OPatch and Oracle Universal Installer versions and directories, and lists the patches currently installed in *Oracle\_Home*. This is the directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Converged Application Server and WebLogic Server. For example, the following shows a sample of the information displayed at the beginning of the output:

```
Oracle Interim Patch Installer version 13.9.4.2.6
Copyright (c) 2021, Oracle Corporation. All rights reserved.

Oracle Home           : Oracle_Home
Central Inventory     : /export/oraInventory
   from                : Oracle_Home/oraInst.loc
OPatch version        : 13.9.4.2.6
OUI Version           : 13.9.4.0.0
Log file location     : Oracle_Home/cfgtoollogs/opatch/opatch2015-12-16_11-16-55AM_1.log
```

For more information, see "[OPatch Utility Reference](#)".

#### **Note**

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 Converged Application Server Installation

Before you start any patch operation, back up the contents of the *Oracle\_Home* directory. You can back up the contents of *Oracle\_Home* by using your preferred method, such as ZIP, TAR, cp -r, or cpio.

## 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 the following environment variables:

- Set your PATH environment variable to include the path to your *Oracle\_Home*/OPatch directory and to your ZIP software.
- Set your ORACLE\_HOME environment variable to your *Oracle\_Home* directory.

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

```
which opatch
which unzip
```

#### **Note**

If your system cannot find the path to the software, double-check that your environment variables are set correctly.

# Installing Converged Application Server Patches

To install a Converged Application Server patch:

1. Determine whether you need to stop all servers in your Converged Application Server 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.

2. Log in to the target system.
3. 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.

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 your temporary directory 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
```

OPatch validates the patch and makes sure that there are no conflicts with the software already installed in *Oracle\_Home* before applying the patch to your Converged Application Server 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
```

For more information, see "[OPatch Utility Reference](#)".

9. Determine whether you need to restart all servers in your Converged Application Server 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](#)".

## Installing the Priority Call Handling Patch

Installing the Priority Call Handling patch on Converged Application Server requires post-installation steps not covered by the usual patch process.

1. Add the OPatch directory to your PATH variable.

```
export PATH="$PATH:$ORACLE_HOME/OPatch"
```

2. Verify the current patch inventory:

Run `opatch lsinv` and record the output for reference.

3. Unzip the patch file and navigate to the newly created directory.

```
unzip 36869676.zip
cd 36869676/
```

4. Apply the patch:

```
opatch apply
```

5. Verify patch application:

Run `opatch lsinv` again to confirm the patch appears in the inventory.

6. Copy the configuration file `priority-call-config.xml` to the directory `<domain_name>/config/custom/`

```
cp custom/pch_config/priority-call-config.xml ~/Domain_Home/config/custom/
```

7. Edit your domain's `config.xml` to include the custom resource definition for `prioritycallconfig`:

```
<custom-resource>
  <name>prioritycallconfig</name>
  <target>BEA_ENGINE_TIER_CLUST</target>
  <descriptor-file-name>custom/priority-call-config.xml</descriptor-file-
name>
  <resource-
class>com.bea.wcp.sip.management.descriptor.resource.PriorityCallConfigReso
urce</resource-class>
  <descriptor-bean-
class>com.bea.wcp.sip.management.descriptor.beans.PriorityCallConfigBean</
descriptor-bean-class>
</custom-resource>
```

### Note

If you are using the base domain, set the `<target>` value to `AdminServer`.

8. Restart servers in the domain, one by one, to activate the patch and configuration changes.

## Troubleshooting

OPatch is reliable and protects *Oracle\_Home* and the inventory. It can bring back the contents of the *Oracle\_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.

## 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 *Oracle\_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 *Oracle\_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 Converged Application Server system.
2. Roll back the patch with the following command:

```
opatch 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 *Oracle\_Home/OPatch* directory. The following shows the syntax for running the OPatch utility:

```
opatch [-help] [-report] [command]
```

where:

- **-help** lists the commands and options supported by the utility.  
Use the **-help** parameter together with a command to view detailed information for the OPatch command. For example:  

```
opatch apply -help
```
- **-report** prints the actions without executing the command.
- *command* is one of these OPatch commands:
  - **apply** [*PatchDirectory*]

This command applies the patch to the software located in *Oracle\_Home*. If you do not run the utility from the directory in which the patch content resides (*PatchDirectory*), include the complete path to the directory.

For the command to work properly, the ORACLE\_HOME environment variable must be set to *Oracle\_Home*. See [Dealing with Conflicts When You Run the Apply Command](#).

#### – **Isinventory**

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

```
-----
Oracle Interim Patch Installer version 13.9.4.2.6
Copyright (c) 2021, Oracle Corporation. All rights reserved.

