

Bogotá, Noviembre 30 de 2021

Señores

Fondo De Prestaciones Económicas Cesantías Y Pensiones Foncep
Ciudad

Para efectos exclusivamente informativos y en virtud de la orden de pedido presentada por nuestro distribuidor autorizado **NEXSYS DE COLOMBIA S.A.S.**, usted es titular de las siguientes licencias de programas Oracle:

Nombre del Programa	Tipo de Licencia	Cantidad
Oracle WebCenter Content - Processor Perpetual	Full Use	1
Oracle SOA Suite for Oracle Middleware – Processor Perpetual	Full Use	1
Oracle SOA Suite for Oracle Middleware – Named User Plus Perpetual	Full Use	10
Oracle WebLogic Server Enterprise Edition - Named User Plus Perpetual	Full Use	10
Oracle WebLogic Server Enterprise Edition - Processor Perpetual	Full Use	1
Oracle WebLogic Suite - Named User Plus Perpetual	Full Use	10
Oracle WebLogic Suite – Processor Perpetual	Full Use	1

Oracle Unified Business Process Management Suite – Named User Plus Perpetual	Full Use	10
Oracle Unified Business Process Management Suite – Processor Perpetual	Full Use	1
Oracle WebCenter Content - Named User Plus Perpetual	Full Use	10

Sin otro particular, aprovechamos la ocasión de enviarle un cordial saludo.

Atentamente,
ORACLE COLOMBIA LTDA.

DocuSigned by:

31E32AF041E146...
German Mayorga
Alliances & Channels Manager



Bogotá, 03 de diciembre 2021

OCP TECH CO-124/2021

NIT 900222314-5

Señores

Fondo de Prestaciones Económicas Cesantías y Pensiones Foncep

Carrera 6 Nro 14 98 piso 6

Ciudad

Ref.: Orden de compra 80732

Asunto: Adquisición, instalación y puesta en funcionamiento de un sistema de gestión de documentos electrónicos de archivo- SGDEA

Cordial Saludo,

Nos es grato haber sido adjudicados del proceso de acuerdo con la orden de compra de la referencia, correspondiente a la contratación de servicios y licencias de Oracle en el marco del contrato Instrumento de generación de demanda de CCE.

Por medio de la presente, cumplimos en brindar mayor detalle sobre los servicios ACS de Oracle adquiridos.

En relación a los ítems 1 y 2 de la orden de compra referente a la contratación de servicios de ACS Oracle, los mismos corresponden a 25 jornadas del perfil Gerente Técnico y 335 jornadas del perfil Ingeniero Soporte Avanzado, donde cada jornada equivale a 8 horas, estos servicios serán utilizados en el proyecto Sistema de Gestión Documental de Archivos de FONCEP a partir del acta de inicio correspondiente.

Sin otro particular,

A handwritten signature in black ink, appearing to be 'MH', written over a horizontal line.

Marcelo Herrera

Representante legal

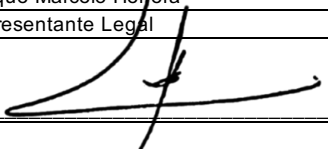
OCP TECH COLOMBIA SAS NIT 900222314-5

Info.co@ocp.tech

Tel + 601 4423209 + 57 3134653030

AK 9 #115-06 Oficina 701 Edificio Tierra Firme

Fase	Eta	Actividades	MES 1	MES2	MES3	MES4	MES5	MES6	MES7	MES8	MES9	MES10	MES11	MES12	Recursos
1	1	Planificación Proyecto													Gerente de Proyectos Arquitecto de Soluciones Arquitecto Middleware
		Documento Plan de Trabajo													
		Documento Arquitectura													
		Documento Prerequisitos													
		Verificación de Prerequisitos requeridos por producto													
	2	Instalación Ambientes Dev, Qa,Prod (WLS, BPM, WCC)													Gerente de Proyectos Arquitecto de Soluciones Consultores Middleware
		Instalación y configuración de DB WCC (DEV)													
		Instalación Ambiente de Desarrollo (DEV)													
		Instalación y configuración de DB WCC (QA)													
		Instalación Ambiente de Calidad (QA)													
		Instalación y configuración de DB WCC (PROD)													
		Instalación Ambiente de Producción (PROD)													
		Documentación de Instalación y Workbook													
	3	Gestor Documental (DEV,QA,PROD)													Gerente de Proyectos Arquitecto de Soluciones Archivista
	4	Diseño e implementación del Modulo de Comunicaciones BPM (DEV,QA,PROD)													Gerente de Proyectos Profesional Senior Consultor BPM Profesional Senior Java
		Levantamiento de información y Analisis de procesos													
		Diseño de procesos BPM													
		Implementación de procesos BPM													
		Parametrización y Despliegue de procesos BPM													
	5	Proceso de comunicaciones Interna Electrónica (DEV,QA)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	5	Proceso de comunicaciones Entrada Electrónica (DEV,QA)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	6	Proceso de comunicaciones Salida Electrónica (DEV,QA)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	7	Proceso de comunicaciones Entrada Física (DEV,QA)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	8	Proceso de comunicaciones Salida Física (DEV,QA)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	7	Proceso de comunicaciones Interna Electrónica (PROD)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	8	Proceso de comunicaciones Entrada Electrónica (PROD)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	9	Proceso de comunicaciones Salida Electrónica (PROD)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	10	Proceso de comunicaciones Entrada Física (PROD)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	11	Proceso de comunicaciones Salida Física (PROD)													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java
	12	Paso a Producción													Gerente de Proyectos Arquitecto de Soluciones Profesional Senior Consultor BPM Profesional Senior Java

		ACTA DE ENTREGA PROYECTO SGDEA		CÓDIGO:	F-PR-002
				VERSION:	3
				FECHA REVISIÓN:	
				24-feb-15	
Fecha de diligenciamiento: diciembre 17 de 2021					
Datos del cliente					
Empresa cliente:	Fondo de Prestaciones Económicas Cesantías y Pensiones Foncep	Contacto:	Wilson Barrios Delgado		
Teléfonos:	(571) 307 6200	E-mail:	wbarriosd@foncep.gov.co		
Nombre del proyecto:	Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA				
Descripción del proyecto:					
Adquisición, implementación y puesta en marcha de un nuevo Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA que contribuya de manera significativa a fortalecer los procesos de producción, recepción, distribución, consulta, organización, recuperación, disposición final y archivado de los documentos en FONCEP.					
Fecha Inicio	3/12/21	Fecha Entrega	17/12/21		
Trabajo realizado y entregado					
Instalación del sistema de gestión documental SGDEA: - Despliegue de la última versión de los componentes del sistema de gestión documental SGDEA en la plataforma de nube Oracle de la entidad, realizado por personal de Oracle, incluyendo la configuración y parametrización de la herramienta - Pruebas de funcionalidad del sistema instalado y su aceptación por parte de la entidad. Entrega de documento de pruebas y aceptación.					
Certificado de Titularidad de licencias: - El día 03 de diciembre de 2021 se le entregó a la entidad el Certificado de Titularidad de licencias de Oracle.					
Certificación del número de horas de servicio contratadas: - El día 03 de diciembre de 2021 se le entregó a la entidad la nota aclaratoria sobre la cantidad de horas de servicio de Oracle ACS contratadas para la configuración y parametrización del SGDEA de acuerdo con la estimación correspondiente al alcance del anexo técnico.					
Manuales técnicos: - Maqueta de arquitectura tecnológica de los componentes de software del sistema SGDEA implementados por Oracle - Documento de instalación de los componentes de software del sistema SGDEA conforme realizado por Oracle - Documentación complementaria del fabricante sobre el producto Oracle Webcenter Content incluyendo guías de instalación y configuración de producto, guía de despliegue empresarial y arquitecturas de referencia, guía de iniciación al producto Oracle Webcenter Content y documentación de fabricante sobre componentes de la infraestructura de software Oracle					
El cliente certifica que la totalidad de los suministros y servicios reseñados en la presente acta han sido entregados / terminados y que, habiendo sido sometidos a las pruebas de validación y aceptación indicadas, están de acuerdo con las especificaciones formales y demás requisitos contractualmente convenidos y establecidos entre las partes.					
Observaciones					
Quien entrega por parte de OCP TECH			Recibido a satisfacción Cliente		
Nombre:	Enrique Marcelo Herrera		Nombre:	Wilson Barrios Delgado	
Cargo	Representante Legal		Cargo	Jefe de Oficina de Informática y Sistemas	
Firma:			Firma:		
Fecha: 17 de Diciembre de 2021			Fecha: 17 de Diciembre de 2021		

INSTALACION WEBCENTER CONTENT

FONCEP

Autores:	Oscar Hernán Rojas
Fecha Creación:	Diciembre, 2021
Última Actualización:	
Referencia:	Revisión de plataforma
Versión:	1.1

1 Control del Documento

1.1 Registro de Cambios

Fecha	Autor	Versión	Referencia de cambio
16-12-2021	Hernán Rojas	DRAFT	Creación del documento

1.2 Revisores

Nombre	Cargo	Correo
Jaime Rozo	Senior Principal Technical Account Manager	Jaime.enrique.rozo@oracle.com

1.3 Lista de Distribución

Nombre	Cargo	Correo

1.4 Actas de Reunión Asociadas

N.A.

Contenido

1	Control del Documento.....	2
1.1	Registro de Cambios	2
1.2	Revisores.....	2
1.3	Lista de Distribución	2
1.4	Actas de Reunión Asociadas	2
	Introducción	4
2	INSTALACION BASE DE DATOS	5
	Instalación software Grid Infrastructure.....	5
	Instalación software base de datos y creación base de datos wccinfra	6
3	INSTALACION WEBCENTER CONTENT	8
	Instalación Java:	8
	Instalación Oracle Fusion Middleware Infrastructure:	8
	Instalación Oracle WebCenter Content:	13
	Instalación Oracle SOA Suite:	17
	Instalación Oracle OHS:	21
	Ejecución RCU:	26
	Creación de Dominio WLS:	31
	Consolas de Producto:	44

Introducción

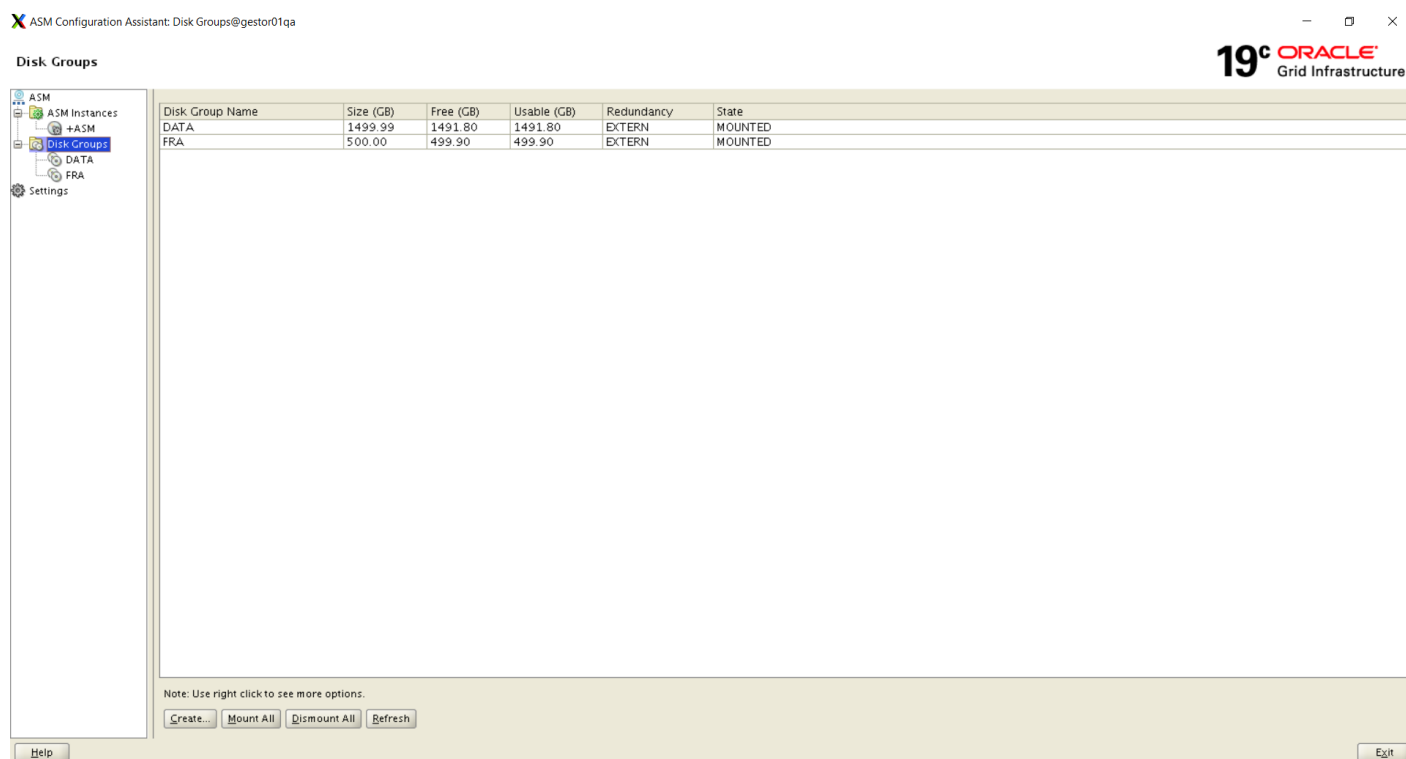
En este documento se entrega como apoyo a la instalación y configuración del Oracle WebCenter Content de FONCEP.

2 INSTALACION BASE DE DATOS

Se realiza instalación de software en versión 19.13 de Grid Infraestructure y de base de datos.

Instalación software Grid Infraestructure

Se realiza la instalación de Grind Infraestructure en versión 19.3 y se actualiza a la versión 19.13, a continuación, se realiza la creación los diskgroups de DATA y de FRA, se anexan los pantallazos correspondientes.



```
[grid@gestor01qa ~]$ id
uid=54322(grid) gid=54321(oinstall) groups=54321(oinstall),54322(dba),54324(backupdba),54325(dgdba),54326(kmdba),54327(asmdba),54328(asmoper),54329(asmadmin),54330(racdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[grid@gestor01qa ~]$ sqlplus / as sysasm

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Dec 17 15:17:38 2021
Version 19.13.0.0.0

Copyright (c) 1982, 2021, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL> show parameters db_unique_name

NAME                                TYPE        VALUE
-----
db_unique_name                       string      +ASM

SQL> SELECT BANNER_FULL
FROM V$VERSION;

BANNER_FULL
-----
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL>
```

Instalación software base de datos y creación base de datos wccinfra

Se realiza la instalación del software de base de datos en versión 19.3 y se actualiza a la versión 19.13 y se realiza la creación de la base de datos para el ambiente de Web Center Content

```
[oracle@gestor01qa ~]$ id
uid=54321(oracle) gid=54321(oinstall) groups=54321(oinstall),54322(dba),54323(oper),54324(backupdba),54325(dgdba),54326(kmdba),54327(asmdba),54329(asmadmin),54
330(racdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[oracle@gestor01qa ~]$ export ORACLE_SID=wccinfra
[oracle@gestor01qa ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Dec 17 16:39:07 2021
Version 19.13.0.0.0

Copyright (c) 1982, 2021, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL> show parameters db_unique_name

NAME                                TYPE        VALUE
-----
db_unique_name                      string      wccinfra
SQL> select BANNER_FULL
2 from v$version;

BANNER_FULL
-----
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL> █
```

Database Configuration Assistant - Configure an existing database - Step 7 of 9@gestor01qa

Summary

- [Database Operation](#)
- [Select Database](#)
- [Database Options](#)
- [Data Vault Option](#)
- [Connection Mode](#)
- [Oracle R Configuration](#)
- Summary**
- Progress Page
- Finish

Database Configuration Assistant

Database New Configuration

- Database Name: wccinfra
- Configure Oracle Database Vault: No
- Configure Oracle Label Security: No
- Configure Oracle Label Security with OID: No
- Configure Oracle R: Yes
- Tablespace for Oracle R configuration: SYSAUX
- Database components

Help

< Back

Next >

Finish

Cancel

3 INSTALACION WEBCENTER CONTENT

A continuación, se presentan las pantallas de instalación del producto Oracle WebCenter Content

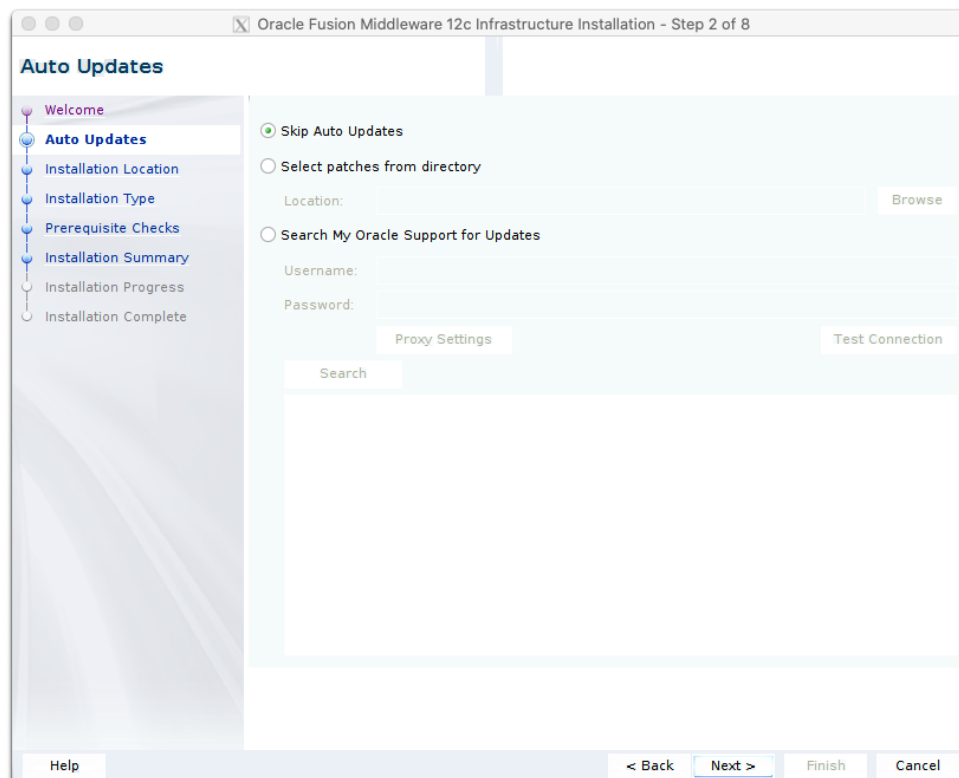
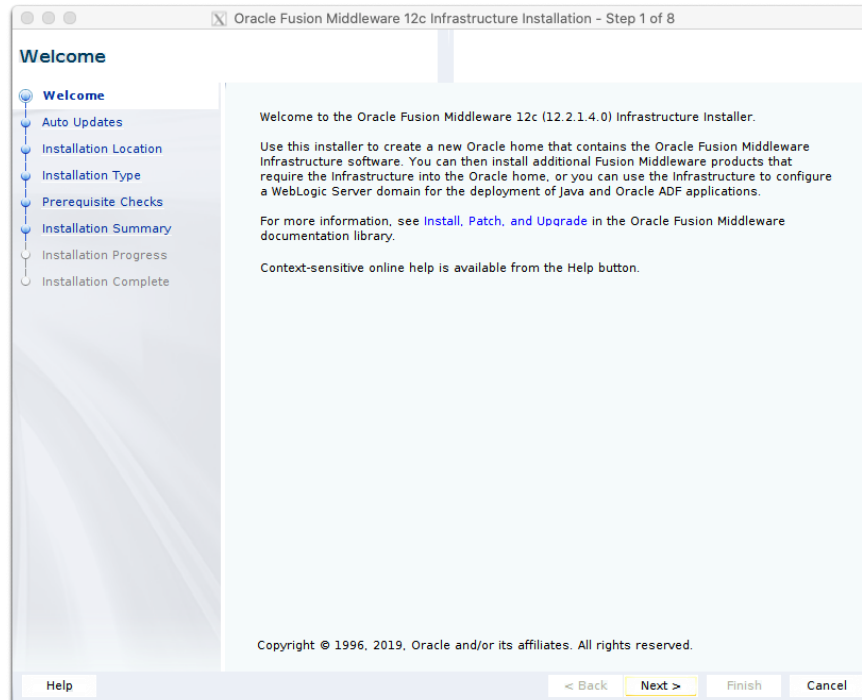
Instalación Java:

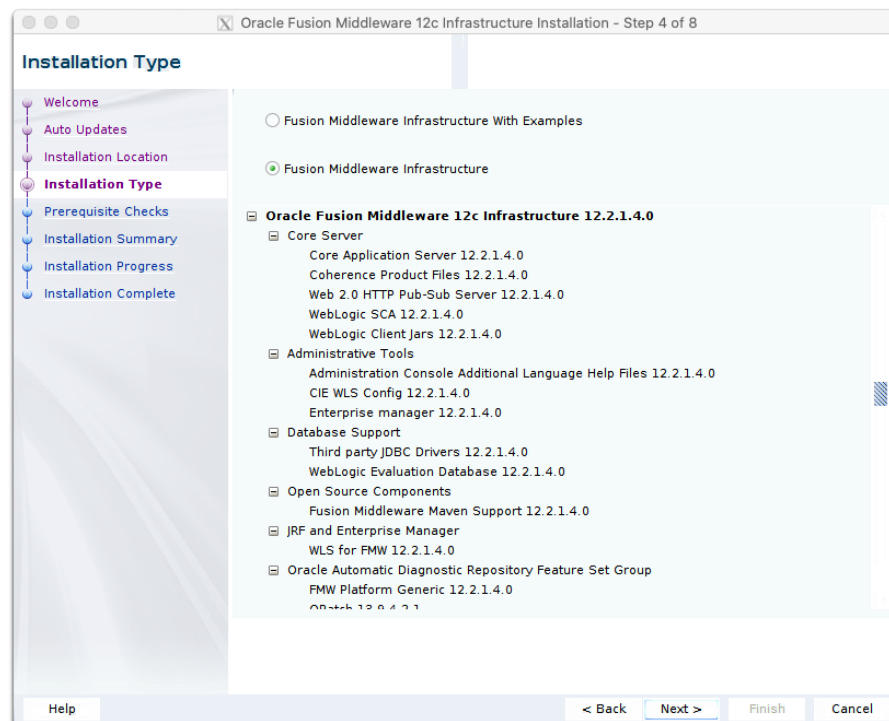
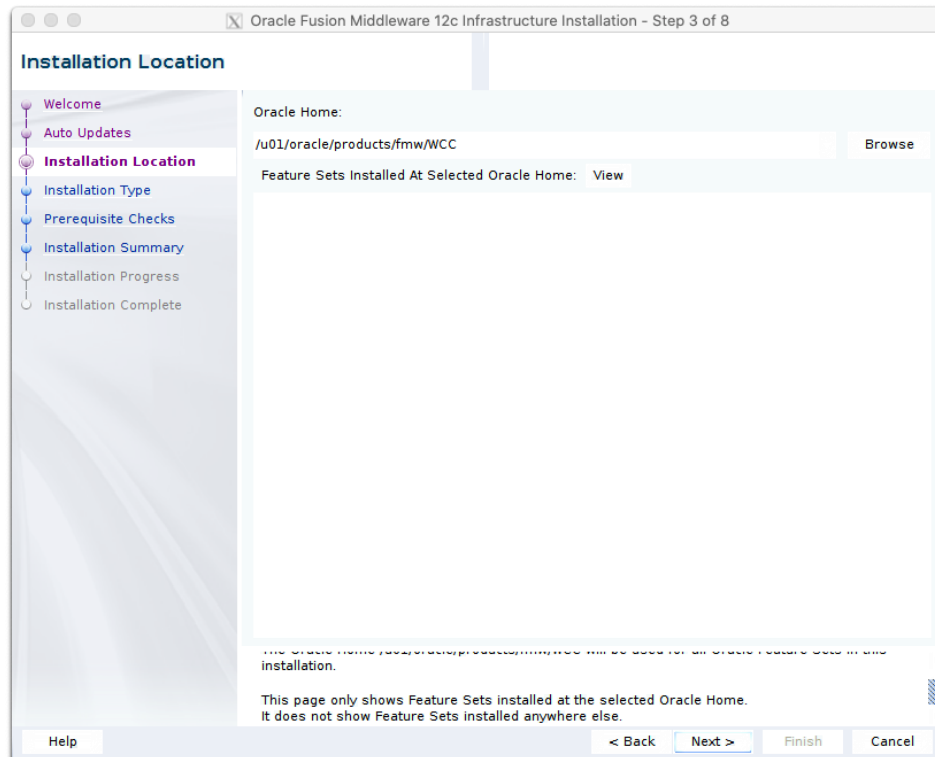
Se realizo la instalación del componente Oracle JDK version 1.8.0_311 sobre el servidor **gestormdqa**. En la ruta `/u01/oracle/products/jdk`