Oracle Home           : Oracle_Home
Central Inventory     : /export/oraInventory
   from                : Oracle_Home/oraInst.loc
OPatch version       : 13.9.4.2.6
OUI Version          : 13.9.4.0.0
Log file location    : Oracle_Home/cfgtoollogs/opatch/
opatch2021-11-24_06-53-05AM_1.log

OPatch detects the Oracle Home as "Oracle_Home"

-----
Interim patches (2) :

Patch 33416881 : applied on Wed Nov 24 06:53:05 GMT 2021
Unique Patch ID: 24443925
Patch description: "WLS PATCH SET UPDATE 14.1.1.0.210930"
   Created on 30 Sep 2021, 15:53:34 hrs PST8PDT
   Bugs fixed:
     30965440, 31564423, 32235275, 32528774, 31765550, 31742292, 32371861
     30912052, 31353368, 31950565, 31525147, 32868847, 25900775, 31770512
     31401659, 32544020, 31975788, 31510290, 32651810, 31918617, 32647611
     32054481, 33034990, 32373306, 32503912, 30285053, 31287540, 31671559
     32847474, 31332368, 31199699, 32408938, 32312961, 30284059, 32789767
     31316252, 31567049, 32068710, 31232471, 31475287, 31922313, 32248716
     33166329, 32875528, 32097062, 31816475, 32235872, 31247235, 33207639
     33152312, 33114718, 32883876, 31913015, 31995447, 32953480, 31047981
     32244262, 31943068, 30885114, 33245345, 31332264, 32077936, 32959192
     31583896, 31088577, 31498405, 32301793, 30838007, 31483821, 33063225
     33141458, 33171421, 30885128, 32214441, 29449188, 32976692, 31157988
     32519960, 31765567, 31142740, 30964331, 32226530, 31539237, 31492196
     30245934, 32832099, 32472196, 32228228, 32069620, 32697451, 32520971
     31011293, 31526201, 32064362, 32133880, 31441174, 30652362, 32950042
     32307656, 32639821, 32415913, 32893667, 31234573, 32108759, 33164116
     31113242, 31234666, 32593893, 31657139, 32920991, 32099344, 31160218
     30927469, 32497814, 30961904, 32962304, 31184158, 33170754, 32425607
     31380363

Patch 33286174 : applied on Wed Nov 24 06:52:09 GMT 2021
Unique Patch ID: 24406033
Patch description: "Bundle patch for Oracle Coherence Version 14.1.1.0.7"
   Created on 21 Sep 2021, 12:11:28 hrs PST8PDT
   Bugs fixed:
     31201347, 31214284, 31806281, 31944953, 32124447, 32341371, 32581868
     32816973, 32822629, 32503887, 32421840, 32973306, 33286174
-----
```

#### – **rollback -id PatchNumber**

This command removes the specified patch from the *Oracle\_Home* directory, 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 24406033** to roll back the patch shown in the following sample **lsinventory** output:

```
-----  
Interim patches (1) :  
  
Patch 33286174 : applied on Wed Nov 24 06:52:09 GMT 2021  
Unique Patch ID: 24406033  
Patch description: "Bundle patch for Oracle Coherence Version 14.1.1.0.7"  
Created on 21 Sep 2021, 12:11:28 hrs PST8PDT  
Bugs fixed:  
    31201347, 31214284, 31806281, 31944953, 32124447, 32341371, 32581868  
    32816973, 32822629, 32503887, 32421840, 32973306, 33286174  
-----
```

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*.

# 11

## Troubleshooting

This chapter describes how to troubleshoot Oracle Communications Converged Application Server installations.

### About Troubleshooting Converged Application Server Installations

The Converged Application Server 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 process.

#### About Converged Application Server Installation Log Files

The Converged Application Server installation logs 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 *Oracle\_Home/orainst.loc* file. *Oracle\_Home* is the directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Converged Application Server and WebLogic Server.

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

- **installdate-time-stamp.log**  
The main log file.
- **installdate-time-stamp.out**  
This log file contains the output and error streams during the installation.
- **installProfiledate-time-stamp.log**  
This log file contains the overall statistics such as time taken to complete the installation, as well as configuration, memory, and CPU details.
- **oralInstalldate-time-stamp.out**  
This log file contains the output stream of the copy session.
- **oralInstalldate-time-stamp.err**  
This log file contains the error stream of the copy session.

#### Changing the Installer Logging Level

To change the logging level, add the **-logLevel** parameter when you start the installer at a command prompt. For example:

```
java -jar occas_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**

## About Domain Configuration Log Files

If you encounter errors when configuring a Converged Application Server domain, you can start the Fusion Middleware Configuration Wizard with the appropriate logging options.

To enable domain configuration logging, go to *Oracle\_Home/oracle\_common/common/bin* and enter the following command:

```
./config.sh -log=log_filename -log_priority=log_level
```

**Table 11-1 Configuration Wizard Log File Options**

Parameter	Description
<b>-log</b>	<p>Specify the location of your log file.</p> <p>If you specify a log file name, it is created in the same directory as the <b>config.sh</b> script unless you add a path component. Log files are otherwise created in <i>Oracle_Home/logs</i>.</p> <p>Other values that can be specified with <b>-log</b> are:</p> <ul style="list-style-type: none"> <li>• <b>stdout</b> Writes the error message to the standard output stream.</li> <li>• <b>stderr</b> Writes the error message to the standard error stream.</li> <li>• <b>disable</b> Disables default logging so that no log files are generated in <i>Oracle_Home/logs</i>.</li> </ul>
<b>-Log_priority</b>	<p>Specify the level of detail you want included in your logs.</p> <p>The following list shows the acceptable values:</p> <ul style="list-style-type: none"> <li>• <b>OFF</b></li> <li>• <b>SEVERE</b></li> <li>• <b>WARNING</b></li> <li>• <b>INFO</b></li> <li>• <b>CONFIG</b></li> <li>• <b>FINE</b></li> <li>• <b>FINER</b></li> <li>• <b>FINEST</b></li> </ul>

## AIC Troubleshooting

Consider the following when troubleshooting the AI Connector.