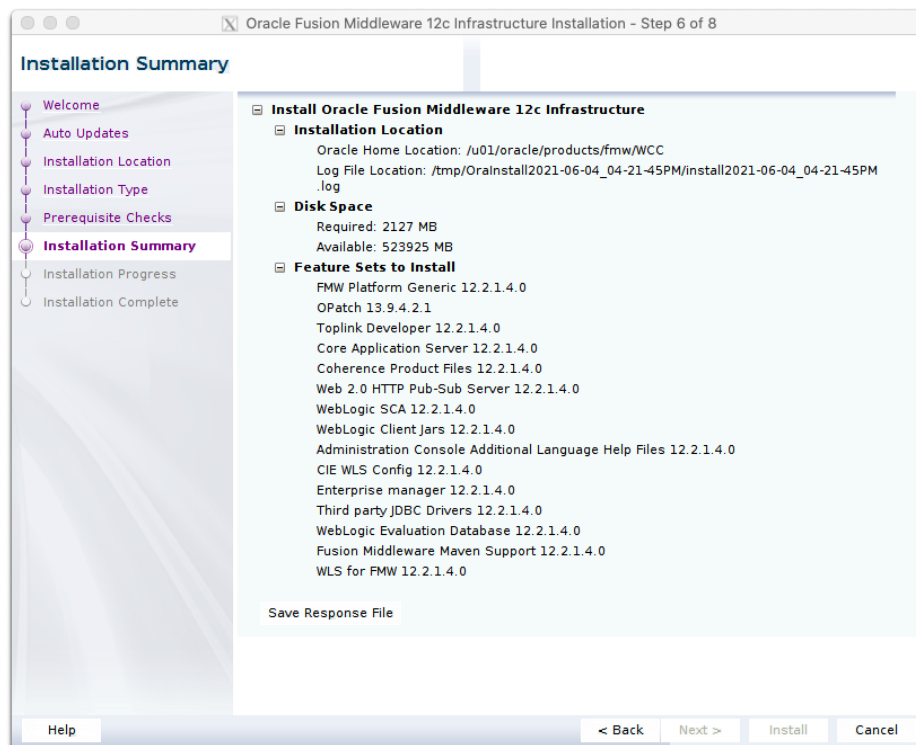
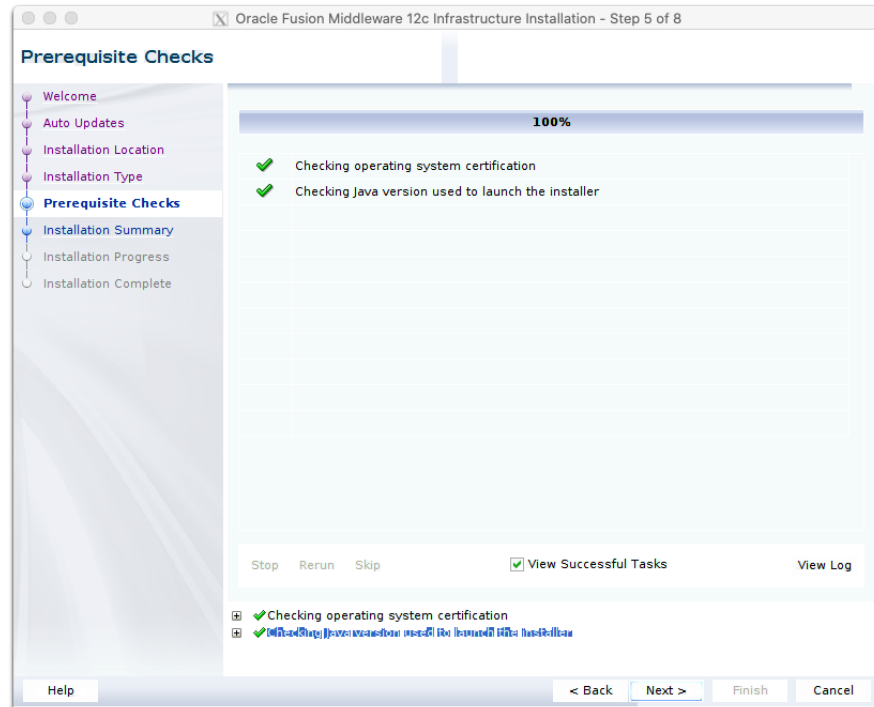
```
[oracle@gestormdqa products]$ java -version
java version "1.8.0_311"
Java(TM) SE Runtime Environment (build 1.8.0_311-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.311-b11, mixed mode)
```

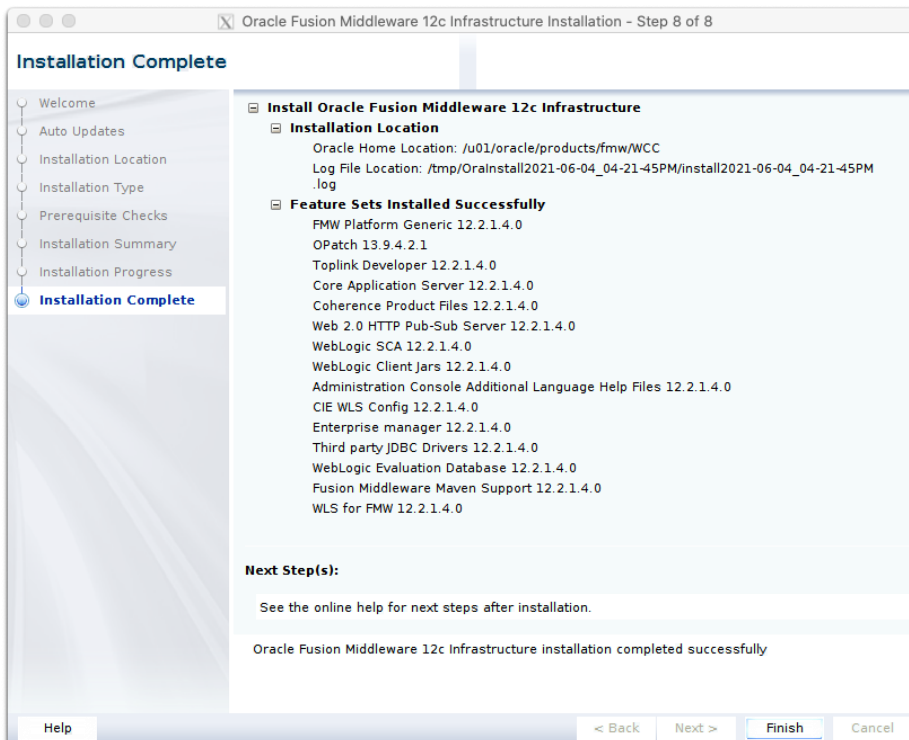
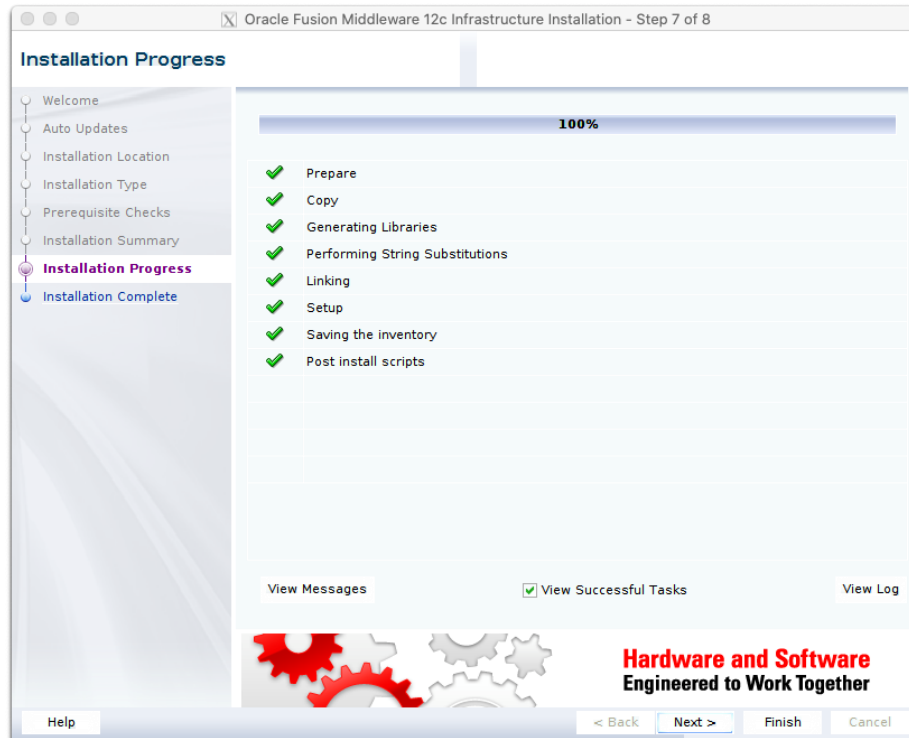
Instalación Oracle Fusion Middleware Infrastructure:



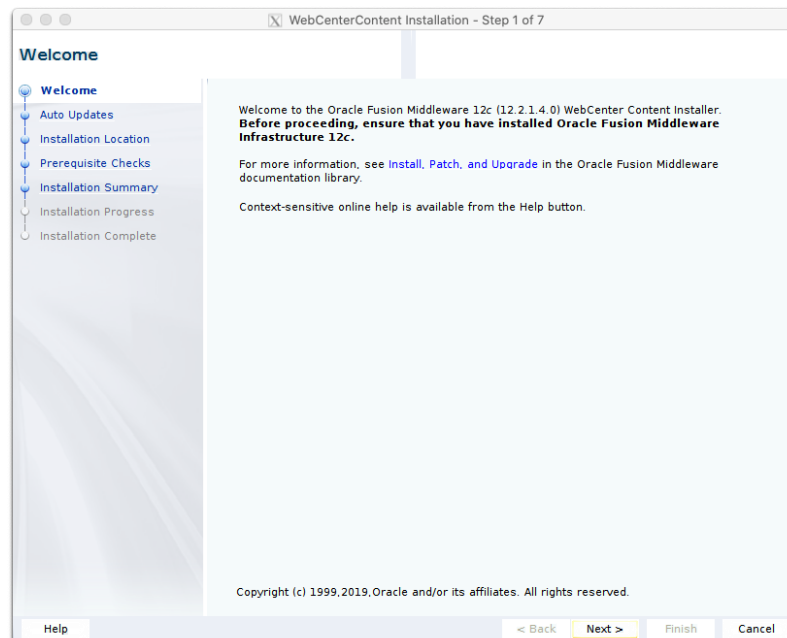
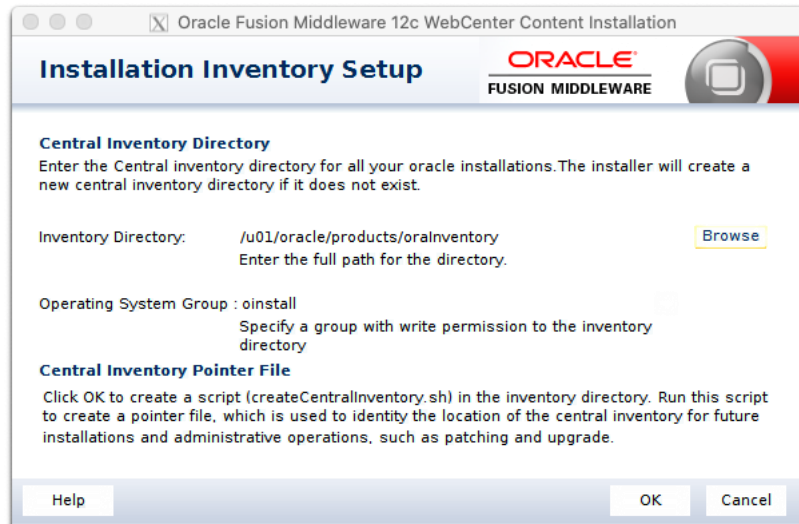








Instalación Oracle WebCenter Content:



WebCenterContent Installation - Step 2 of 7

Auto Updates

Welcome

- Auto Updates**
- Installation Location
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

☒ Skip Auto Updates

☐ Select patches from directory

Location:

☐ Search My Oracle Support for Updates

Username:

Password:

WebCenterContent Installation - Step 3 of 7

Installation Location

Welcome

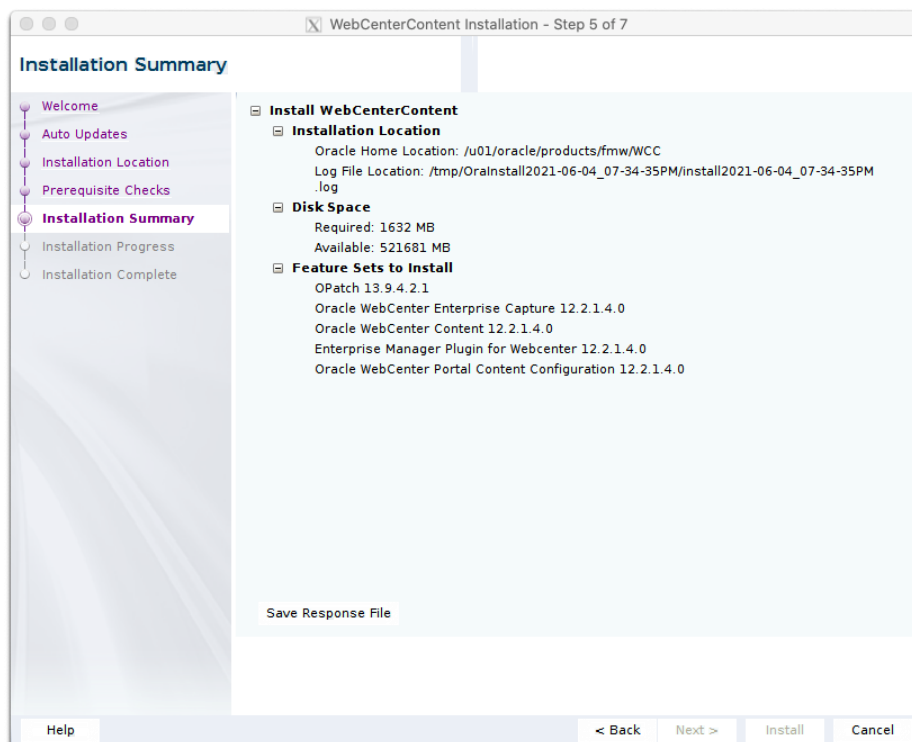
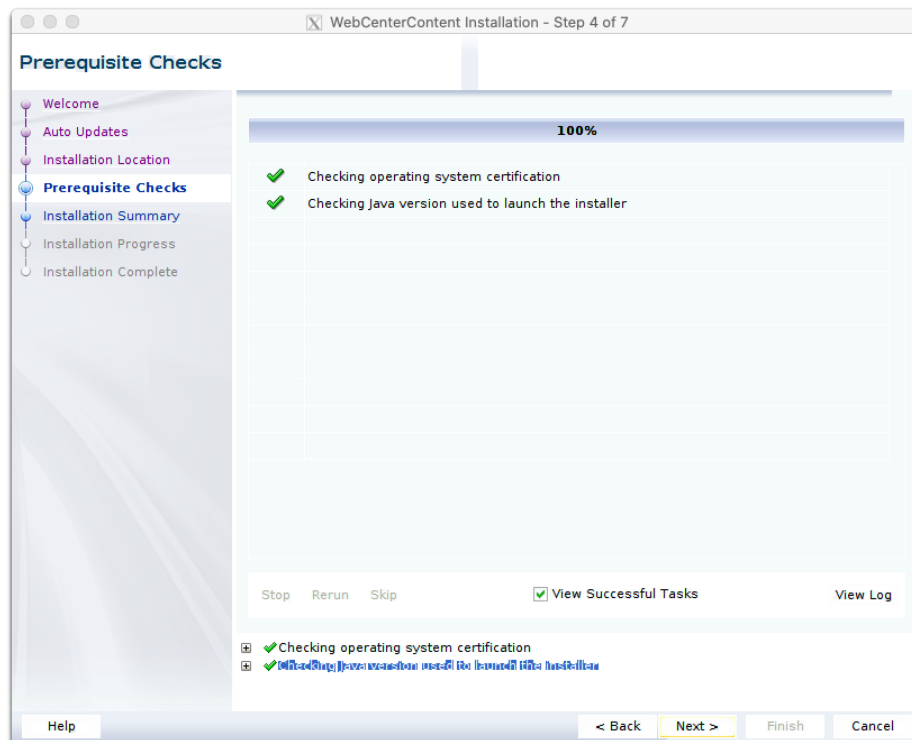
- Auto Updates**
- Installation Location**
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

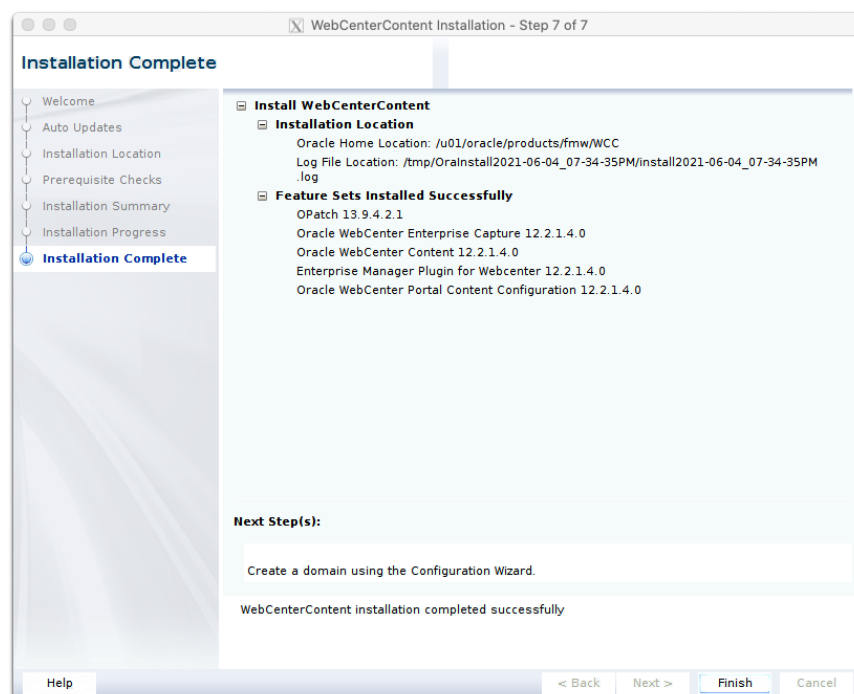
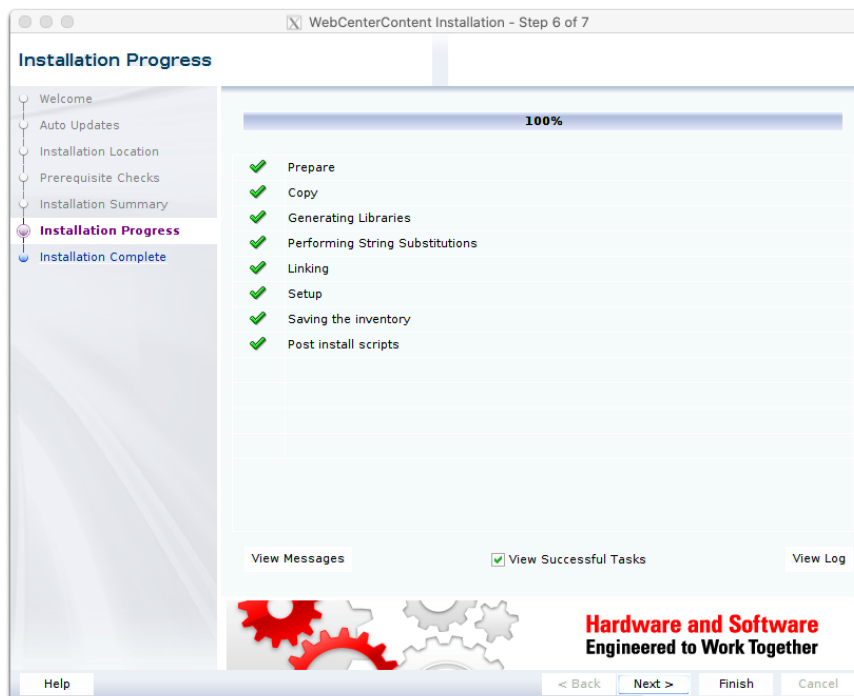
Oracle Home:

Feature Sets Installed At Selected Oracle Home:

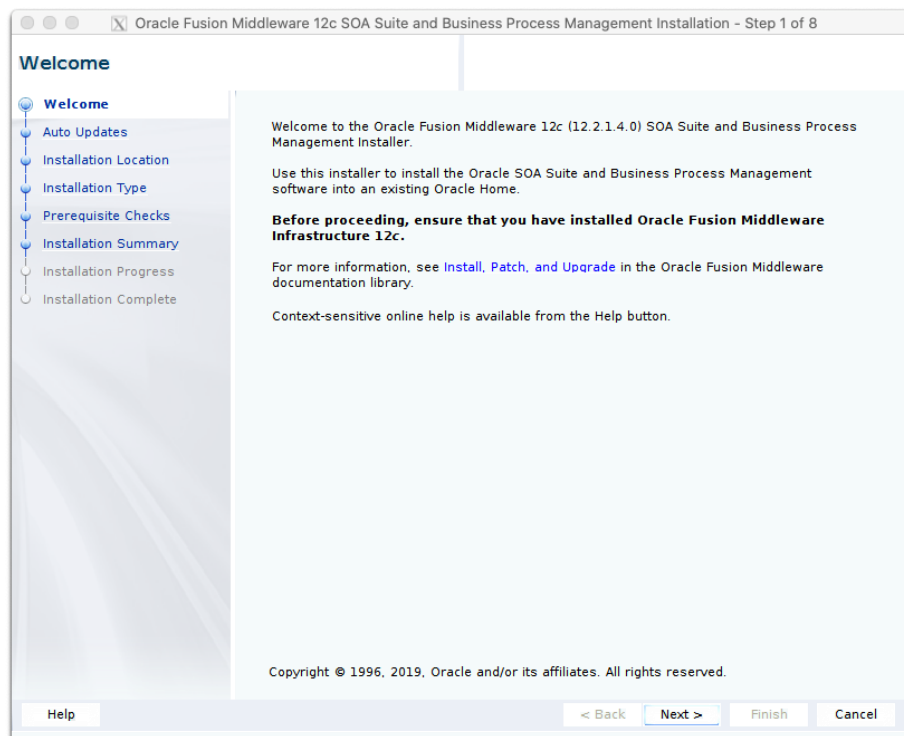
The Oracle Home /path/to/oracle/home/ will be used for all Oracle Feature Sets in this installation.

This page only shows Feature Sets installed at the selected Oracle Home. It does not show Feature Sets installed anywhere else.





Instalación Oracle SOA Suite:



Oracle Fusion Middleware 12c SOA Suite and Business Process Management Installation - Step 2 of 8

Auto Updates

- Welcome
- Auto Updates**
- Installation Location
- Installation Type
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

☒ Skip Auto Updates

☐ Select patches from directory

Location: [Browse](#)

☐ Search My Oracle Support for Updates

Username:

Password:

[Proxy Settings](#) [Test Connection](#)

Search

Oracle Fusion Middleware 12c SOA Suite and Business Process Management Installation - Step 3 of 8

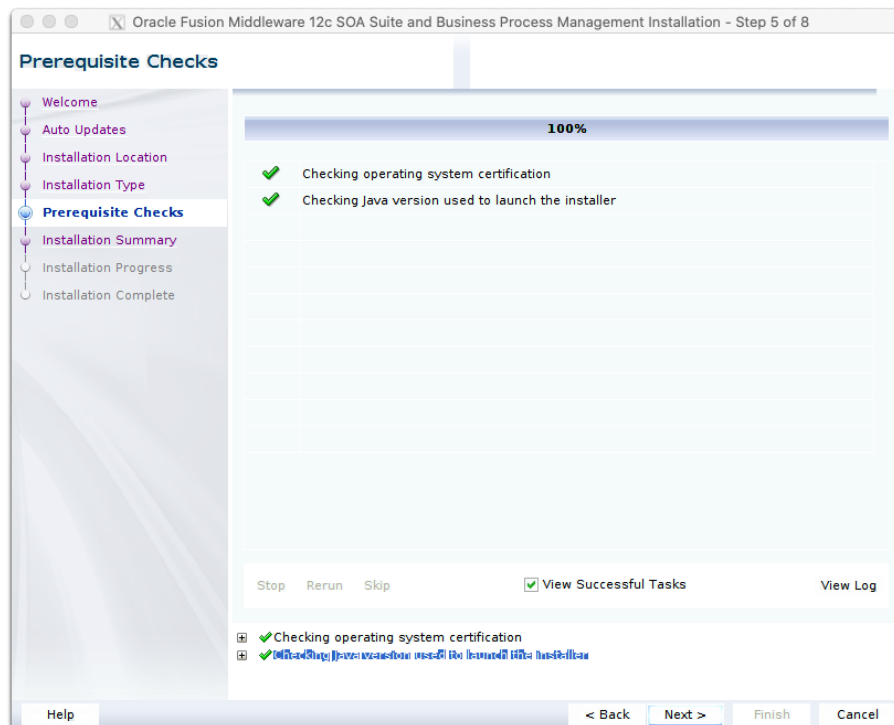
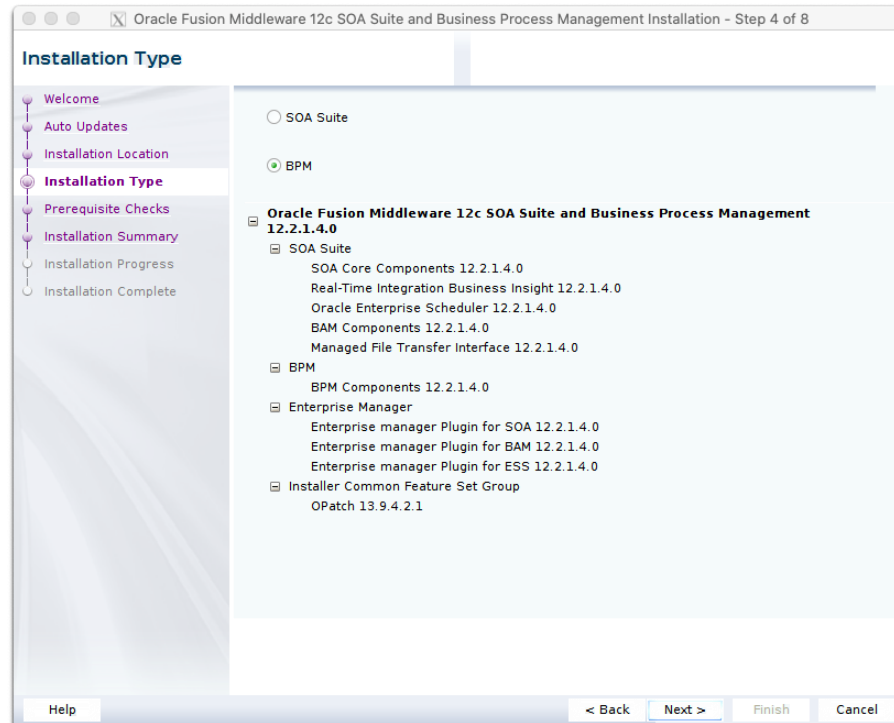
Installation Location

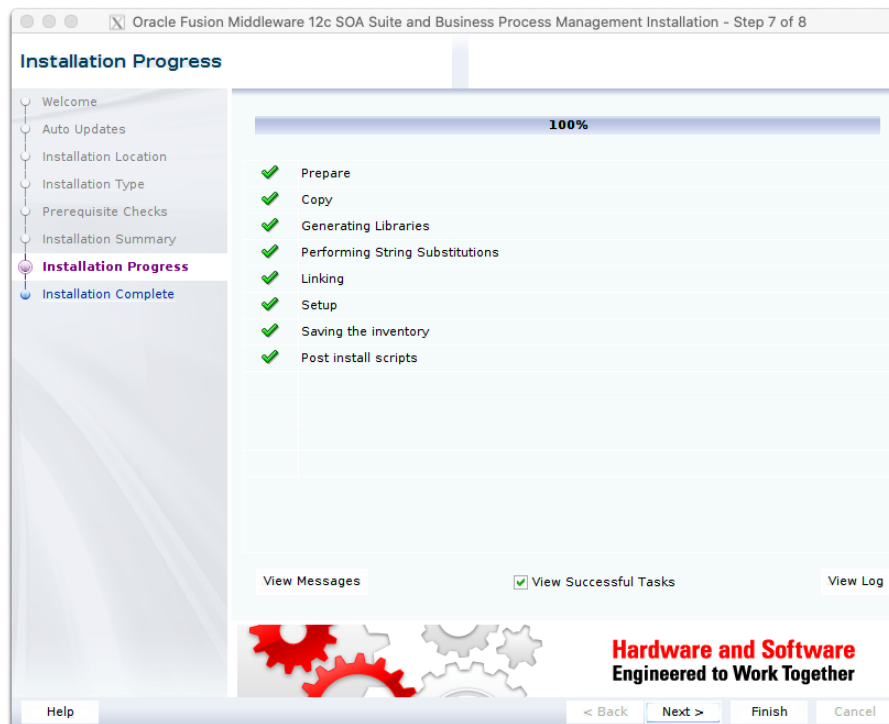
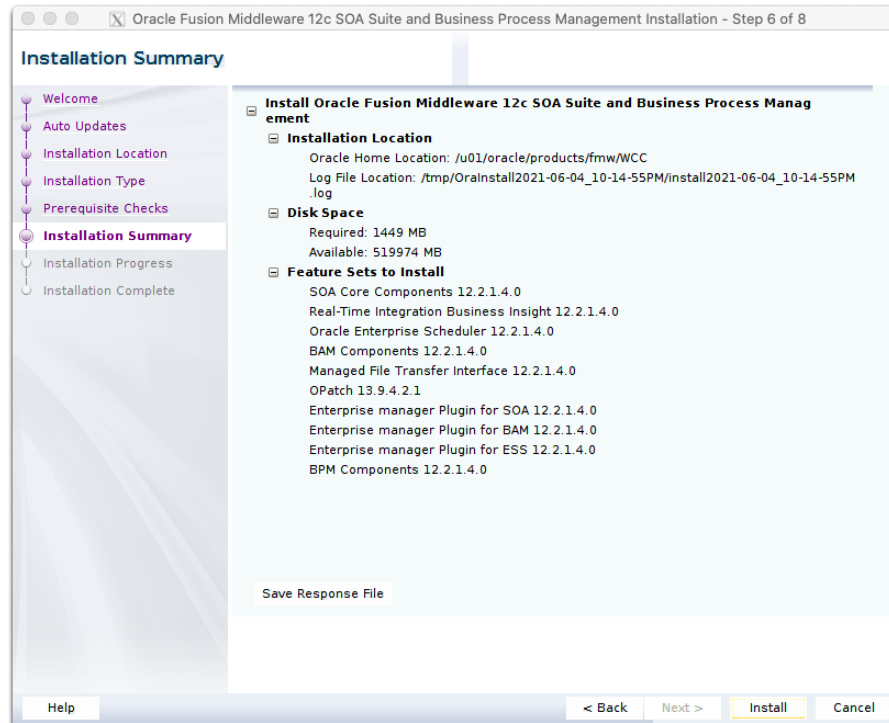
- Welcome
- Auto Updates
- Installation Location**
- Installation Type
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

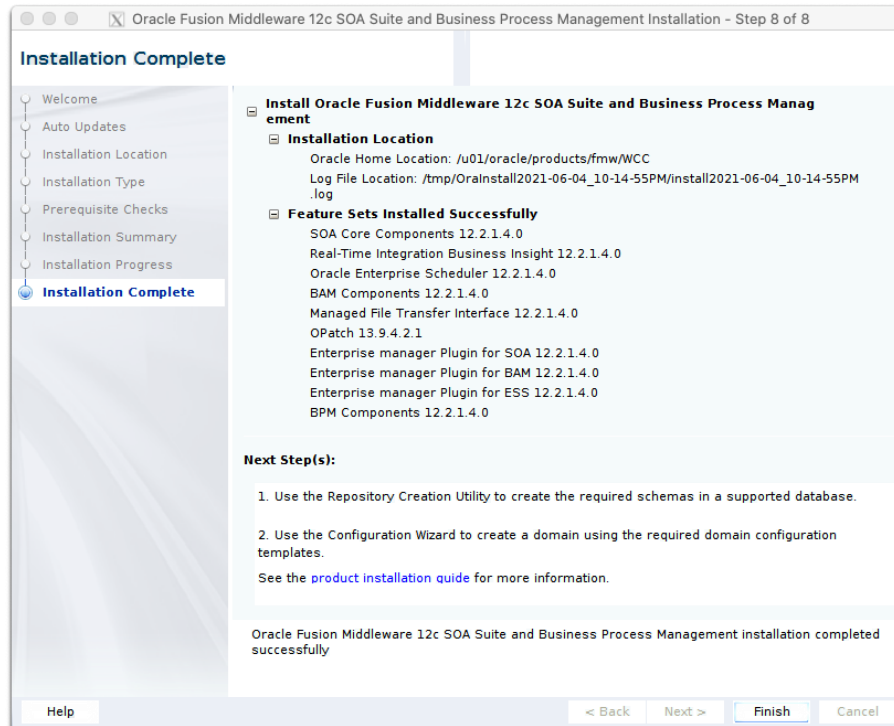
Oracle Home: [Browse](#)

Feature Sets Installed At Selected Oracle Home: [View](#)

This page only shows Feature Sets installed at the selected Oracle Home. It does not show Feature Sets installed anywhere else.

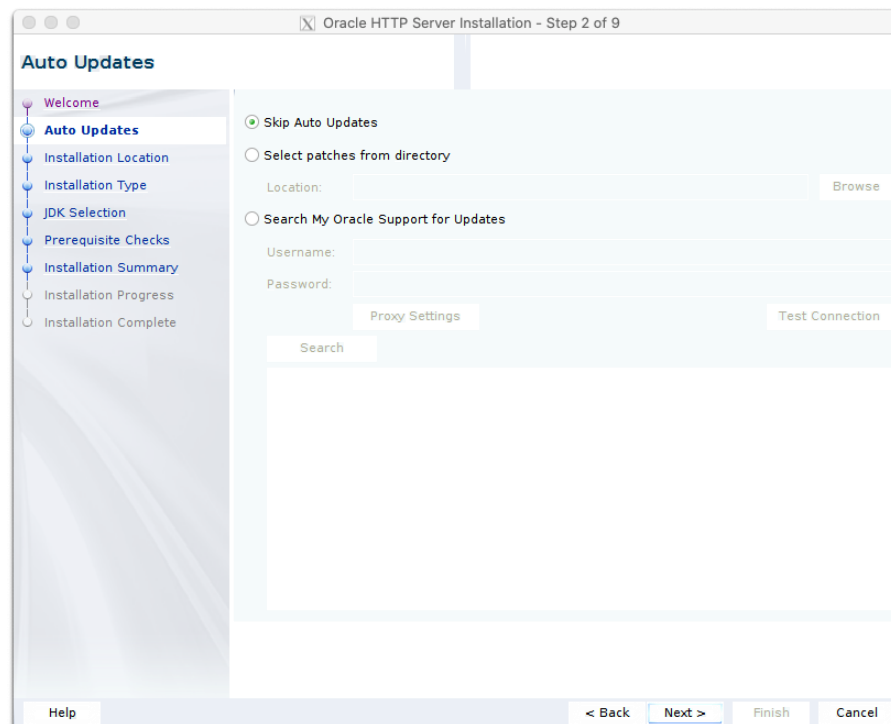


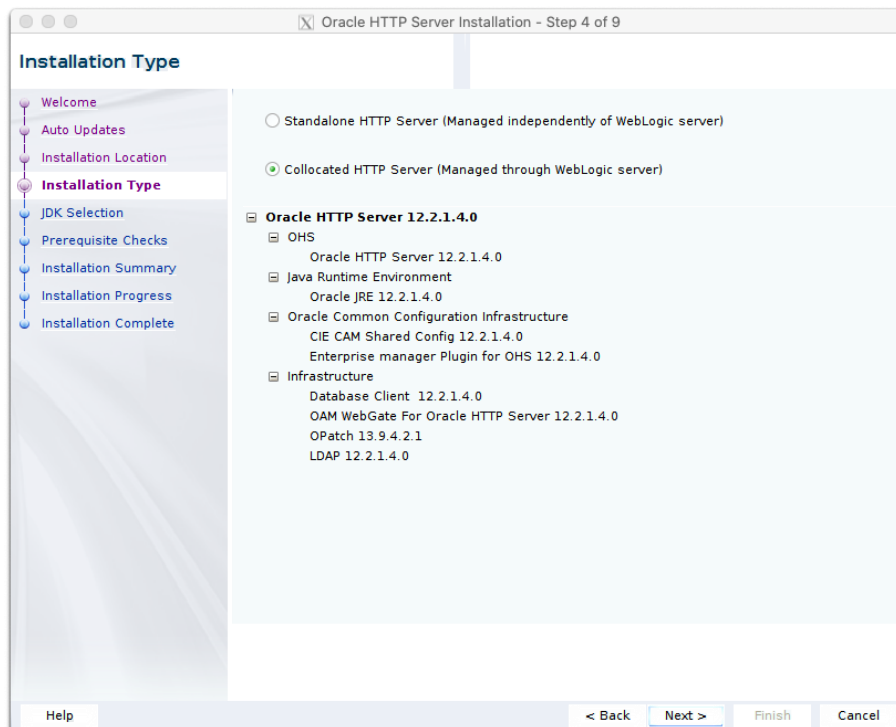
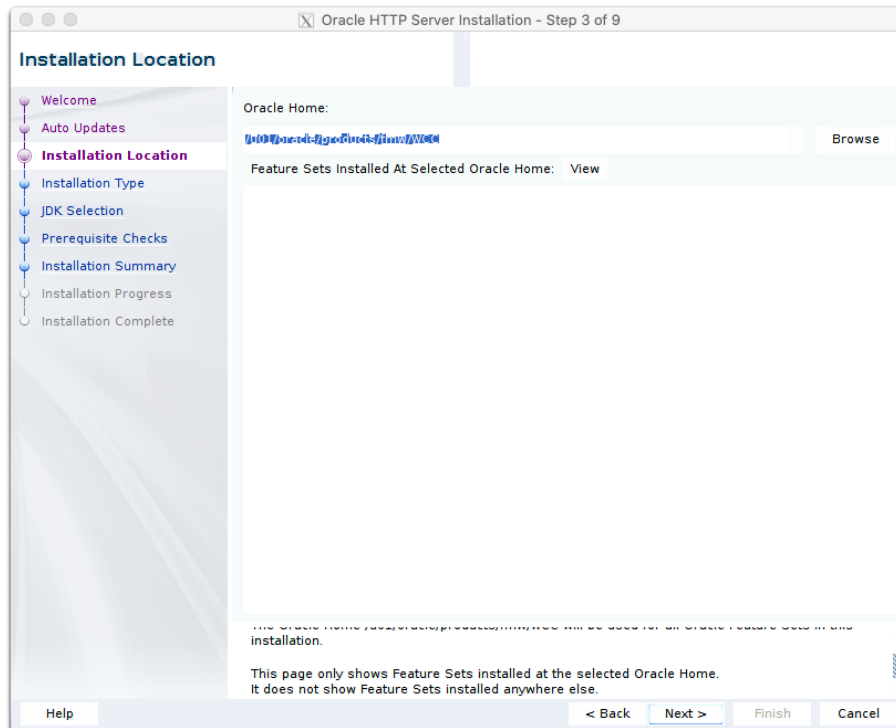


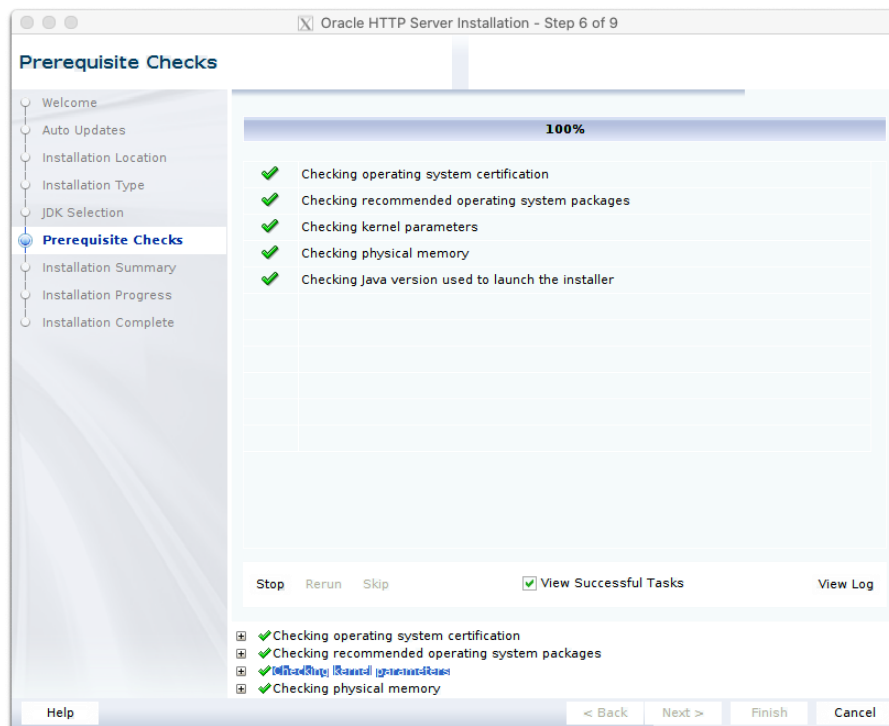
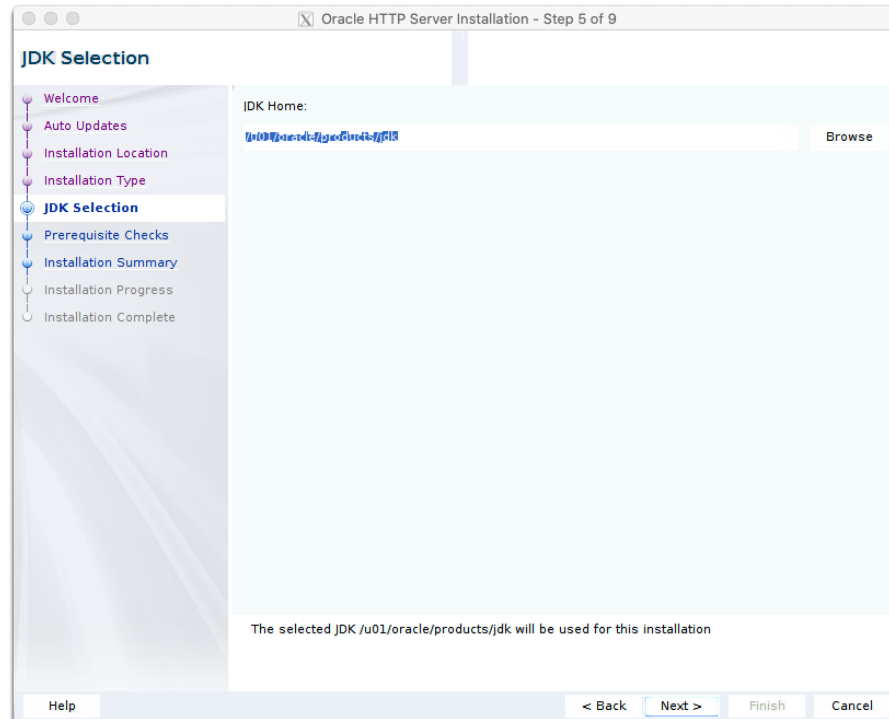


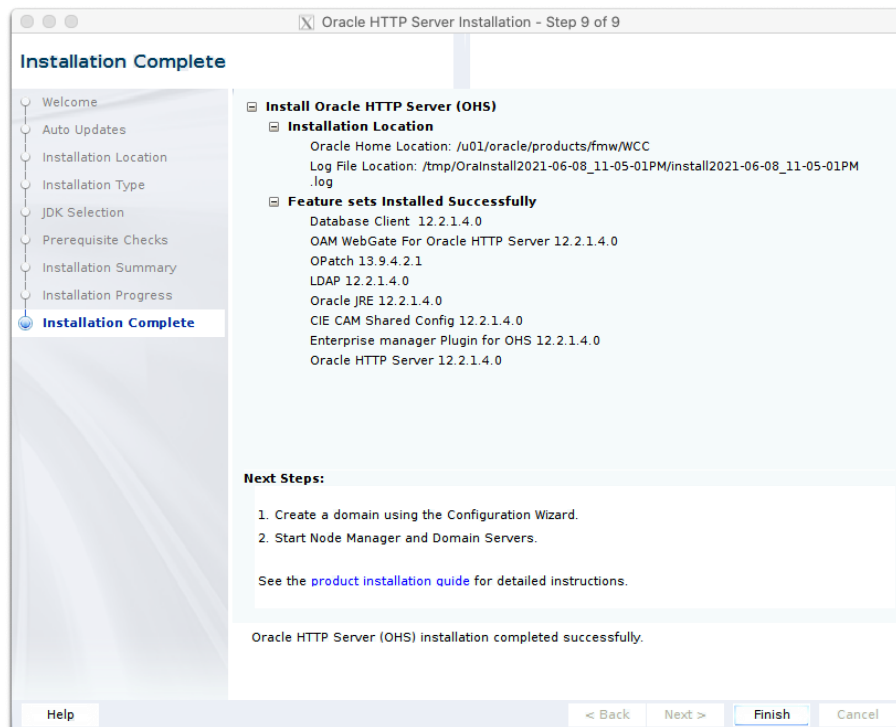
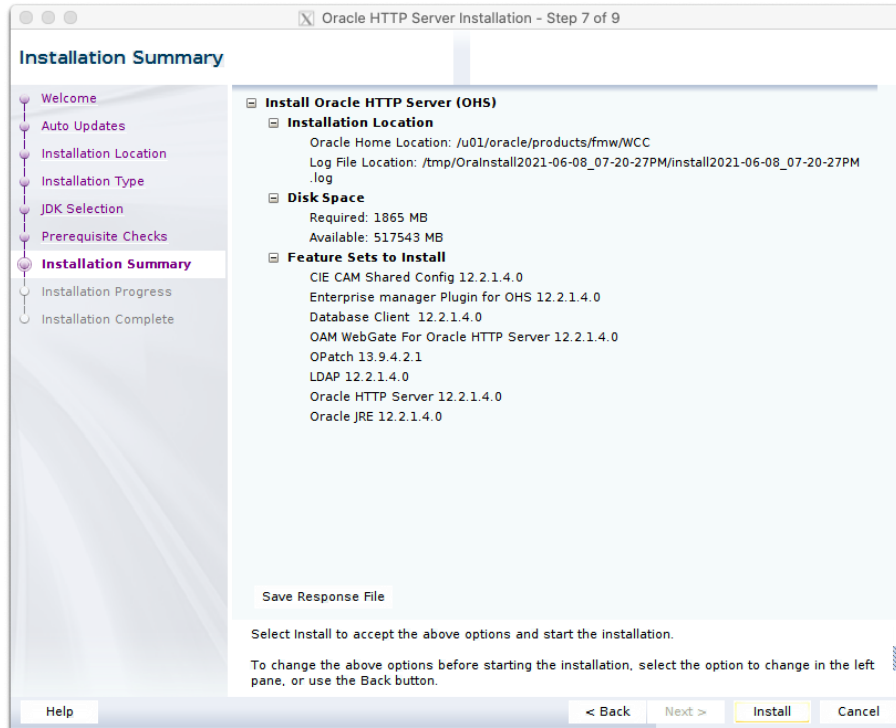
Instalación Oracle OHS:



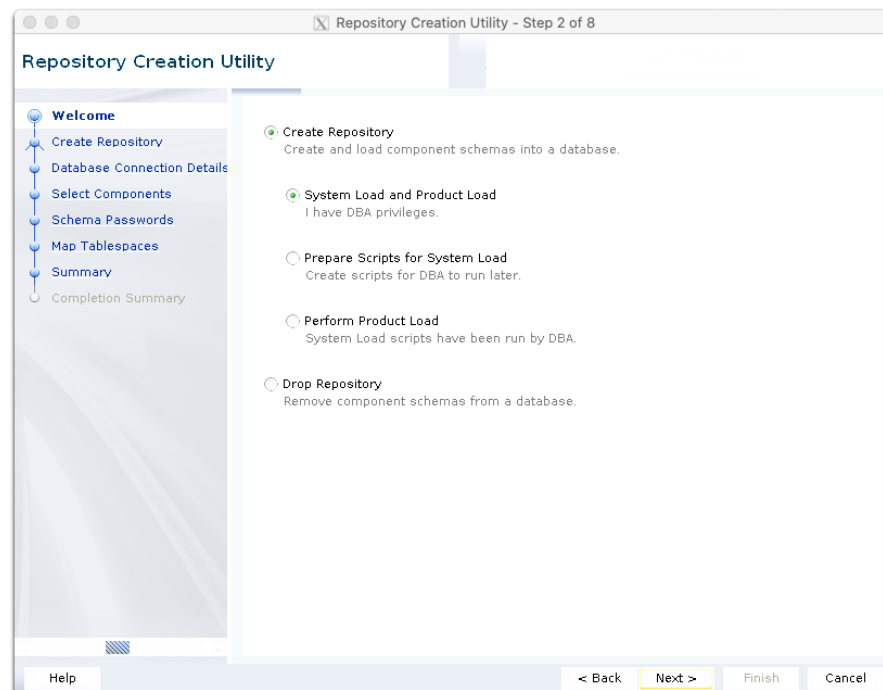
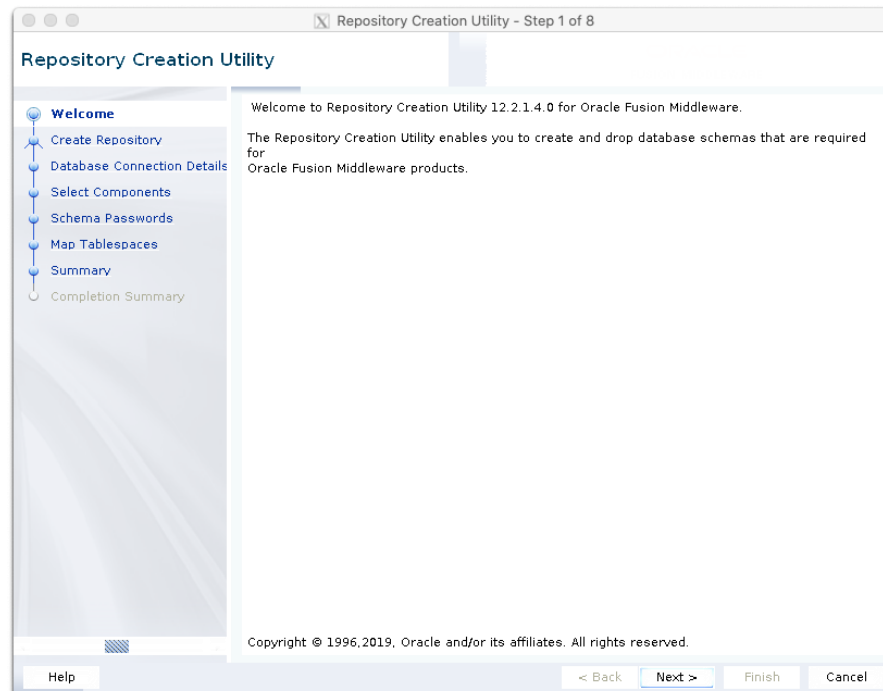








Ejecución RCU:



Repository Creation Utility - Step 3 of 8

Repository Creation Utility

Database Type: Oracle Database

Connection String Format: ☒ Connection Parameters ☐ Connection String

Connect String

Host Name: 10.160.4.48

Port: 1521

Service Name: wccinfra

Username: sys

Password:

Role: SYSDBA

Help < Back Next > Finish Cancel

Repository Creation Utility - Checking Prerequisites

Checking Global Prerequisites

- ✓ Initializing repository configuration metadata 00:06.620(sec)
- ✓ Obtain properties of the specified database 00:00.200(ms)
- ✓ Check requirement for specified database 00:01.904(sec)

Operation completed. Click OK to continue to next page.