### JVM Troubleshooting

- Use tools like Java Flight Recorder (JFR) and Java Mission Control (JMC) to capture and analyze JVM runtime behavior for performance issues.
- Collect JVM diagnostics using the `jcmd` utility to identify memory, thread, and GC-related problems.
- Monitor key JVM metrics such as heap usage, garbage collection activity, and thread performance to detect bottlenecks early.
- Analyze GC logs and memory usage to identify memory leaks or excessive garbage collection pauses.

### Startup Failures

Issue: Starting the AIC fails with this message:

```
ERROR [main] c.o.n.a.AICStartUp - Configured OCI config file does not exist  
or is not readable/regular: /home/sdp/.oci/config
```

Resolution:

- Verify that in the AIC VM `.oci` configuration is present and AIC gets connected to OCI properly.
- Validate that in the `$sh startAIC.sh` we should get the below console Logs.

```
INFO [main] c.o.n.a.AICStartUp - Registering OCI provider...  
INFO [main] c.o.n.a.p.i.o.OCIAIServiceProvider - OCI AI Service Provider  
initialized  
INFO [main] c.o.n.a.p.AIServiceRegistry - Registered AI provider: oci  
with capabilities: [SPEECH_TO_TEXT]  
INFO [main] c.o.n.a.AICStartUp - OCI provider registered  
INFO [main] c.o.n.a.AICStartUp - Initializing AI Connections Manager...  
INFO [main] c.o.n.a.AICStartUp - AI Connections Manager initialized  
INFO [main] c.o.n.a.AICStartUp - Initializing provider configurations...  
INFO [main] c.o.n.a.p.AIConnectionsManager - Initializing AI services  
with 1 provider configurations  
INFO [main] c.o.n.a.p.i.o.OCIAIServiceProvider - OCI AI Service Provider  
initialized  
INFO [main] c.o.n.a.p.AIConnectionsManager - Initialized AI service  
provider: oci  
INFO [main] c.o.n.a.AICStartUp - Provider configurations initialized  
INFO [main] c.o.n.a.AICStartUp - Initializing orchestration service...
```

### Enable Debug Logs

Enable debug logs to get detailed visibility into AGS/MGS processing and internal flows (request/response), which helps in troubleshooting issues.

1. In the Edit Tree, select **Custom Resource**, and then **serverdebug**, and then **SIP Server Debug**, and then **Servers**, and then **<engine-name>**.

2. Enable the MGS slider to get MGS debug logs.
3. Enable the AGS slider to get AGS debug logs.
4. Select **Save**, select the shopping cart, and select **Commit Changes**.

# 12

## Uninstalling

This chapter describes how to uninstall Oracle Communications Converged Application Server and its components.

### Uninstalling Converged Application Server Components in GUI Mode

To uninstall Converged Application Server components in GUI mode:

1. Go to the `Oracle_Home/oui/bin` directory, and enter the following in a command window:  

```
./deinstall.sh
```
2. 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 the software you want to uninstall. For example, select Oracle Communications Converged Application Server-8.2.0.0.0.
  - b. Click **Uninstall**.
3. From the Welcome screen, click **Next**.  
The Deinstallation Summary screen appears.
4. 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.
5. Click **Deinstall**.  
The Deinstallation Progress screen appears, and a progress bar indicates the status of the uninstallation process.
6. When the uninstallation process is complete, click **Next**.  
The Deinstallation Complete screen appears.
7. Click **Finish**.  
The uninstaller exits.

### Uninstalling Converged Application Server Components in Silent Mode

This section describes how to uninstall Converged Application Server components in silent mode on all platforms.

Use silent mode to uninstall duplicate installations on multiple machines. In silent mode, you create and use a **response\_uninstall.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 Converged Application Server components in silent mode:

1. Create a text file on your target system.
2. Add the following contents to your 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=Oracle Communications Converged Application Server~8.2.0.0.0

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

where `SELECTED_DISTRIBUTION` is set to the component to uninstall. For Converged Application Server, set `SELECTED_DISTRIBUTION` to **Oracle Communications Converged Application Server~8.2.0.0.0**.

3. Save the file with the name **response\_uninstall.rsp**.
4. Go to the `Oracle_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, `Oracle_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:

```
The uninstall of Oracle Communications Converged Application Server 8.2.0.0.0 completed
successfully.
Logs successfully copied to /export/oraInventory/logs.
```