OK

Repository Creation Utility - Step 4 of 8

Repository Creation Utility

Specify a unique prefix for all schemas created in this session, so you can easily locate, reference, and manage the schemas later.

☐ Select existing prefix

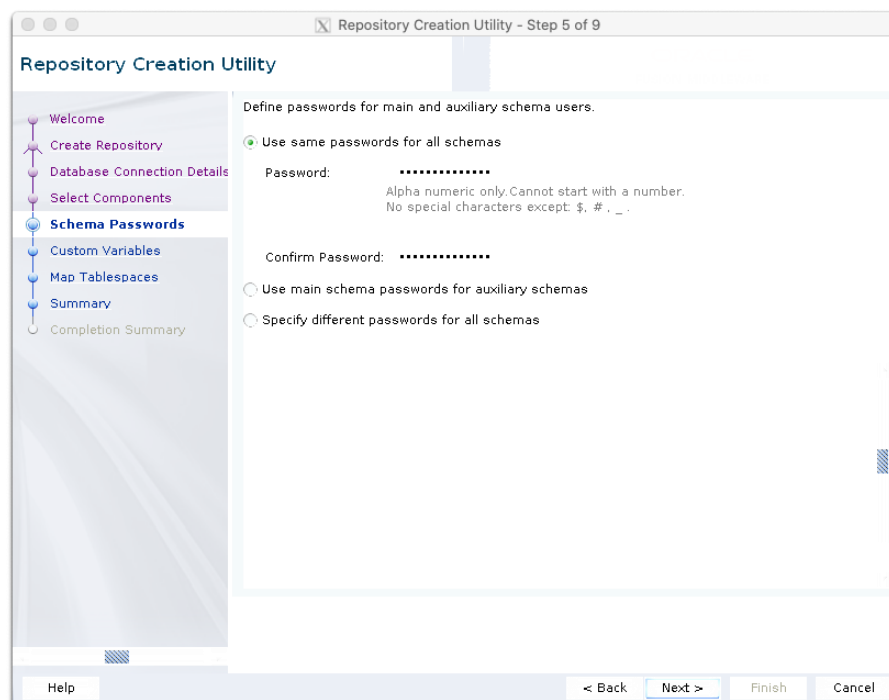
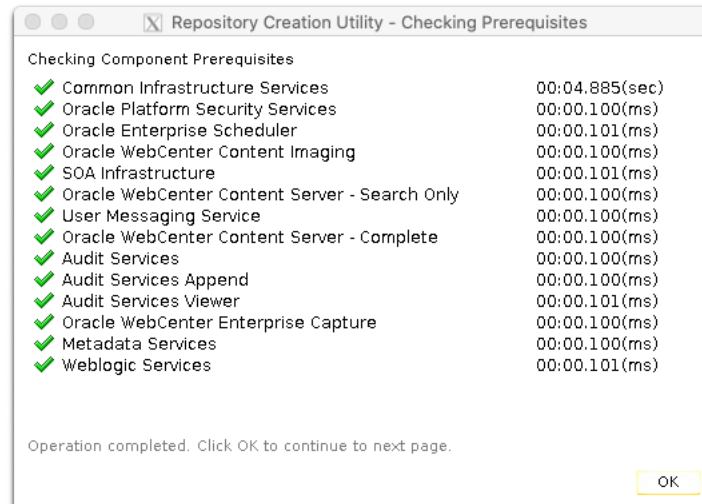
☒ Create new prefix: WCCQA

Alpha numeric only. Cannot start with a number. No special ...

Component	Schema Owner
☒ Common Infrastructure Services *	WCCQA_STB
☒ Oracle Enterprise Scheduler	WCCQA_ESS
☒ Oracle Platform Security Services	WCCQA_OPSS
☒ User Messaging Service	WCCQA_UMS
☒ Audit Services	WCCQA_IAU
☒ Audit Services Append	WCCQA_IAU_APPEND
☒ Audit Services Viewer	WCCQA_IAU_VIEWER
☒ Metadata Services	WCCQA_MDS
☒ Weblogic Services *	WCCQA_WLS
☒ SOA Suite	
☒ SOA Infrastructure	WCCQA_SOAINFRA
☒ WebCenter Content	
☒ Oracle WebCenter Content Imaging	WCCQA_IPM
☒ Oracle WebCenter Content Server - Search ...	WCCQA_OCSSEARCH
☒ Oracle WebCenter Content Server - Complete	WCCQA_OCS
☒ Oracle WebCenter Enterprise Capture	WCCQA_CAPTURE

* Mandatory component. Mandatory components cannot be deselected.

Help < Back Next > Finish Cancel



Repository Creation Utility - Step 6 of 9

Repository Creation Utility

Enter value for the following custom variables.

Component	Custom Variable	Medium	Value
SOA Infrastructure	Database Profile	Medium	No
	Healthcare Integration	No	

Help < Back Next > Finish Cancel

Repository Creation Utility - Step 7 of 9

Repository Creation Utility

Default and temporary tablespaces for the selected components appear in the table below. To create new tablespaces or modify existing tablespaces, use the Manage Tablespaces Button

Manage Tablespaces

Component	Schema Owner	Default Tablespace	Temp Tablespace
Common Infrastructu...	WCCQA_STB	*WCCQA_STB	*WCCQA_IAS_TEMP
Oracle Enterprise Sc...	WCCQA_ESS	*WCCQA_ESS	*WCCQA_IAS_TEMP
Oracle Platform Secu...	WCCQA_OPSS	*WCCQA_IAS_OPSS	*WCCQA_IAS_TEMP
Oracle WebCenter Co...	WCCQA_IPM	*WCCQA_IPM	*WCCQA_IPM_TEMP
SOA Infrastructure	WCCQA_SOAINFRA	*WCCQA_SOAINFRA	*WCCQA_IAS_TEMP
Oracle WebCenter Co...	WCCQA_OCSSEARCH	*WCCQA_OCSSEARCH	*WCCQA_OCSSEARCH...
User Messaging Serv...	WCCQA_UMS	*WCCQA_IAS_UMS	*WCCQA_IAS_TEMP
Oracle WebCenter Co...	WCCQA_OCS	*WCCQA_OCS	*WCCQA_OCS_TEMP
Audit Services	WCCQA_IAU	*WCCQA_IAU	*WCCQA_IAS_TEMP
Audit Services Append	WCCQA_IAU_APPEND	*WCCQA_IAU	*WCCQA_IAS_TEMP
Audit Services Viewer	WCCQA_IAU_VIEWER	*WCCQA_IAU	*WCCQA_IAS_TEMP
Oracle WebCenter En...	WCCQA_CAPTURE	*WCCQA_CAPTURE	*WCCQA_CAPTURE_TE...
Metadata Services	WCCQA_MDS	*WCCQA_MDS	*WCCQA_IAS_TEMP
Weblogic Services	WCCQA_WLS	*WCCQA_WLS	*WCCQA_IAS_TEMP

* Default tablespaces (specified in the configuration files) are to be created upon confirmation.

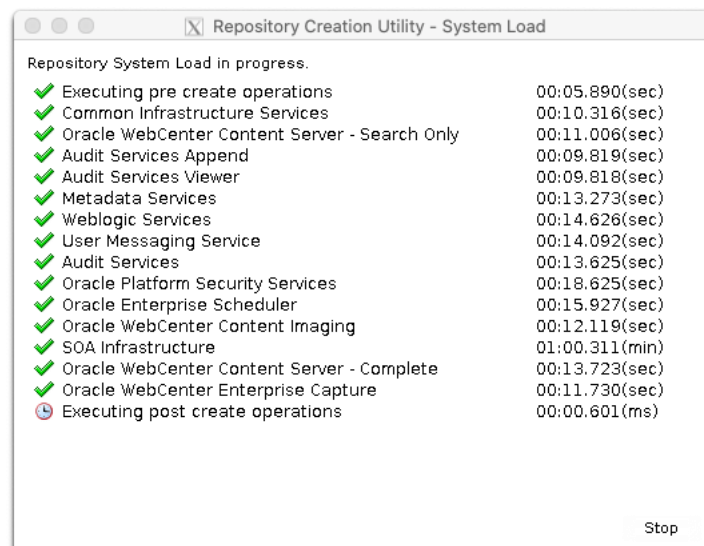
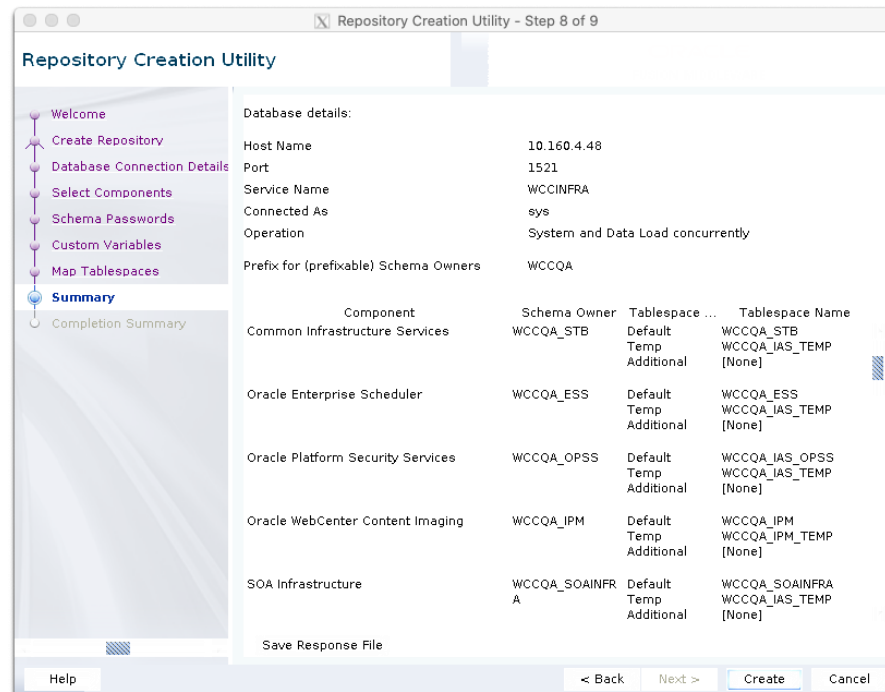
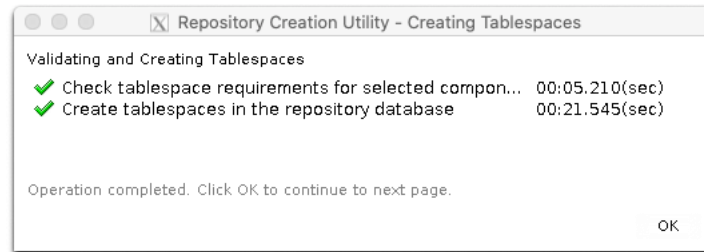
Help < Back Next > Finish Cancel

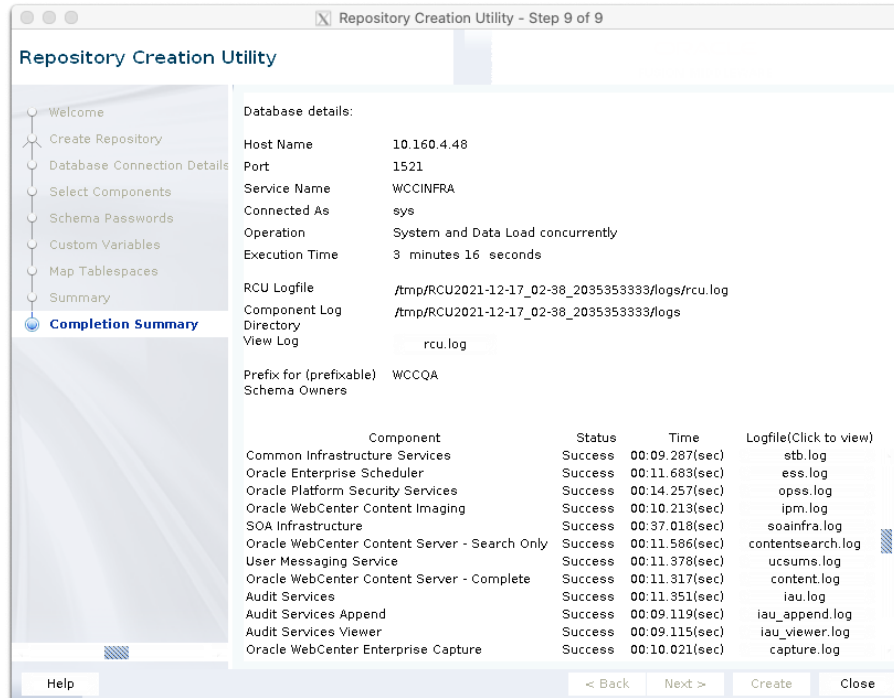
Repository Creation Utility - Confirmation

? Any tablespaces that do not already exist in the selected schemas will be created.

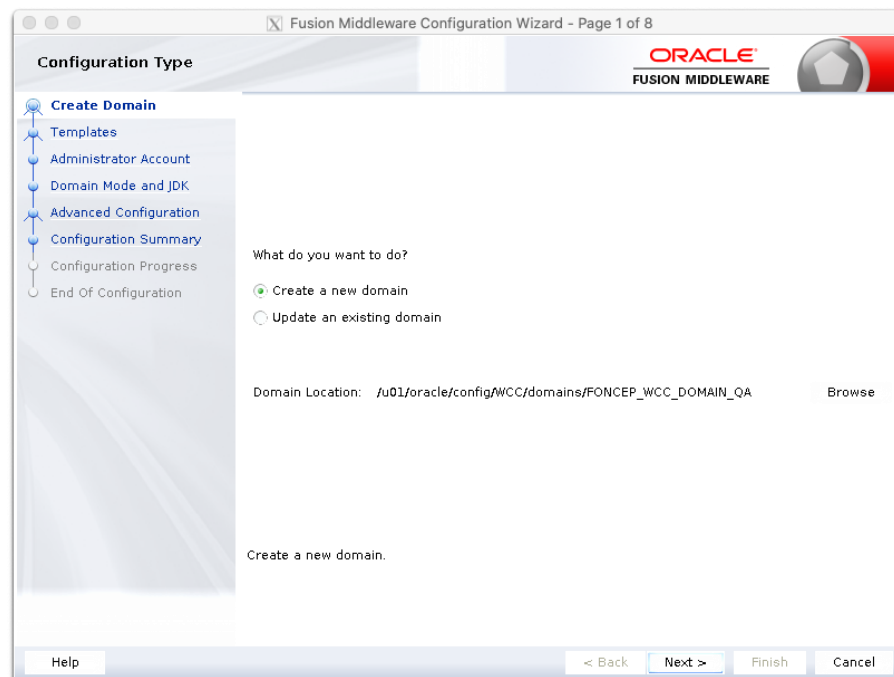
Click OK to create tablespaces.
Click Cancel to return to the wizard.

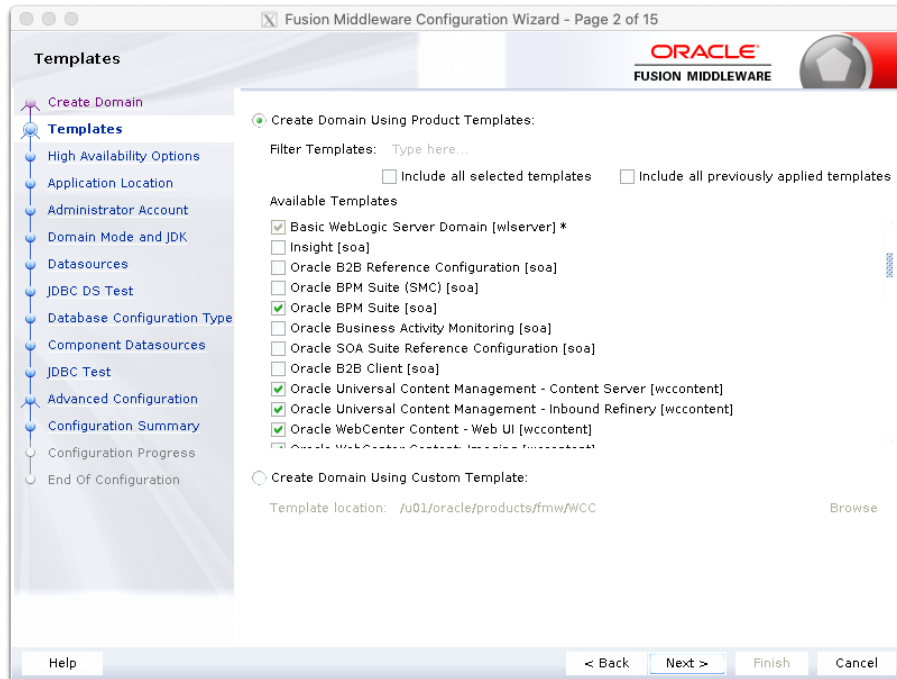
OK Cancel





Creación de Dominio WLS:





Fusion Middleware Configuration Wizard - Page 4 of 17

Application Location

Oracle
FUSION MIDDLEWARE

- Create Domain
- Templates
- High Availability Options
- Application Location**
- Administrator Account
- Domain Mode and JDK
- Datasources
- JDBC DS Test
- Database Configuration Type
- Component Datasources
- JDBC Test
- Credentials
- Keystore
- Advanced Configuration
- Configuration Summary
- Configuration Progress
- End Of Configuration

Domain name: FONCEP_WCC_DOMAIN_QA

Domain location: /u01/oracle/config/WCC/domains

Application location: /u01/oracle/config/WCC/domains/applications Browse

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 4 of 12

Administrator Account

Oracle
FUSION MIDDLEWARE

- Create Domain
- Templates
- Application Location
- Administrator Account**
- Domain Mode and JDK
- Database Configuration Type
- Component Datasources
- JDBC Test
- Advanced Configuration
- Configuration Summary
- Configuration Progress
- End Of Configuration

Name weblogic

Password

Confirm Password

Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 5 of 12

Domain Mode and JDK

Oracle
FUSION MIDDLEWARE

[Create Domain](#)
[Templates](#)
[Application Location](#)
[Administrator Account](#)
Domain Mode and JDK
[Database Configuration Type](#)
[Component Datasources](#)
[JDBC Test](#)
[Advanced Configuration](#)
[Configuration Summary](#)
[Configuration Progress](#)
[End Of Configuration](#)

Domain Mode

☐ Development
 Utilize boot properties for username and password, and poll for applications to deploy.

☒ Production
 Require the entry of a username and password, and do not poll for applications to deploy.

JDK

☒ Oracle HotSpot 1.8.0_291 /u01/oracle/products/jdk
☐ Other JDK Location: Browse

[Help](#)
[< Back](#)
[Next >](#)
[Finish](#)
[Cancel](#)

Fusion Middleware Configuration Wizard - Page 7 of 17

JDBC Data Sources

Oracle
FUSION MIDDLEWARE

[Create Domain](#)
[Templates](#)
[High Availability Options](#)
[Application Location](#)
[Administrator Account](#)
[Domain Mode and JDK](#)
Datasources
[JDBC DS Test](#)
[Database Configuration Type](#)
[Component Datasources](#)
[JDBC Test](#)
[Credentials](#)
[Keystore](#)
[Advanced Configuration](#)
[Configuration Summary](#)
[Configuration Progress](#)
[End Of Configuration](#)

Vendor: Oracle Driver: *Oracle's Driver (Thin) for Service connections; Ve

☒ Connection Parameters ☐ Connection URL String

Host Name: 10.160.4.48

DBMS/Service: wccinfra Port: 1521

Username: WCCQA_MDS Password:

Oracle RAC configuration for data sources:

☐ Convert to GridLink ☐ Convert to RAC multi data source ☐ Don't convert

Edits to the data above will affect all checked rows in the table below.

	Data Source	DBMS/Service	Host Name	Port	Username	Password
☒	mds-WCCUIMDSREPO	wccinfra	10.160.4.48	1521	WCCQA_MDS	

[Help](#)
[< Back](#)
[Next >](#)
[Finish](#)
[Cancel](#)

Fusion Middleware Configuration Wizard - Page 8 of 17

JDBC Data Sources Test

ORACLE FUSION MIDDLEWARE

- Create Domain
- Templates
- High Availability Options
- Application Location
- Administrator Account
- Domain Mode and JDK
- Datasources
- JDBC DS Test**
- Database Configuration Type
- Component Datasources
- JDBC Test
- Credentials
- Keystore
- Advanced Configuration
- Configuration Summary
- Configuration Progress
- End Of Configuration

Status	Data Source	JDBC Connection URL
☒	mds-WCCUIMDSREPO	jdbc:oracle:thin:@//10.160.4.48:1521/wccinfra

Test Selected Connections Cancel Testing

Connection Result Log

Data Source=mds-WCCUIMDSREPO
Driver=oracle.jdbc.OracleDriver
URL=jdbc:oracle:thin:@//10.160.4.48:1521/wccinfra
User=WCCQA_MDS
Password=*****
SQL Test=SELECT 1 FROM MDS_COMPONENTS

CFGFWK-64213: Test Successful!
CFGFWK-64213: JDBC connection test was successful.

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 9 of 17

Database Configuration Type

ORACLE FUSION MIDDLEWARE

- Create Domain
- Templates
- High Availability Options
- Application Location
- Administrator Account
- Domain Mode and JDK
- Datasources
- JDBC DS Test
- Database Configuration Type**
- Component Datasources
- JDBC Test
- Credentials
- Keystore
- Advanced Configuration
- Configuration Summary
- Configuration Progress
- End Of Configuration

Specify AutoConfiguration Options Using:

☒ RCU Data ☐ Manual Configuration

Enter the database connection details using the schema credentials corresponding to Common Infrastructure Services component in the Repository Creation Utility. The Wizard uses this connection to automatically configure the datasources required for components in this domain.

Vendor: Oracle Driver: *Oracle's Driver (Thin) for Service connections; ...

☒ Connection Parameters ☐ Connection URL String

Host Name: 10.160.4.48
DBMS/Service: wccinfra Port: 1521
Schema Owner: WCCQA_STB Schema Password: *****

Get RCU Configuration Cancel

Connection Result Log

Successfully Done.

Click "Next" button to continue.

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 10 of 17

JDBC Component Schema

Vendor: Driver:

☒ Connection Parameters ☐ Connection URL String

Host Name: DBMS/Service: Port: Schema Owner: Schema Password:

Oracle RAC configuration for component schemas:

☐ Convert to GridLink ☐ Convert to RAC multi data source ☐ Don't convert

Edits to the data above will affect all checked rows in the table below.

☐	Component Schema	DBMS/Service	Host Name	Port	Schema Ow...	Schema Pasw...
☐	UCM Schema	WCCINFRA	10.160.4.48	1521	WCCQA_OCS	
☐	SOA EDN (XA)	WCCINFRA	10.160.4.48	1521	WCCQA_SOAI	
☐	SOA EDN (Local)	WCCINFRA	10.160.4.48	1521	WCCQA_SOAI	
☐	IPM Schema	WCCINFRA	10.160.4.48	1521	WCCQA_IPM	
☐	LocalSvcTbl Schema	WCCINFRA	10.160.4.48	1521	WCCQA_STB	
☐	User Messaging Ser	WCCINFRA	10.160.4.48	1521	WCCQA_UMS	
☐	SOA (XA)	WCCINFRA	10.160.4.48	1521	WCCQA_SOAI	

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 11 of 17

JDBC Component Schema Test

☒ Status Component Schema JDBC Connection URL

☒	UCM Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA EDN (XA)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA EDN (Local)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	IPM Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	LocalSvcTbl Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	User Messaging Service	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA (XA)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA (Local)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	WLS Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W

Test Selected Connections Cancel Testing

Connection Result Log

Component Schema=UCM Schema
Driver=oracle.jdbc.OracleDriver
URL=jdbc:oracle:thin:@//10.160.4.48:1521/WCCINFRA
User=WCCQA_OCS
Password=*****
SQL Test=select 1 from schema_version_registry where owner=(select user from dual) and mr_type

CFGFWK-64213: Test Successful!
CFGFWK-64213: JDBC connection test was successful
999999

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 12 of 17

Credentials

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Configuration Summary
Configuration Progress
End Of Configuration

+ Add - Delete Discard Changes

Key Name	Username	Password	Store Name
wccadfConnectUser	weblogic	*****	oracle.wcc.security

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 13 of 17

Keystore

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Configuration Summary
Configuration Progress
End Of Configuration

Store Key Name ums/apns Discard Changes

Alias	Trusted Certificate
Alias	

Alias	Private Key	Password	Identity Certificate

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 14 of 26

Advanced Configuration

ORACLE
FUSION MIDDLEWARE

- Create Domain
- Templates
- High Availability Options
- Application Location
- Administrator Account
- Domain Mode and JDK
- Datasources
- JDBC DS Test
- Database Configuration Type
- Component Datasources
- JDBC Test
- Credentials
- Keystore
- Advanced Configuration**
- Administration Server
- Node Manager
- Managed Servers
- Clusters
- Server Templates
- Coherence Clusters
- Machines
- Help

☒ **Administration Server**
Modify Settings

☐ **File Store**
Modify Settings

☒ **Node Manager**
Configure Node Manager

☒ **Topology**
Add, Delete or Modify Settings for Managed Servers, Clusters, Virtual Targets and Coherence

☒ **System Components**
Configure and Target System Components

☐ **Domain Frontend Host Capture**
Configure Domain Frontend Host

☐ **Deployments and Services**
Target to Servers or Clusters

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 15 of 26

Administration Server

ORACLE
FUSION MIDDLEWARE

- Create Domain
- Templates
- High Availability Options
- Application Location
- Administrator Account
- Domain Mode and JDK
- Datasources
- JDBC DS Test
- Database Configuration Type
- Component Datasources
- JDBC Test
- Credentials
- Keystore
- Advanced Configuration
- Administration Server**
- Node Manager
- Managed Servers
- Clusters
- Server Templates
- Coherence Clusters
- Machines
- Help

Server Name

Listen Address All Local Addresses

Listen Port 7001

Enable SSL ☐

SSL Listen Port

Server Groups Unspecified

The name must not be null or empty and may not contain any : , = * ? % / _ cloned.

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 16 of 26

Node Manager

Node Manager Type

☐ Per Domain Default Location

☒ Per Domain Custom Location

Node Manager Home: [Browse](#)

☐ Manual Node Manager Setup

Node Manager Credentials

Username:

Password:

Confirm Password:

Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 17 of 26

Managed Servers

[Add](#) [Clone](#) [Delete](#) [Discard Changes](#)

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WCCADF_server1	All Local Address...	16225	☐	Disabled	UCM-ADF...
UCM_server1	All Local Address...	16200	☐	Disabled	UCM-MGD...
IBR_server1	All Local Address...	16250	☐	Disabled	IBR-MGD...
IPM_server1	All Local Address...	16000	☐	Disabled	IPM-MGD...
SOA_server1	All Local Address...	9103	☐	Disabled	SOA-MGD...
CUST_server1	All Local Address...	9105	☐	Disabled	Unspecified

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 21 of 27

Machines

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Administration Server
Node Manager
Managed Servers
Clusters
Server Templates
Coherence Clusters
Machines
Help

Machine Unix Machine

+ Add X Delete Discard Changes

Name	Enable	Post Bind GID	Enable	Post Bind UID	Node Manager Listen Address	Node Manager
gestormdqa	☐	nobody	☐	nobody	gestormdqa	5556

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 22 of 27

Assign Servers to Machines

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Administration Server
Node Manager
Managed Servers
Clusters
Server Templates
Coherence Clusters
Machines
Help

Servers

Machines

- UnixMachine
 - gestormdqa
 - AdminServer
 - CUST_server1
 - IBR_server1
 - IPM_server1
 - SOA_server1
 - UCM_server1
 - WCCADF_server1

Select **one or more** servers in the left pane and **one** machine in the right pane. Then use the right arrow button (>) to assign the server or servers to the machine.

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 25 of 29

System Components

+ Add - Delete Discard Changes

System Component	Component Type	Restart Interval Seconds	Restart Delay Seconds
ohs1	OHS	3600	0

Navigation: Help < Back Next > Finish Cancel

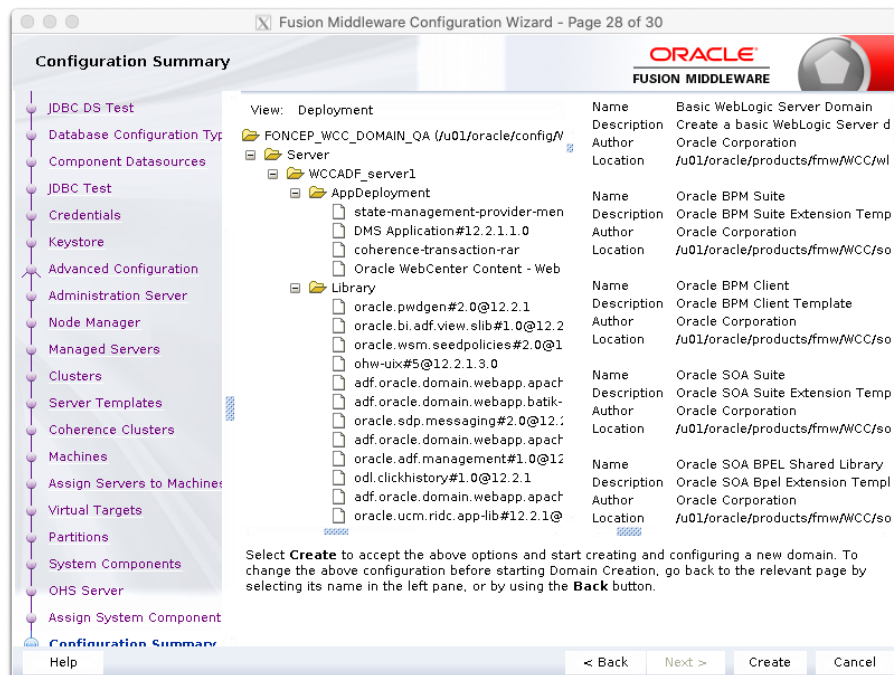
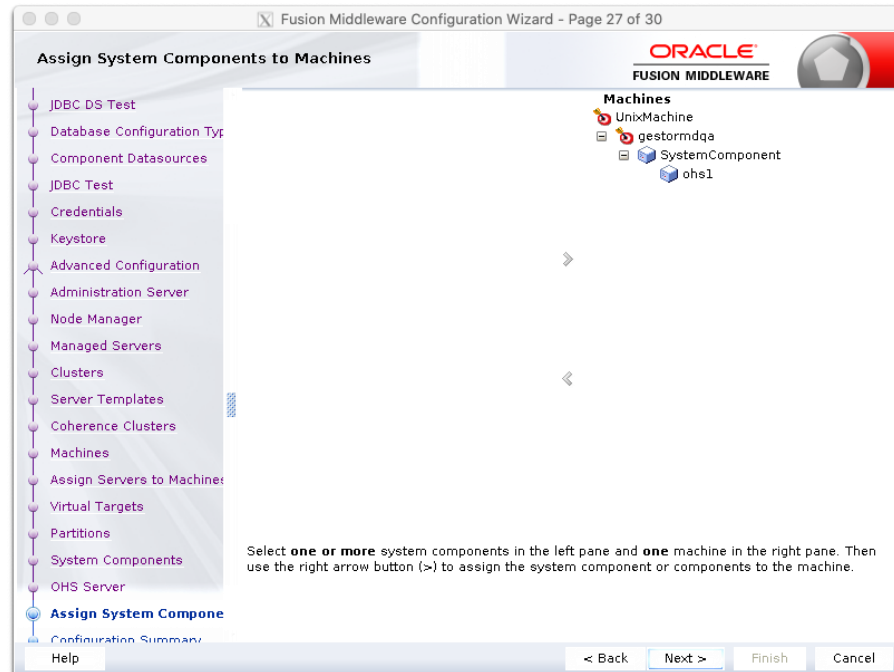
Fusion Middleware Configuration Wizard - Page 26 of 30

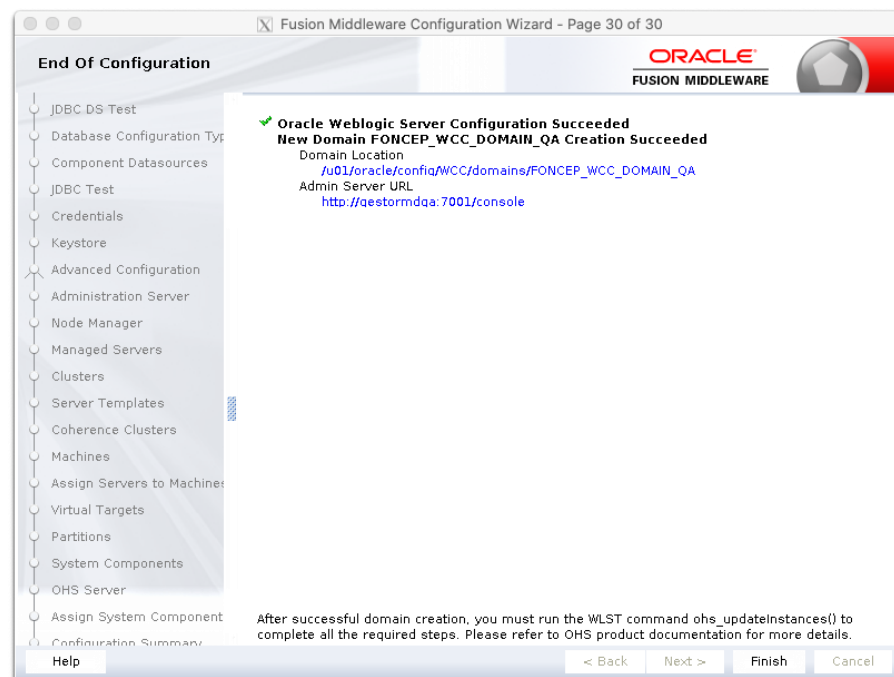
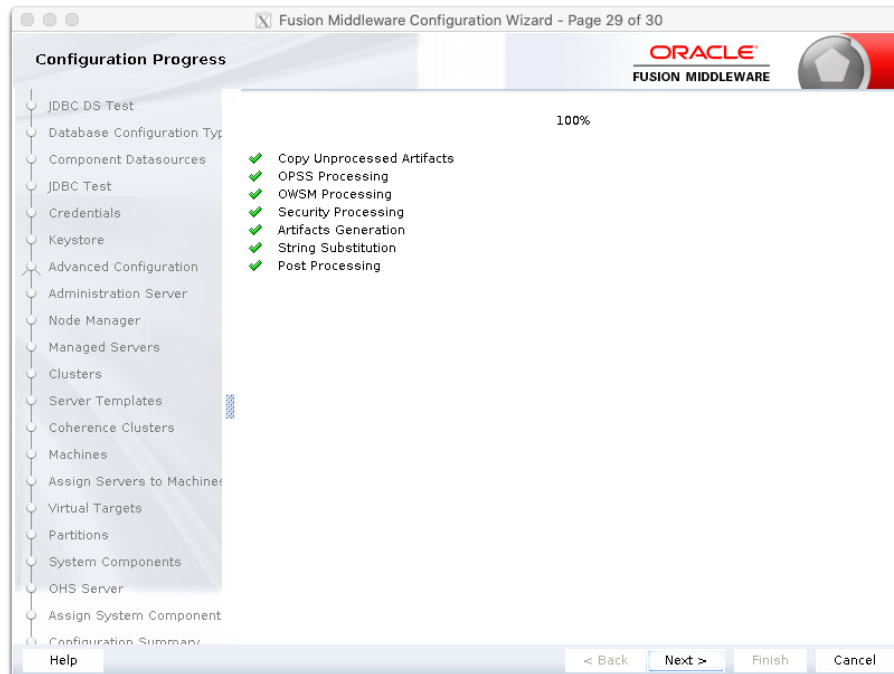
OHS Server

System Component ohs1

Admin Host	127.0.0.1
Admin Port	7779
Listen Address	
Listen Port	7777
SSL Listen Port	4443
Server Name	http://localhost:7777

Navigation: Help < Back Next > Finish Cancel





Consolas de Producto:

WebLogic Server - <http://gestormdqa:7001/console>

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: FONCEP_WCC_DOMAIN_QA

Home > Summary of Machines > gestormdqa > Summary of Servers

Summary of Servers

Configuration Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration. This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

Servers (Filtered - More Columns Exist)

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

New Clone Delete Showing 1 to 7 of 7 Previous Next

Name	Type	Cluster	Machine	State	Health	Listen Port
AdminServer(admin)	Configured		gestormdqa	RUNNING	OK	7001
CUST_server1	Configured		gestormdqa	RUNNING	OK	9105
IBR_server1	Configured		gestormdqa	RUNNING	OK	16250
IPM_server1	Configured		gestormdqa	RUNNING	OK	16000
SOA_server1	Configured		gestormdqa	RUNNING	OK	9103
UCM_server1	Configured		gestormdqa	RUNNING	OK	16200
WCCADF_server1	Configured		gestormdqa	RUNNING	OK	16225

New Clone Delete Showing 1 to 7 of 7 Previous Next

How do I...
 • Create Managed Servers
 • Clone servers
 • Delete Managed Servers
 • Delete the Administration Server
 • Start and stop servers
 • View objects in the JNDI tree

System Status

Enterprise Manager Fusion Middleware Control- <http://gestormdqa:7001/em>

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain weblogic

FONCEP_WCC_DOMAIN_QA

WebLogic Domain

Information
Certain functionality on this page is available only when you own the edit session lock. To obtain the lock, click "Lock and Edit" in the Change Center menu.

Servers
7 Up

Clusters
0 Clusters

Deployments
6 Down 25 Up

Administration Server

Name AdminServer
Host gestormdqa.segqa.segdmz.oraclevcn.com
Listen Port 7001

Servers

View Create Delete Control

Name	Status	Cluster	Machine	State	Health	Listen Port	C Usage
AdminServer(admin)	Running		gestormdqa	Running	OK	7001	0
CUST_server1	Running		gestormdqa	Running	OK	9105	Unavail
IBR_server1	Running		gestormdqa	Running	OK	16250	0
IPM_server1	Running		gestormdqa	Running	OK	16000	0
SOA_server1	Running		gestormdqa	Running	OK	9103	0

Columns Hidden 34 Servers 7 of 7

WebCenter Content - <http://gestormdqa:16200/cs>

WebCenter Content Configuration

Node Information

Cluster Node Identifier: UCM_server1

*** Content Server Instance Folder:** /u01/oracle/config/WCC/domains/FONCEP_WCC_

*** Native File Repository Location:** /u01/oracle/config/WCC/domains/FONCEP_WCC_

*** Weblayout Folder:** /u01/oracle/config/WCC/domains/FONCEP_WCC_

*** User Profile Folder:** /u01/oracle/config/WCC/domains/FONCEP_WCC_

Content Server URL Prefix: /cs/

Instance Information

Is New Content Server Instance: ☒

Server Socket Port: 4444

Incoming Socket Connection Address Security Filter: 127.0.0.1|10.160.4.149|0:0:0:0:0:0:1

*** Web Server HTTP/HTTPS Address:** gestormdqa.segqa.segdmz.oraclevcn.com:1620

Web Address Is HTTPS: ☐

Company Mail Server: mail

Administrator E-Mail Address: sysadmin@example.com

*** Server Instance Name:** gestormdqa_4444

*** Server Instance Label:** gestormdqa_4444

*** Server Instance Description:** Instance gestormdqa_4444

Is Auto Number Enabled: ☒

Auto Number Prefix: gestormdqa_444

SOA Suite - <http://gestormdqa:9103/soa-infra>

Welcome to the Oracle SOA/BPM Platform on WebLogic

SOA Version: v12.2.1.4.0 - MAIN_190828.0353.3300
WebLogic Server 12.2.1.4.0 (12.2.1.4.0)
Running on: SOA_server1

The following composites are currently deployed:

1. default/SimpleApproval!1.0*soa_6c7ecaaf-81ee-497b-81c9-29d8d0f320b9
 - [Test client](#)

Links

[SOA Composer](#)
[BPM Worklist](#)
[Business Process Composer](#)
[Business Process Workspace](#)
[B2B Console](#)

Oracle BPM - <http://gestormdqa:9103/integration/worklistapp>

Views + ✎ ✕

Actions ▾

Status ▾ **Title** 🔍

Me & My Group All ▾ **Assigned** ▾

Number **Creator** **Assigned** **Priority**

Inbox

My Tasks (0)

Initiated Tasks

Administrative Tasks

Views

Due Soon

High Priority

Past Day

Past Week

Past Month

Past Quarter

New Tasks

No data to display

Please select a task to see the details

User Communication Preference - <http://gestormdqa:9103/sdpmessaging/userprefs-ui>

ORACLE User Communication Preferences

< Home Help Settings Logout > weblogic

Available Channels

View ▾

Name	Type	Address	Default
No data to display			

Messaging Filters

View ▾

Name	Description	Enabled
No data to display		

SOA Composer - <http://gestormdqa:9103/soa/composer/>

ORACLE SOA Composer

Links ▾ weblogic

+ Create Session

Deployment View ▾

- SOA Infra
 - Composites
 - Metadata
 - CaseManagementBaseDictionary
 - DynamicRouting.rules

WebServices Manager - <http://gestormdqa:9103/wsm-pm/>

[Validate Policy Manager](#)

Copyright © 2007, 2019, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Inbound Refinery - <http://gestormdqa:16250/ibr>

Inbound Refinery Configuration

Instance Information

Inbound Refinery Instance Identifier:	IBR_server1
* Inbound Refinery Instance Folder:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
* Native File Repository Location:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
* Weblayout Folder:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
* User Profile Folder:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
Register Start Menu Actions:	☒
* Server Socket Port:	5555
Incoming Socket Connection Address Security Filter:	127.0.0.1 0:0:0:0:0:0:1
* Web Server HTTP/HTTPS Address:	gestormdqa.segqa.segdmz.oraclevcn.com:1625
Web Address Is HTTPS:	☐
Inbound Refinery URL Prefix:	/ibr/
* Server Instance Name:	gestormdqa379250cncom16250
* Server Instance Label:	gestormdqa379250cncom16250
* Server Instance Description:	Instance gestormdqa379250cncom16250

*** - Required**

Oracle Colombia,
Calle 100 No. 13 - 21 Piso 15
Bogotá, Colombia

Phone: +57 1 611 96 00
Fax: +57 1 611 96 00



Hardware and Software, Engineered to Work Together

CONNECT WITH US



Copyright © 2014, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0715

Sistema de Gestión Documental – SGD PRODUCCION

LBR

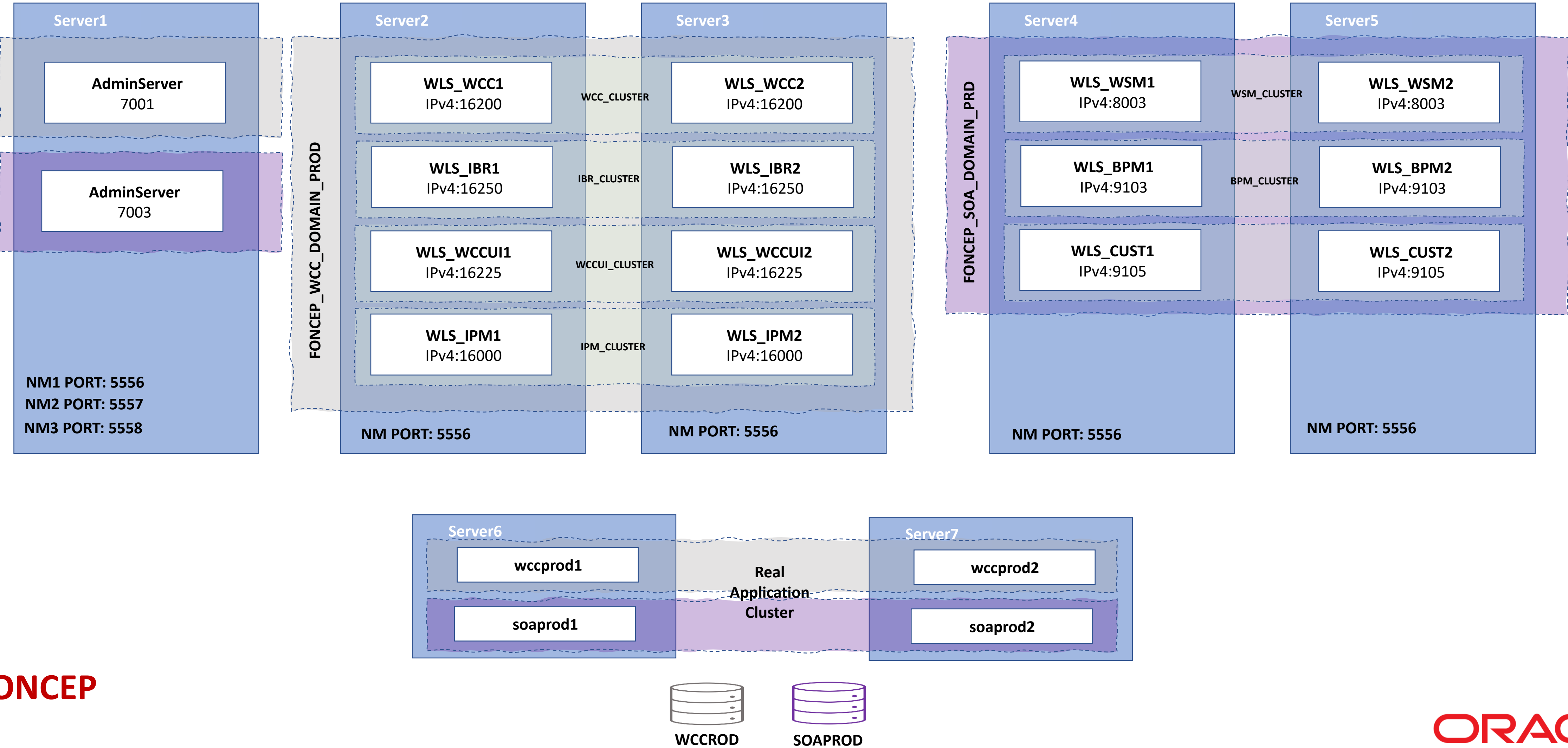
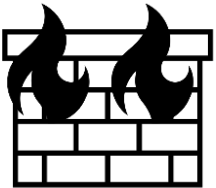
adminwcc.foncep.local

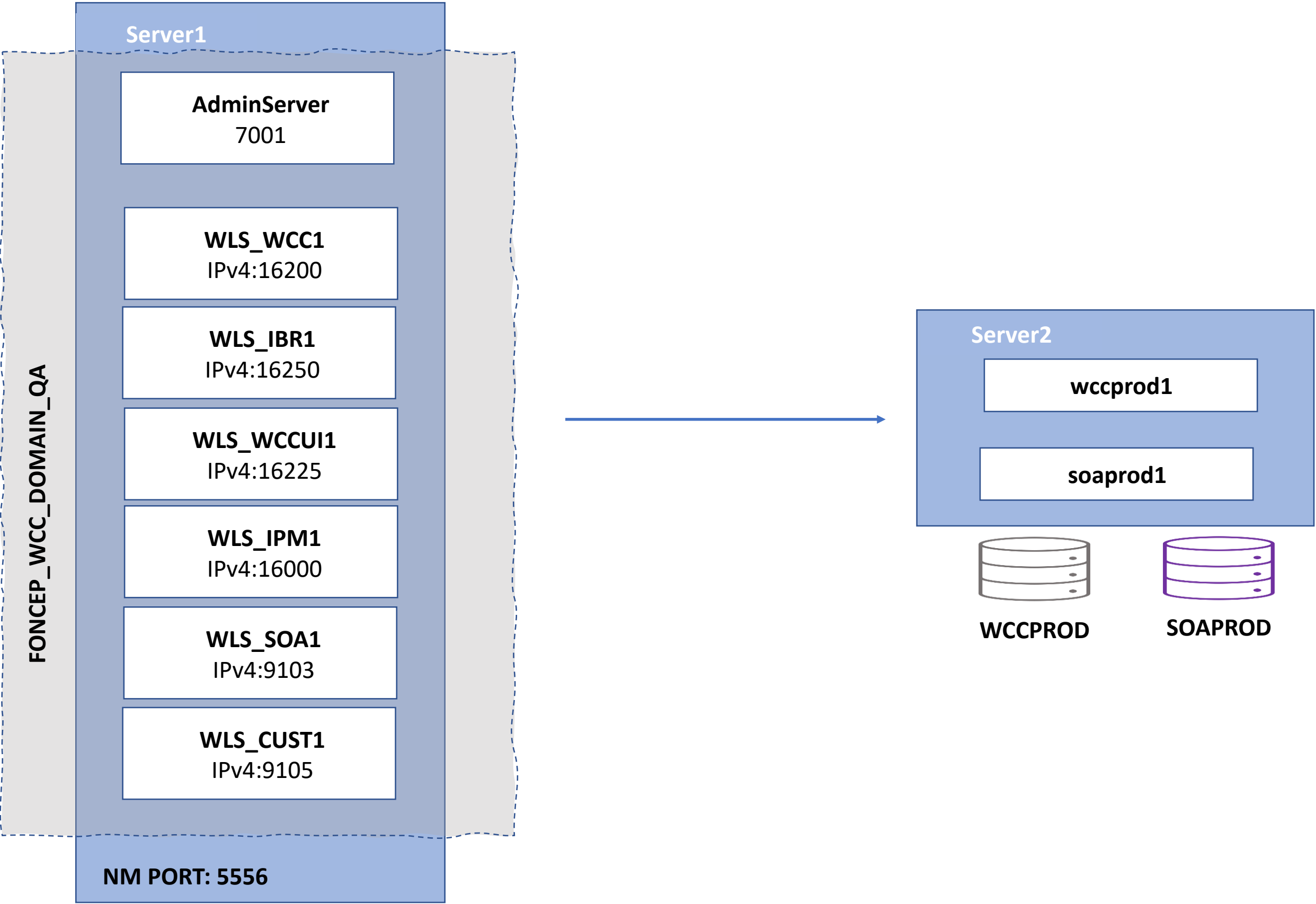
wcc.foncep.local

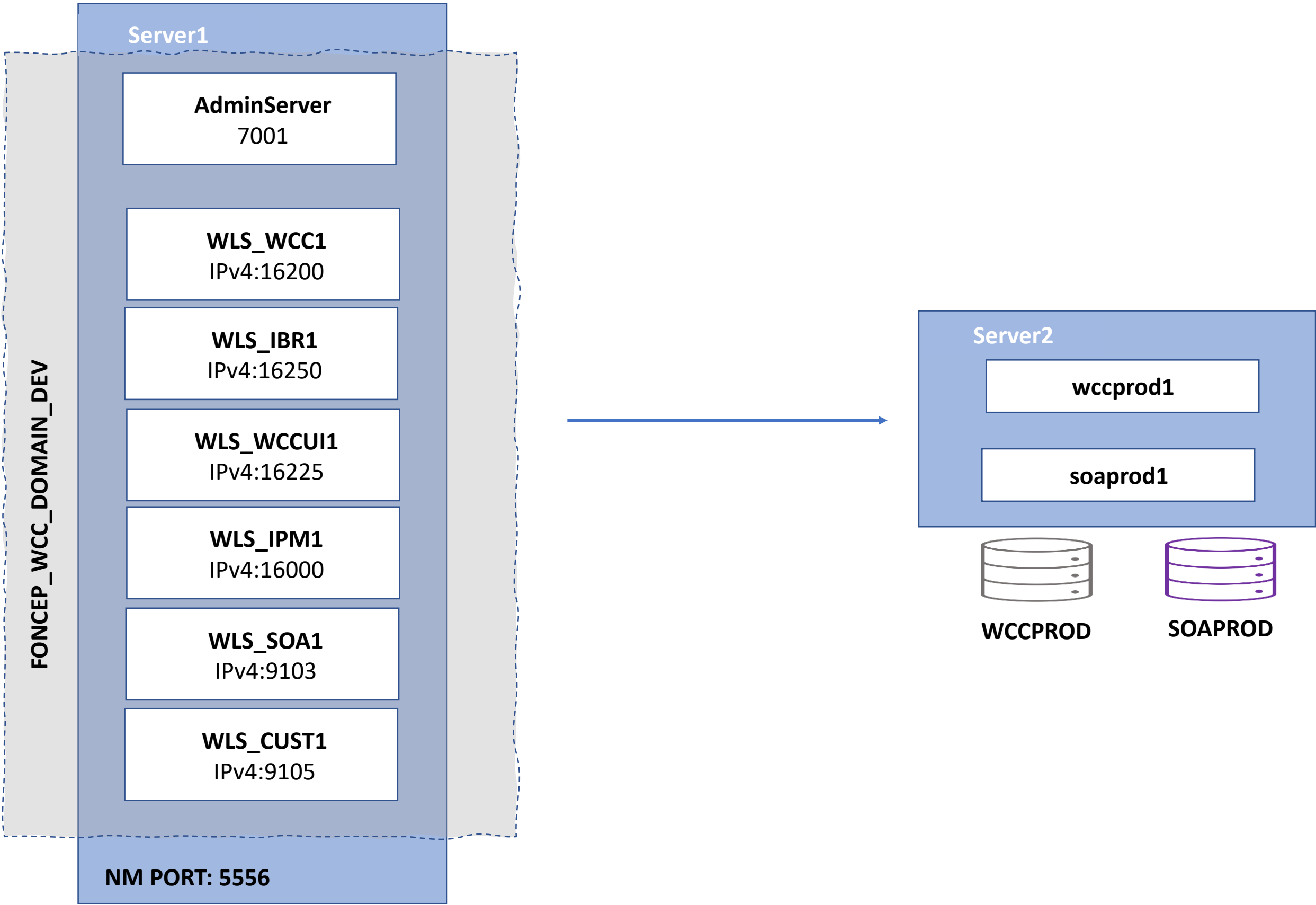
adminsoa.foncep.local

soa.foncep.local

DMZ







DOCUMENTACIÓN DE PRODUCTOS DEL FABRICANTE ORACLE

- ▶ Guía de Instalación y Configuración de Oracle Webcenter Content

Oracle® Fusion Middleware - Installing and Configuring Oracle WebCenter Content

<https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/inecm/installing-and-configuring-oracle-webcenter-content.pdf>

- ▶ Guía para el Despliegue Empresarial de Oracle Webcenter Content

Oracle® Fusion Middleware - Enterprise Deployment Guide for Oracle WebCenter Content

<https://docs.oracle.com/middleware/1221/core/CMEDG/CMEDG.pdf>

<https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.3/cmedg/enterprise-deployment-guide-oracle-webcenter-content.pdf>

- ▶ Guía de Iniciación y documentación de Oracle Webcenter Content

<https://docs.oracle.com/en/middleware/webcenter/content/12.2.1.4/index.html>

- ▶ Documentación de otros componentes de la infraestructura de software Oracle

Oracle Business Process Management

<https://docs.oracle.com/en/middleware/fusion-middleware/bpm/12.2.1.4/index.html>

Oracle SOA Suite

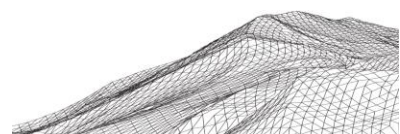
<https://docs.oracle.com/en/middleware/soa-suite/index.html>

Oracle Weblogic Server

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/index.html>

Oracle Database

<https://docs.oracle.com/en/database/oracle/oracle-database/index.html>



Información del Proyecto

Proyecto: **Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA**

Acta de Pruebas de Funcionalidad

Objetivo: Realización de un conjunto de pruebas técnicas para la verificación de la configuración y parametrización de los componentes de software Oracle que integran el Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA

1.1.

1.2. Especificación

Nombre de Prueba	Verificación instalación del SW		Número de Prueba	001	
Descripción Prueba	Acceso a la infraestructura tecnológica de la entidad para verificar los directorios donde fueron desplegados los componentes Oracle		Escenario Prueba	Verificación de la existencia de los directorios con los componentes de software Oracle	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso a las BD		Número de Prueba	002	
Descripción Prueba	Prueba de ingreso a las BD		Escenario Prueba	Ingreso correcto a las BD	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso WebLogic Server		Número de Prueba	003	
Descripción Prueba	Prueba de autenticación a la consola de WebLogic Server con un usuario con privilegios de administrador		Escenario Prueba	Autenticación exitosa en http://gestormdqa:7001/console	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso Enterprise Manager Fusion Middleware Control		Número de Prueba	004	
Descripción Prueba	Prueba de autenticación a la consola de Enterprise Manager Fusion Middleware Control		Escenario Prueba	Autenticación exitosa en http://gestormdqa:7001/em	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso WebCenter Content		Número de Prueba	005	
Descripción Prueba	Prueba de autenticación a la consola de WebCenter Content		Escenario Prueba	Autenticación exitosa en http://gestormdqa:16200/cs y validar la configuración	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso SOA Suite		Número de Prueba	006	
Descripción Prueba	Prueba de autenticación a la consola de SOA Suite		Escenario Prueba	Autenticación exitosa en http://gestormdqa:9103/soa-infra	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso Oracle BPM		Número de Prueba	007	
Descripción Prueba	Prueba de autenticación a la consola de Oracle BPM		Escenario Prueba	Autenticación exitosa en http://gestormdqa:9103/integration/worklistapp	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a User Communication Preference		Número de Prueba	008	
Descripción Prueba	Ingreso correcto a User Communication Preference		Escenario Prueba	Es posible ingresar a http://gestormdqa:9103/sdpMessaging/userprefs-ui y administrar “Available Channels” y “Messaging Filters”	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	20 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a SOA Composer		Número de Prueba	009	
Descripción Prueba	Ingreso correcto a SOA Composer		Escenario Prueba	Es posible ingresar a http://gestormdqa:9103/soa/composer/ y administrar	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a WebServices Manager		Número de Prueba	010	
Descripción Prueba	Ingreso correcto a WebServices Manager		Escenario Prueba	Es posible ingresar a http://gestormdqa:9103/wsm-pm/ y ver Validate Policy Manager	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a Inbound Refinery		Número de Prueba	011	
Descripción Prueba	Ingreso correcto a Inbound Refinery		Escenario Prueba	Es posible ingresar a http://gestormdqa:16250/ibr y validar la configuración	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	20 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

1.3. Asistentes

Nombres y Apellidos	Cargo	Empresa	Correo Electrónico
Jorge García	Coordinador de Infraestructura	FONCEP	jmgarcia@foncep.gov.co
Oscar Hernán Rojas	Ingeniero Soporte Avanzado	ORACLE	oscar.hernan.rojas.rodriguez@oracle.com
Marcela Avendaño	Líder Técnico	OCP TECH	marcela.avendano@ocp.tech

1.4. Desarrollo de las Pruebas

2. Número de Prueba	001
Objetivo	Verificación instalación del software
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	002
Objetivo	Ingreso correcto a las BD
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	003
Objetivo	Autenticación exitosa en http://gestormdqa:7001/console
Resultados de la Prueba	Exitoso

Genero Error	No
Solución	N/A

Número de Prueba	004
Objetivo	Autenticación exitosa en http://gestormdqa:7001/em
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	005
Objetivo	Autenticación exitosa en http://gestormdqa:16200/cs y validar la configuración
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	006
Objetivo	Autenticación exitosa en http://gestormdqa:9103/soa-infra
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	007
Objetivo	Autenticación exitosa en http://gestormdqa:9103/integration/worklistapp

Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	008
Objetivo	Es posible ingresar a http://gestormdqa:9103/sdpMessaging/userprefs-ui y administrar "Available Channels" y "Messaging Filters"
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	009
Objetivo	Es posible ingresar a http://gestormdqa:9103/soa/composer/ y administrar
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	010
Objetivo	Es posible ingresar a http://gestormdqa:9103/wsm-pm/ y ver Validate Policy Manager
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	011

Objetivo	Es posible ingresar a http://gestormdqa:16250/ibr y validar la configuración
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

1.4 Aceptación de las Pruebas

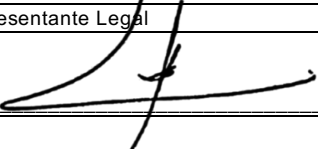
Funcionario Técnico FONCEP: Jorge García

Cargo: Coordinador de Infraestructura

Fecha de Aceptación: 17 de Diciembre 2021

Firma Aceptación:



		ACTA DE ENTREGA PROYECTO SGDEA		CÓDIGO:	F-PR-002
				VERSION:	3
				FECHA REVISIÓN:	
				24-feb-15	
Fecha de diligenciamiento: diciembre 17 de 2021					
Datos del cliente					
Empresa cliente:	Fondo de Prestaciones Económicas Cesantías y Pensiones Foncep	Contacto:	Wilson Barrios Delgado		
Teléfonos:	(571) 307 6200	E-mail:	wbarriosd@foncep.gov.co		
Nombre del proyecto:	Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA				
Descripción del proyecto:					
Adquisición, implementación y puesta en marcha de un nuevo Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA que contribuya de manera significativa a fortalecer los procesos de producción, recepción, distribución, consulta, organización, recuperación, disposición final y archivado de los documentos en FONCEP.					
Fecha Inicio	3/12/21	Fecha Entrega	17/12/21		
Trabajo realizado y entregado					
Instalación del sistema de gestión documental SGDEA: - Despliegue de la última versión de los componentes del sistema de gestión documental SGDEA en la plataforma de nube Oracle de la entidad, realizado por personal de Oracle, incluyendo la configuración y parametrización de la herramienta - Pruebas de funcionalidad del sistema instalado y su aceptación por parte de la entidad. Entrega de documento de pruebas y aceptación.					
Certificado de Titularidad de licencias: - El día 03 de diciembre de 2021 se le entregó a la entidad el Certificado de Titularidad de licencias de Oracle.					
Certificación del número de horas de servicio contratadas: - El día 03 de diciembre de 2021 se le entregó a la entidad la nota aclaratoria sobre la cantidad de horas de servicio de Oracle ACS contratadas para la configuración y parametrización del SGDEA de acuerdo con la estimación correspondiente al alcance del anexo técnico.					
Manuales técnicos: - Maqueta de arquitectura tecnológica de los componentes de software del sistema SGDEA implementados por Oracle - Documento de instalación de los componentes de software del sistema SGDEA conforme realizado por Oracle - Documentación complementaria del fabricante sobre el producto Oracle Webcenter Content incluyendo guías de instalación y configuración de producto, guía de despliegue empresarial y arquitecturas de referencia, guía de iniciación al producto Oracle Webcenter Content y documentación de fabricante sobre componentes de la infraestructura de software Oracle					
El cliente certifica que la totalidad de los suministros y servicios reseñados en la presente acta han sido entregados / terminados y que, habiendo sido a sometidos a las pruebas de validación y aceptación indicadas, están de acuerdo con las especificaciones formales y demás requisitos contractualmente convenidos y establecidos entre las partes.					
Observaciones					
Quien entrega por parte de OCP TECH			Recibido a satisfacción Cliente		
Nombre:	Enrique Marcelo Herrera		Nombre:	Wilson Barrios Delgado	
Cargo	Representante Legal		Cargo	Jefe de Oficina de Informática y Sistemas	
Firma:			Firma:		
Fecha: 17 de Diciembre de 2021			Fecha: 17 de Diciembre de 2021		

INSTALACION WEBCENTER CONTENT

FONCEP

Autores:	Oscar Hernán Rojas
Fecha Creación:	Diciembre, 2021
Última Actualización:	
Referencia:	Revisión de plataforma
Versión:	1.1

1 Control del Documento

1.1 Registro de Cambios

Fecha	Autor	Versión	Referencia de cambio
16-12-2021	Hernán Rojas	DRAFT	Creación del documento

1.2 Revisores

Nombre	Cargo	Correo
Jaime Rozo	Senior Principal Technical Account Manager	Jaime.enrique.rozo@oracle.com

1.3 Lista de Distribución

Nombre	Cargo	Correo

1.4 Actas de Reunión Asociadas

N.A.

Contenido

1	Control del Documento.....	2
1.1	Registro de Cambios	2
1.2	Revisores.....	2
1.3	Lista de Distribución	2
1.4	Actas de Reunión Asociadas	2
	Introducción	4
2	INSTALACION BASE DE DATOS	5
	Instalación software Grid Infrastructure.....	5
	Instalación software base de datos y creación base de datos wccinfra	6
3	INSTALACION WEBCENTER CONTENT	8
	Instalación Java:	8
	Instalación Oracle Fusion Middleware Infrastructure:	8
	Instalación Oracle WebCenter Content:	13
	Instalación Oracle SOA Suite:	17
	Instalación Oracle OHS:	21
	Ejecución RCU:	26
	Creación de Dominio WLS:	31
	Consolas de Producto:	44

Introducción

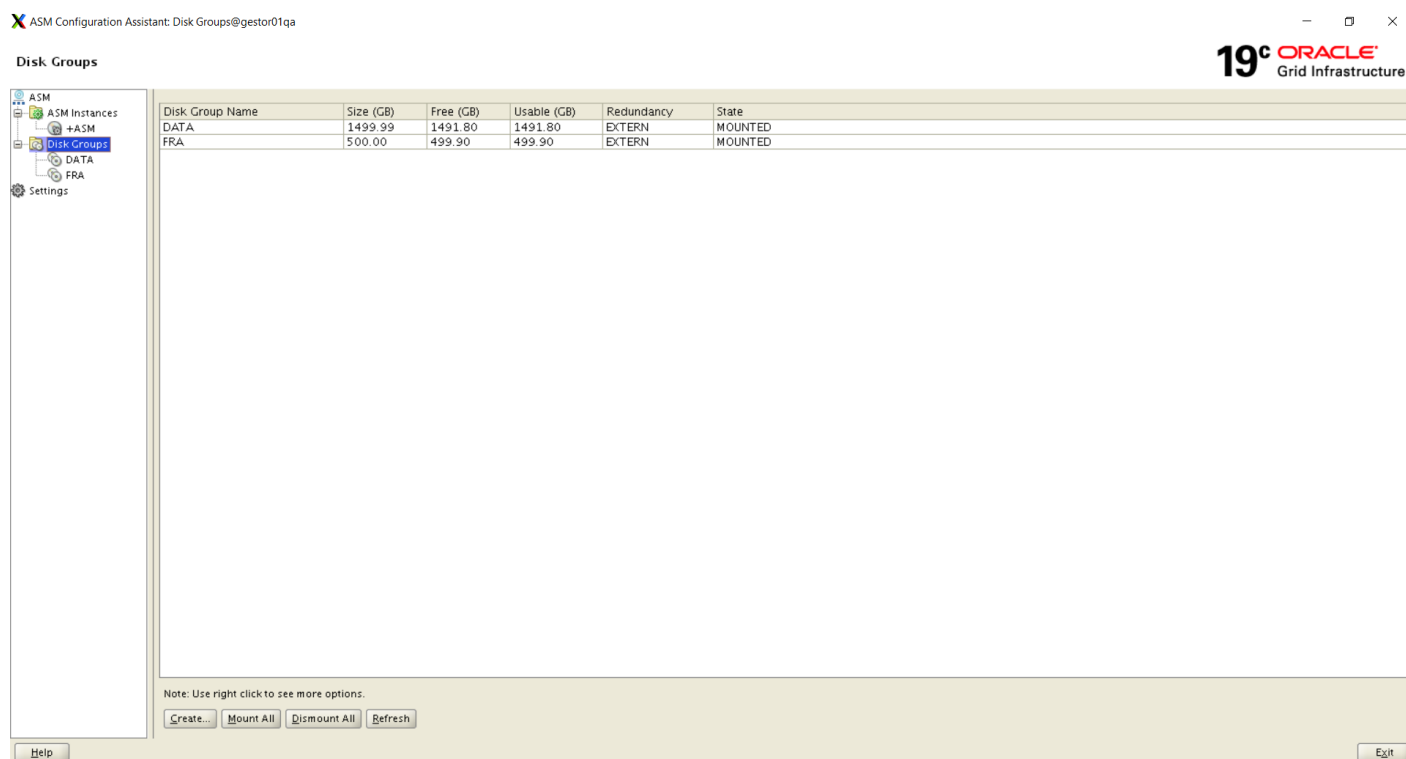
En este documento se entrega como apoyo a la instalación y configuración del Oracle WebCenter Content de FONCEP.

2 INSTALACION BASE DE DATOS

Se realiza instalación de software en versión 19.13 de Grid Infraestructure y de base de datos.

Instalación software Grid Infraestructure

Se realiza la instalación de Grind Infraestructure en versión 19.3 y se actualiza a la versión 19.13, a continuación, se realiza la creación los diskgroups de DATA y de FRA, se anexan los pantallazos correspondientes.



```
[grid@gestor01qa ~]$ id
uid=54322(grid) gid=54321(oinstall) groups=54321(oinstall),54322(dba),54324(backupdba),54325(dgdba),54326(kmdba),54327(asmdba),54328(asmoper),54329(asmadmin),54330(racdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[grid@gestor01qa ~]$ sqlplus / as sysasm

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Dec 17 15:17:38 2021
Version 19.13.0.0.0

Copyright (c) 1982, 2021, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL> show parameters db_unique_name

NAME                                TYPE        VALUE
-----
db_unique_name                      string      +ASM

SQL> SELECT BANNER_FULL
FROM V$VERSION;

BANNER_FULL
-----
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL>
```

Instalación software base de datos y creación base de datos wccinfra

Se realiza la instalación del software de base de datos en versión 19.3 y se actualiza a la versión 19.13 y se realiza la creación de la base de datos para el ambiente de Web Center Content

```
[oracle@gestor01qa ~]$ id
uid=54321(oracle) gid=54321(oinstall) groups=54321(oinstall),54322(dba),54323(oper),54324(backupdba),54325(dgdba),54326(kmdba),54327(asmdba),54329(asmadmin),54
330(racdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[oracle@gestor01qa ~]$ export ORACLE_SID=wccinfra
[oracle@gestor01qa ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Dec 17 16:39:07 2021
Version 19.13.0.0.0

Copyright (c) 1982, 2021, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL> show parameters db_unique_name

NAME                                TYPE        VALUE
-----
db_unique_name                      string      wccinfra
SQL> select BANNER_FULL
2 from v$version;

BANNER_FULL
-----
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.13.0.0.0

SQL> █
```

Database Configuration Assistant - Configure an existing database - Step 7 of 9@gestor01qa

Summary

- [Database Operation](#)
- [Select Database](#)
- [Database Options](#)
- [Data Vault Option](#)
- [Connection Mode](#)
- [Oracle R Configuration](#)
- Summary**
- Progress Page
- Finish

Database Configuration Assistant

Database New Configuration

- Database Name: wccinfra
- Configure Oracle Database Vault: No
- Configure Oracle Label Security: No
- Configure Oracle Label Security with OID: No
- Configure Oracle R: Yes
- Tablespace for Oracle R configuration: SYSAUX
- Database components

Help

< Back

Next >

Finish

Cancel

3 INSTALACION WEBCENTER CONTENT

A continuación, se presentan las pantallas de instalación del producto Oracle WebCenter Content

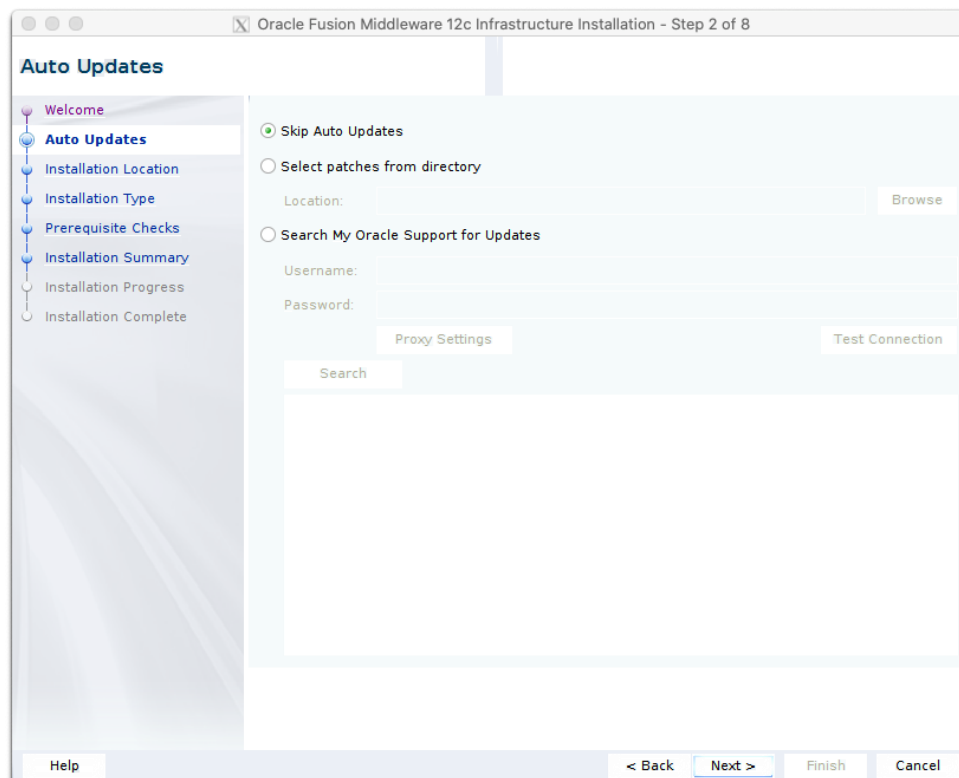
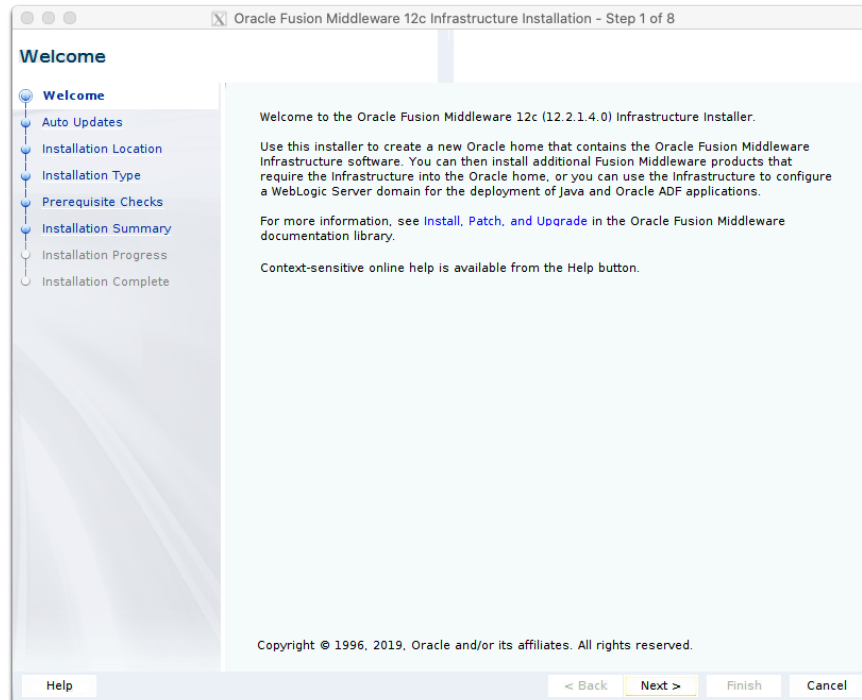
Instalación Java:

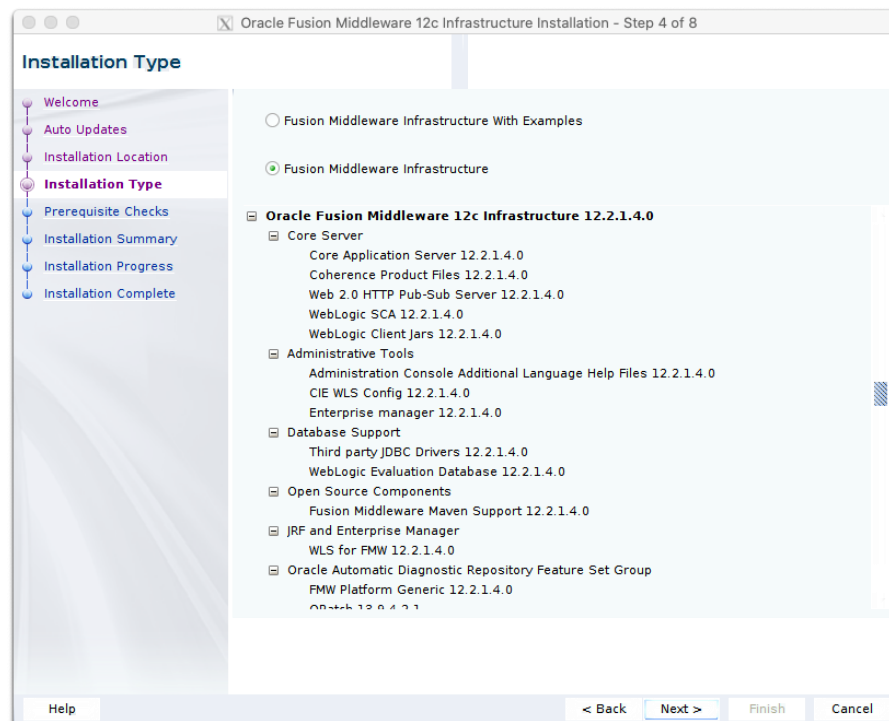
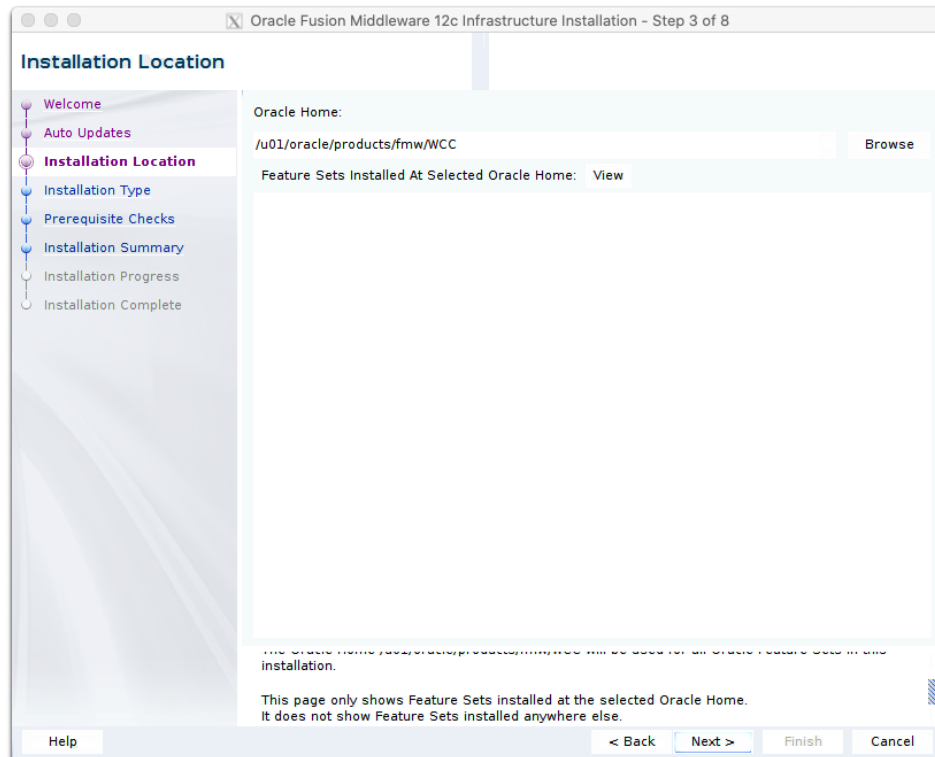
Se realizo la instalación del componente Oracle JDK version 1.8.0_311 sobre el servidor **gestormdqa**. En la ruta `/u01/oracle/products/jdk`

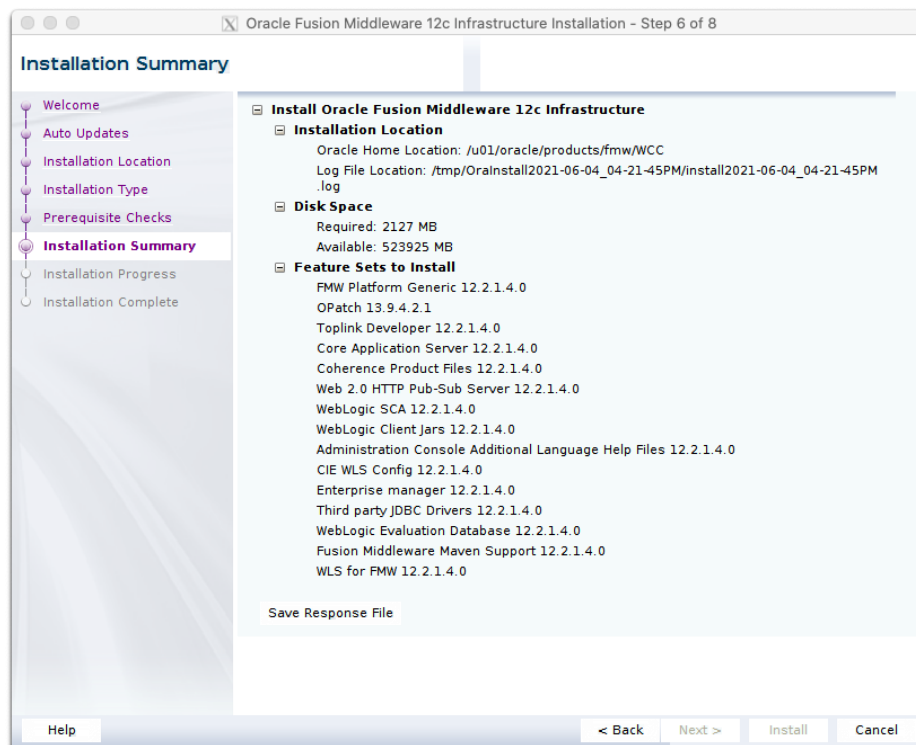
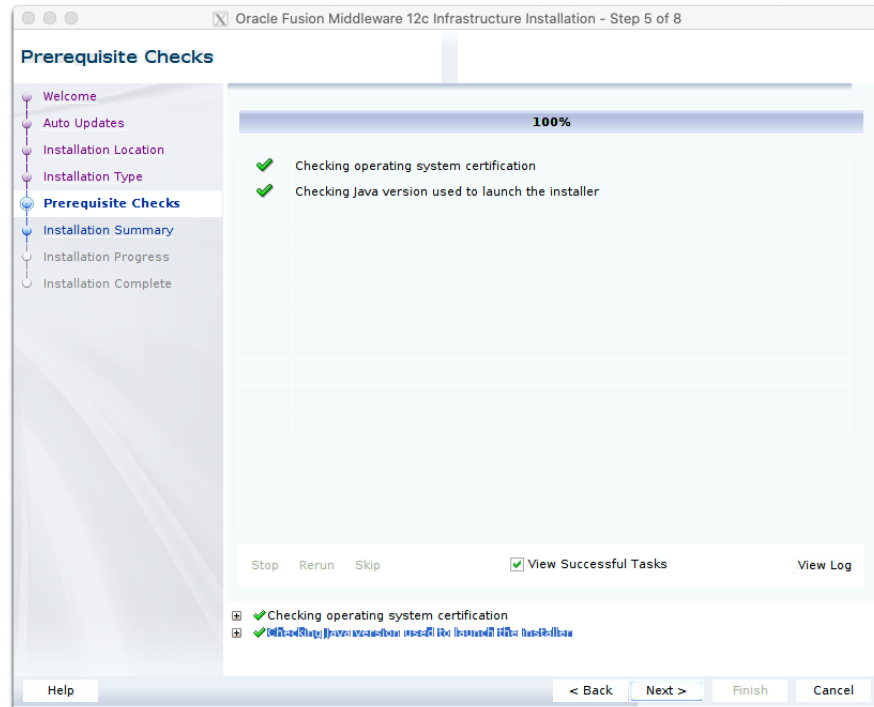
```
[oracle@gestormdqa products]$ java -version
java version "1.8.0_311"
Java(TM) SE Runtime Environment (build 1.8.0_311-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.311-b11, mixed mode)
```

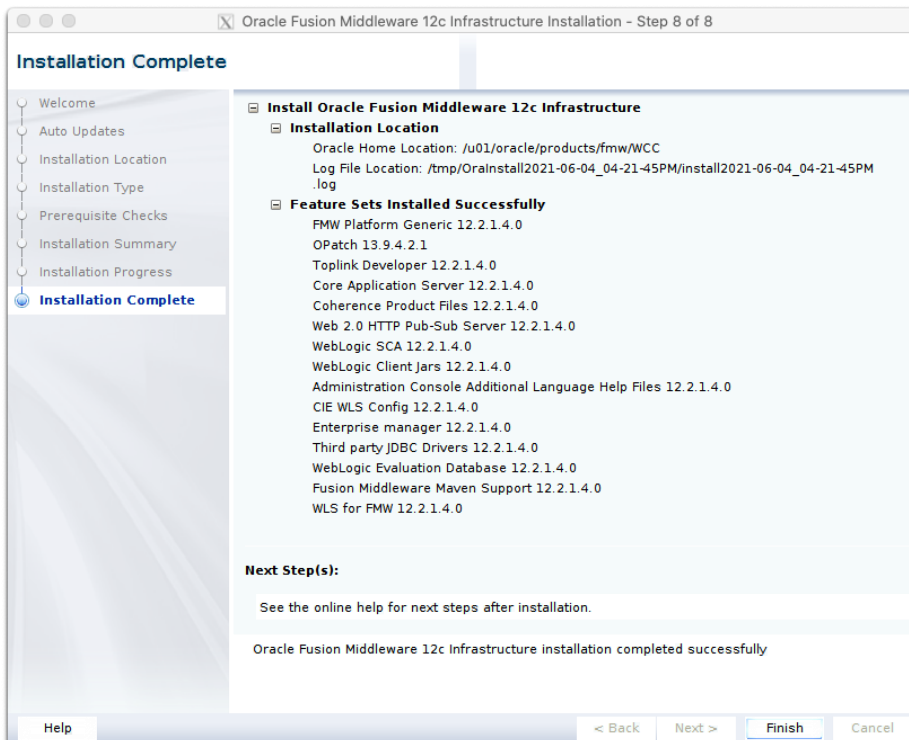
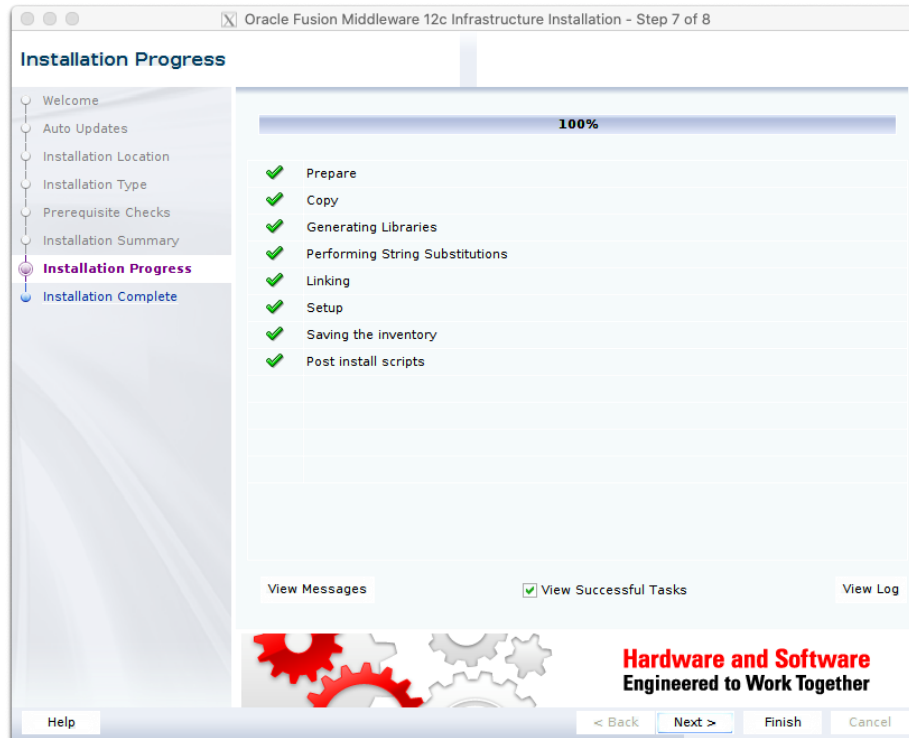
Instalación Oracle Fusion Middleware Infrastructure:



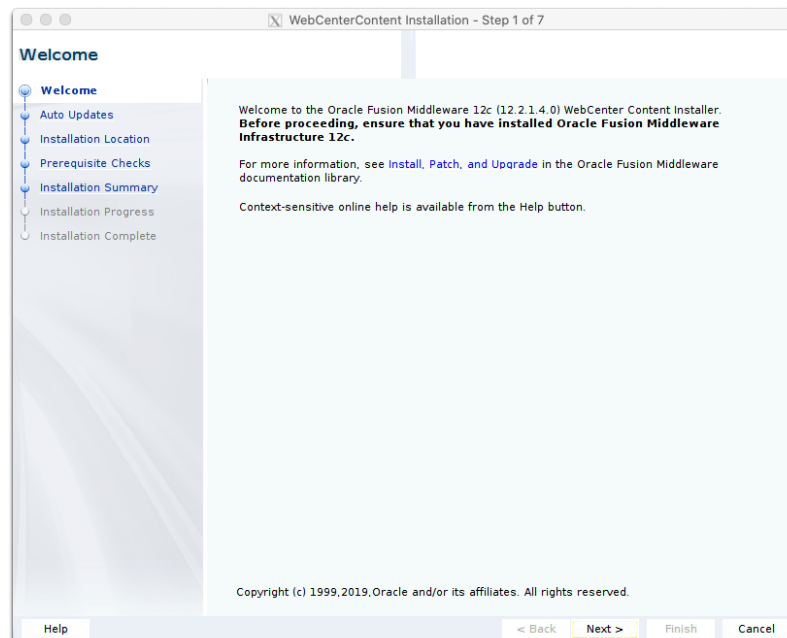
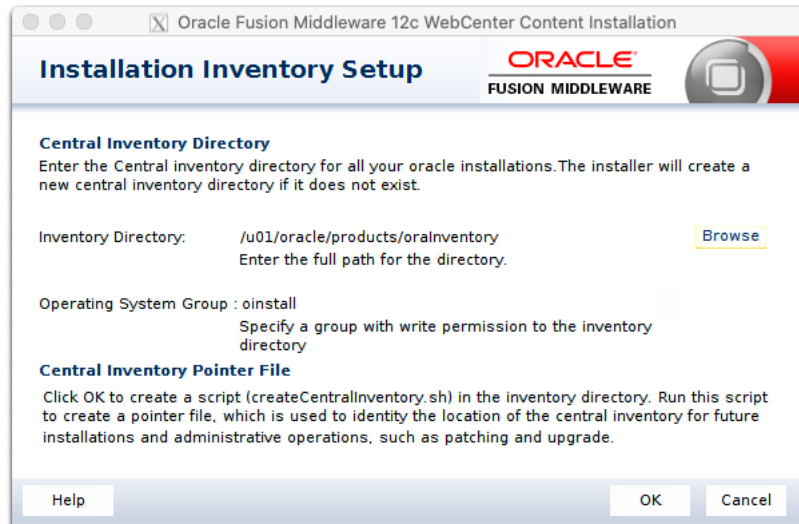








Instalación Oracle WebCenter Content:



WebCenterContent Installation - Step 2 of 7

Auto Updates

Welcome

- Auto Updates**
- Installation Location
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

☒ Skip Auto Updates

☐ Select patches from directory

Location:

☐ Search My Oracle Support for Updates

Username:

Password:

WebCenterContent Installation - Step 3 of 7

Installation Location

Welcome

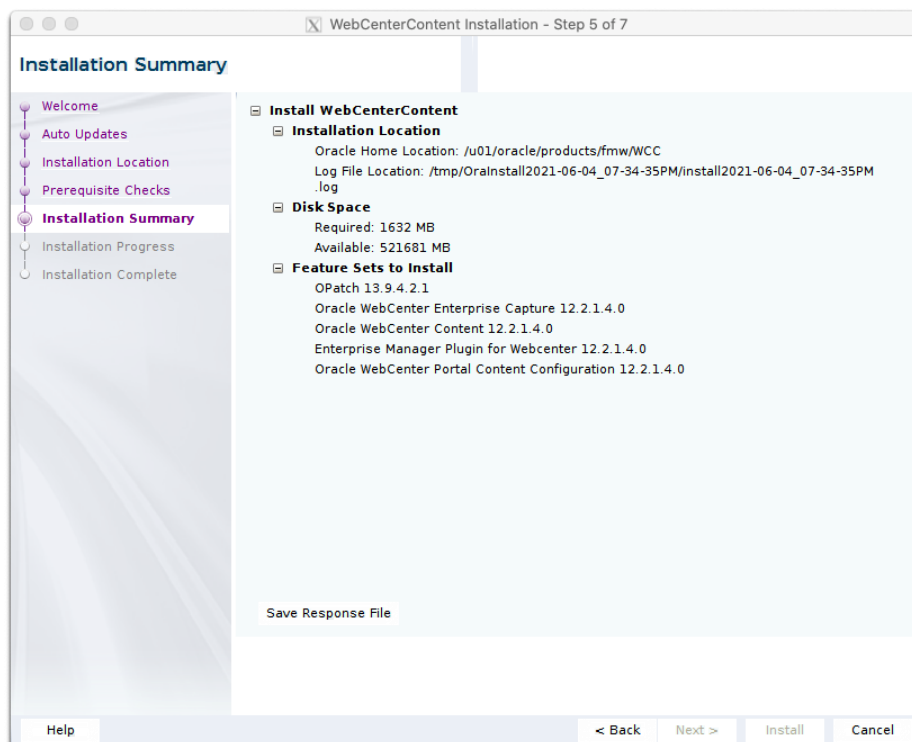
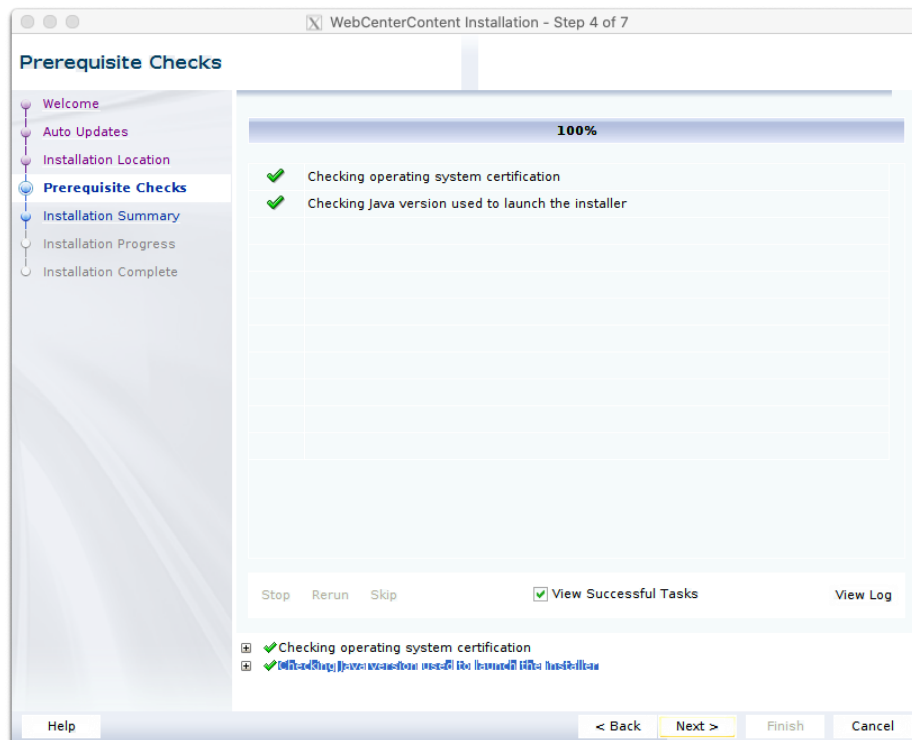
- Auto Updates**
- Installation Location**
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

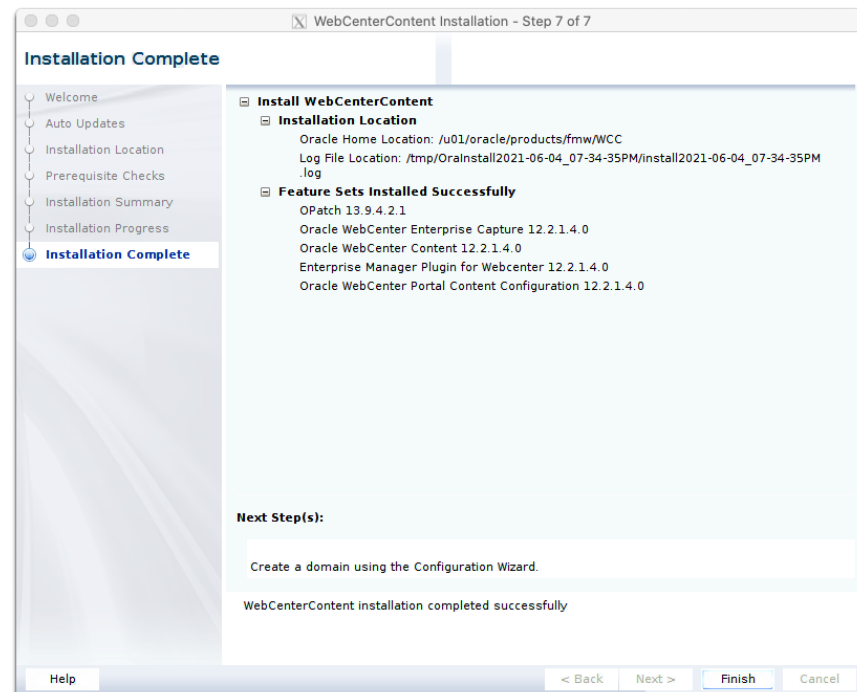
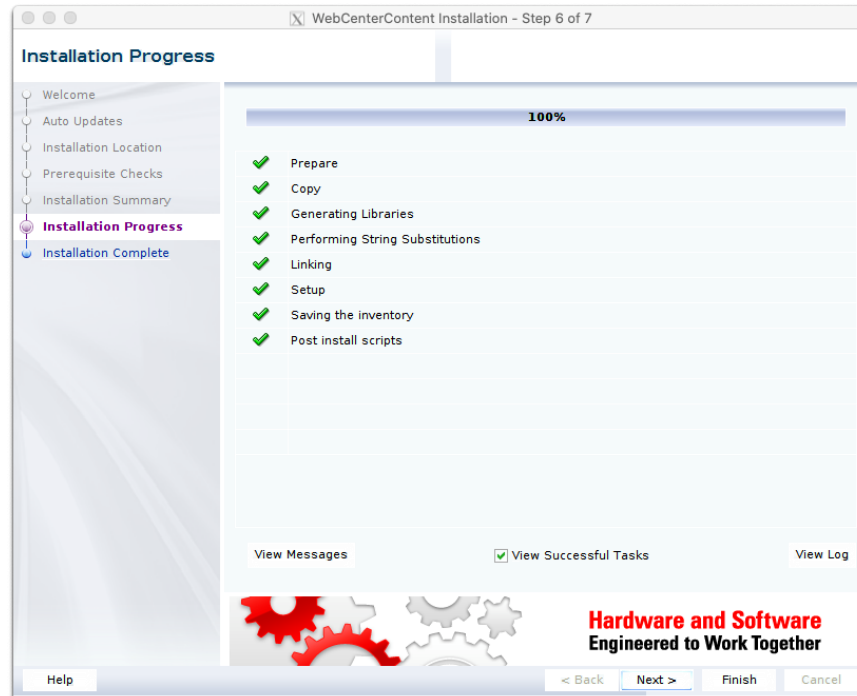
Oracle Home:

Feature Sets Installed At Selected Oracle Home:

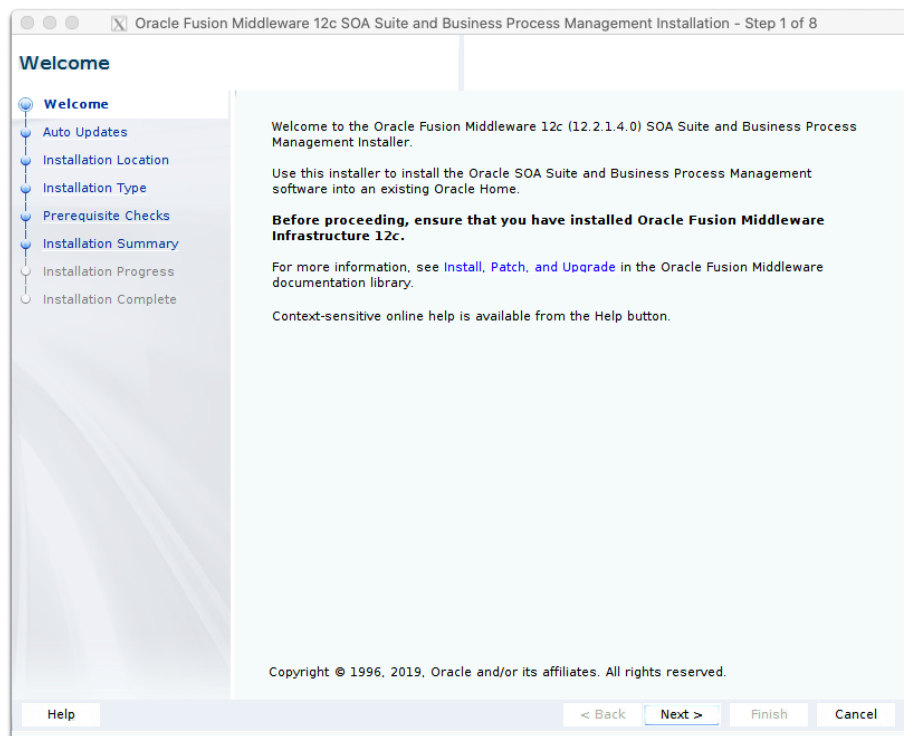
The Oracle Home /path/to/oracle/home/ will be used for all Oracle Feature Sets in this installation.

This page only shows Feature Sets installed at the selected Oracle Home. It does not show Feature Sets installed anywhere else.





Instalación Oracle SOA Suite:



Oracle Fusion Middleware 12c SOA Suite and Business Process Management Installation - Step 2 of 8

Auto Updates

- Welcome
- Auto Updates**
- Installation Location
- Installation Type
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

☒ Skip Auto Updates

☐ Select patches from directory

Location: [Browse](#)

☐ Search My Oracle Support for Updates

Username:

Password:

[Proxy Settings](#) [Test Connection](#)

Search

Oracle Fusion Middleware 12c SOA Suite and Business Process Management Installation - Step 3 of 8

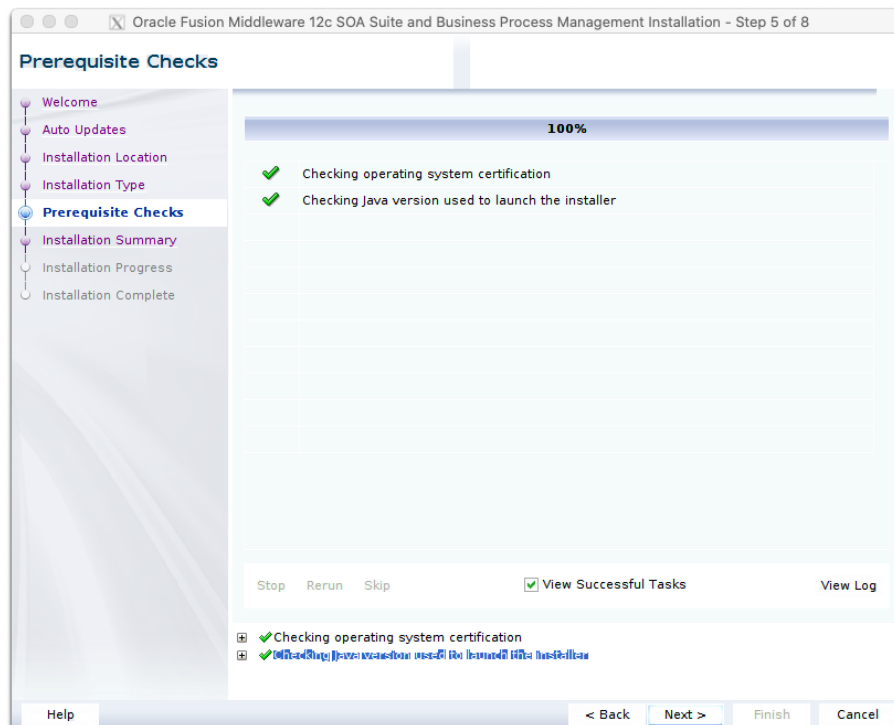
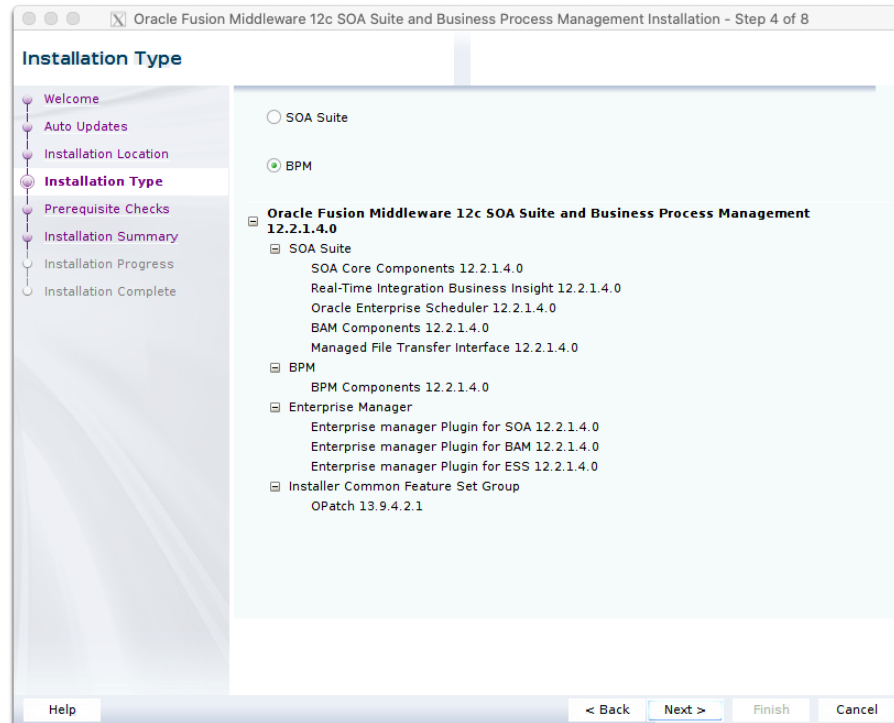
Installation Location

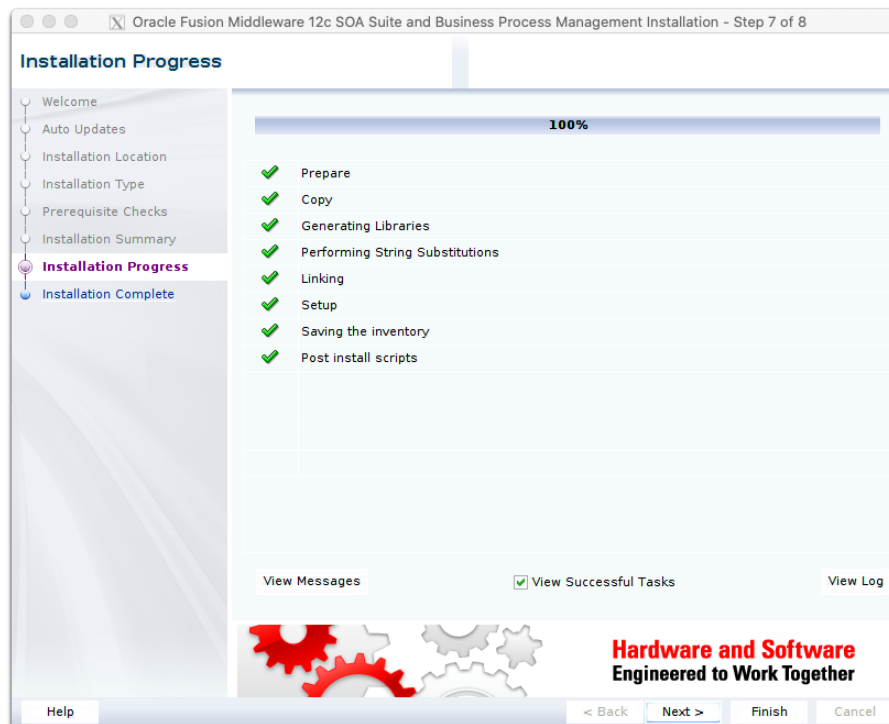
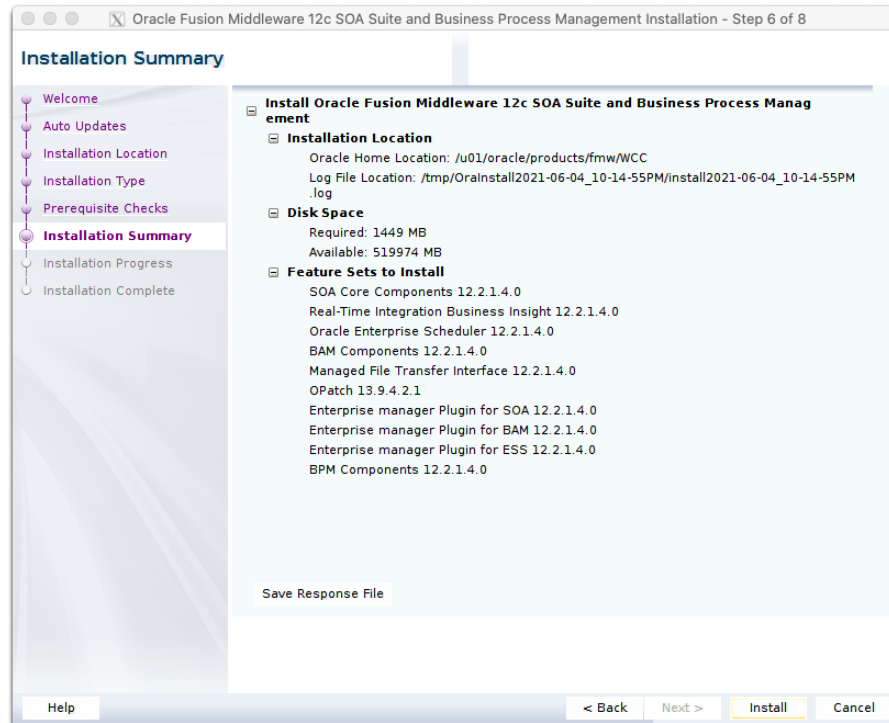
- Welcome
- Auto Updates
- Installation Location**
- Installation Type
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

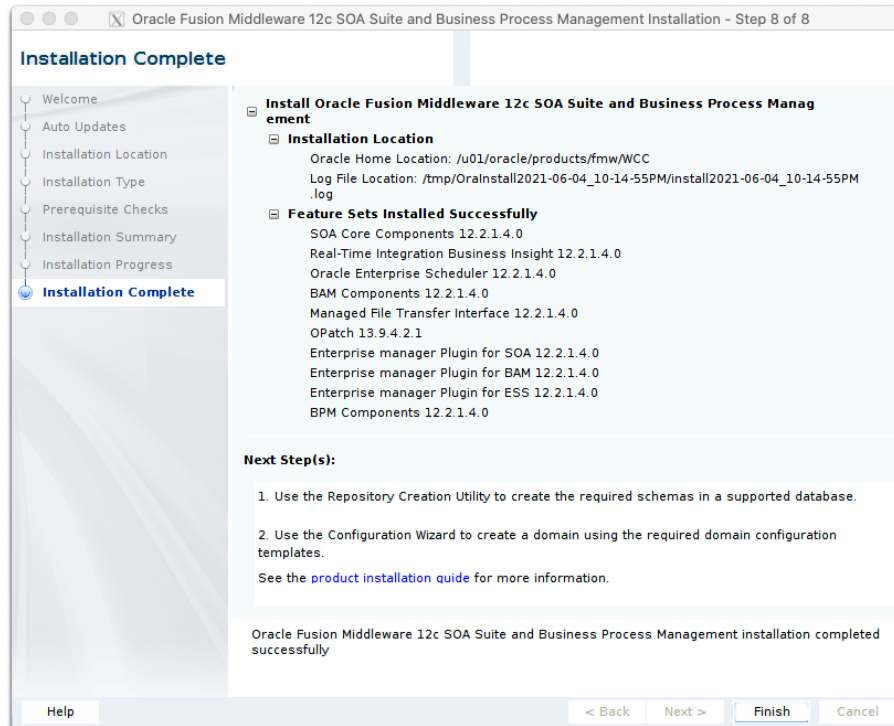
Oracle Home: [Browse](#)

Feature Sets Installed At Selected Oracle Home: [View](#)

This page only shows Feature Sets installed at the selected Oracle Home. It does not show Feature Sets installed anywhere else.

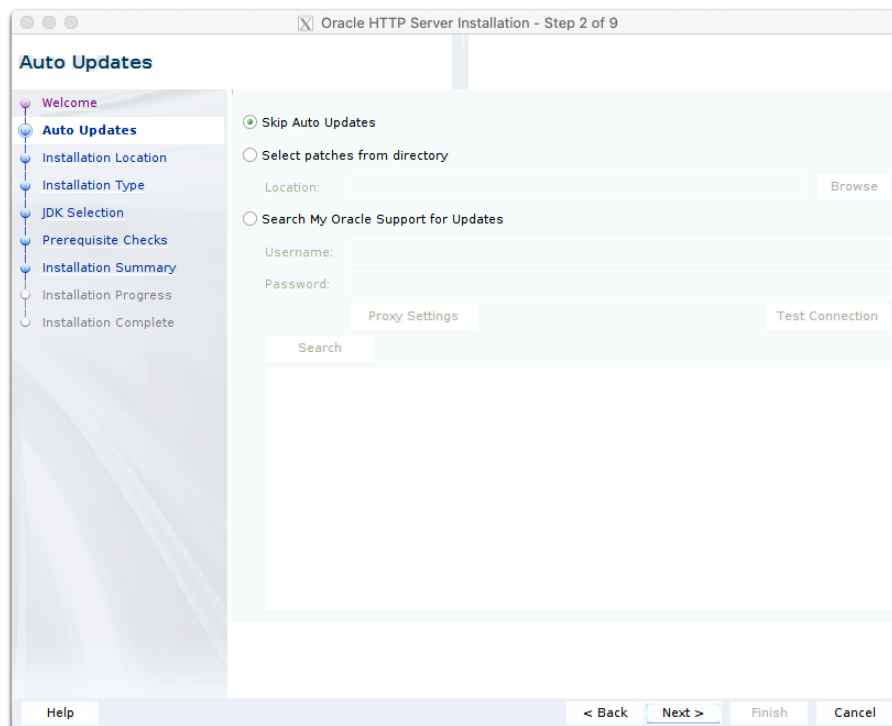


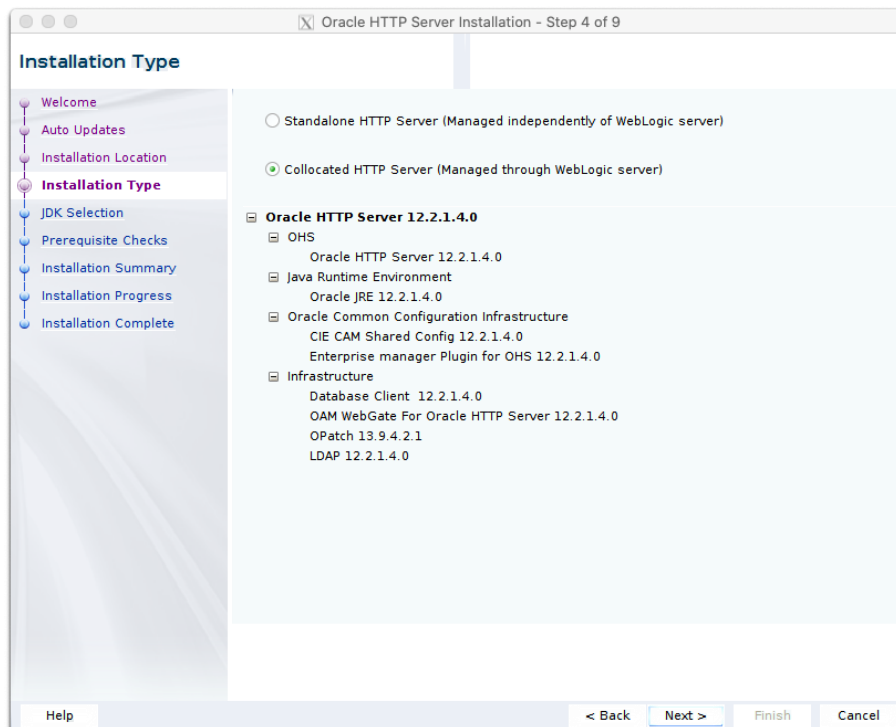
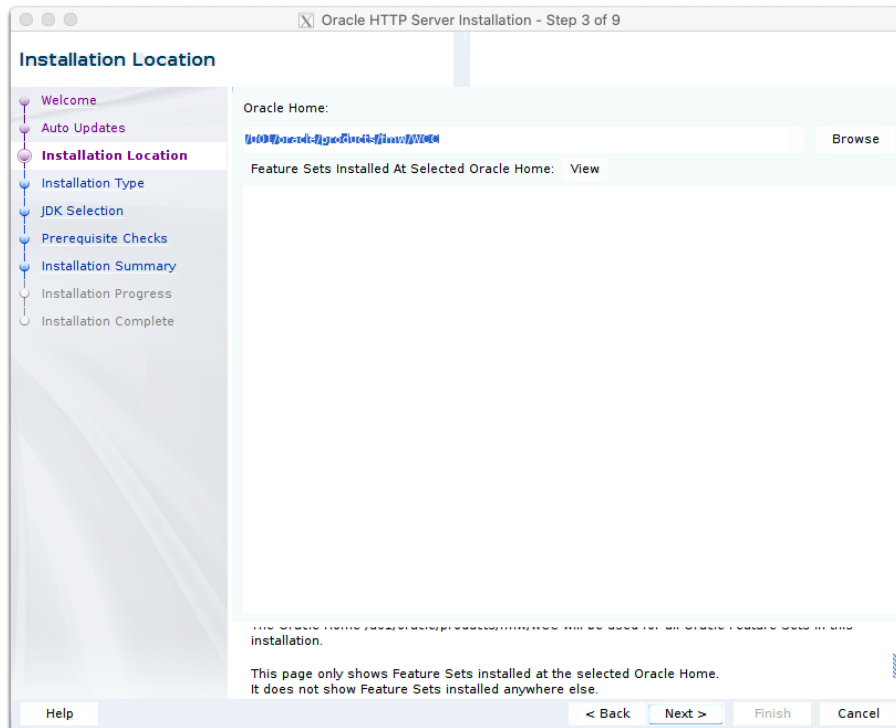


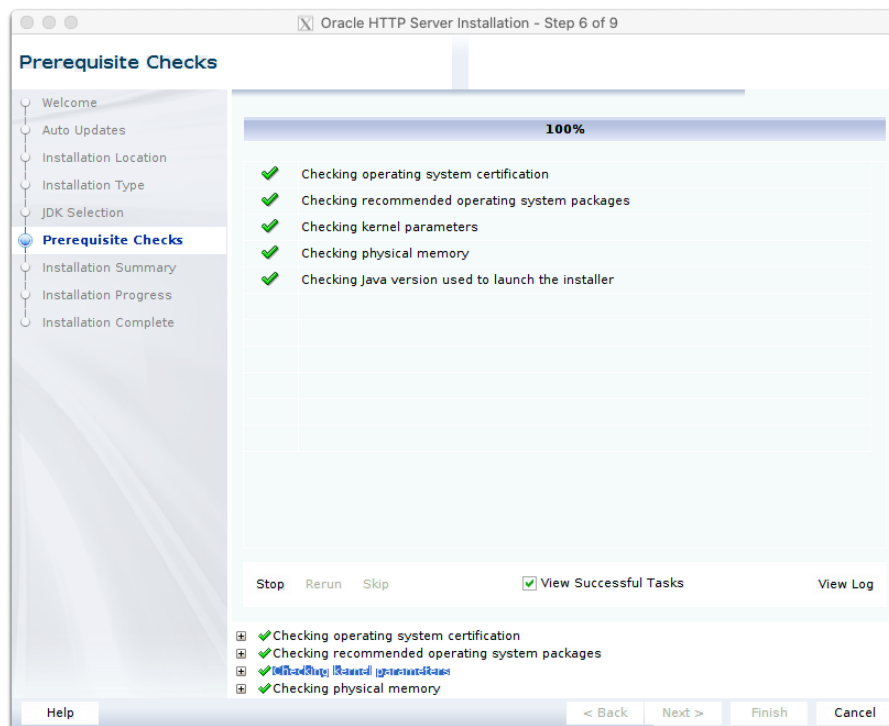
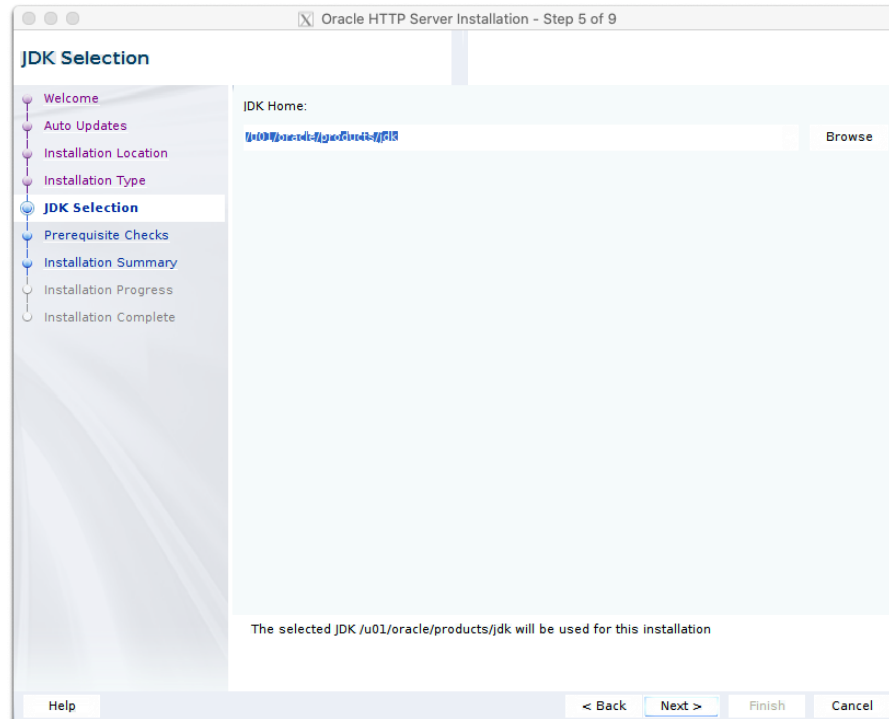


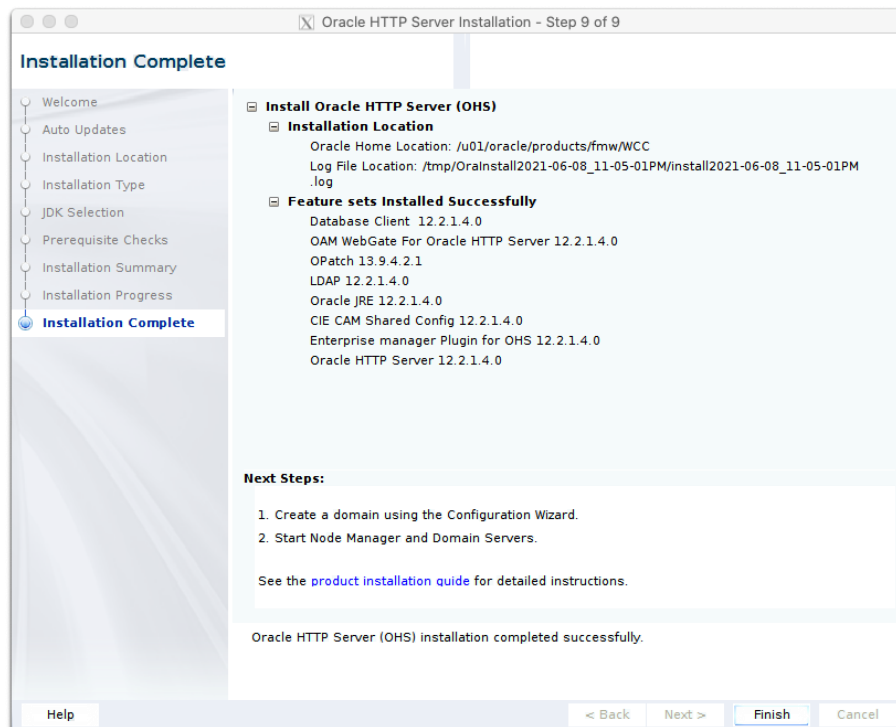
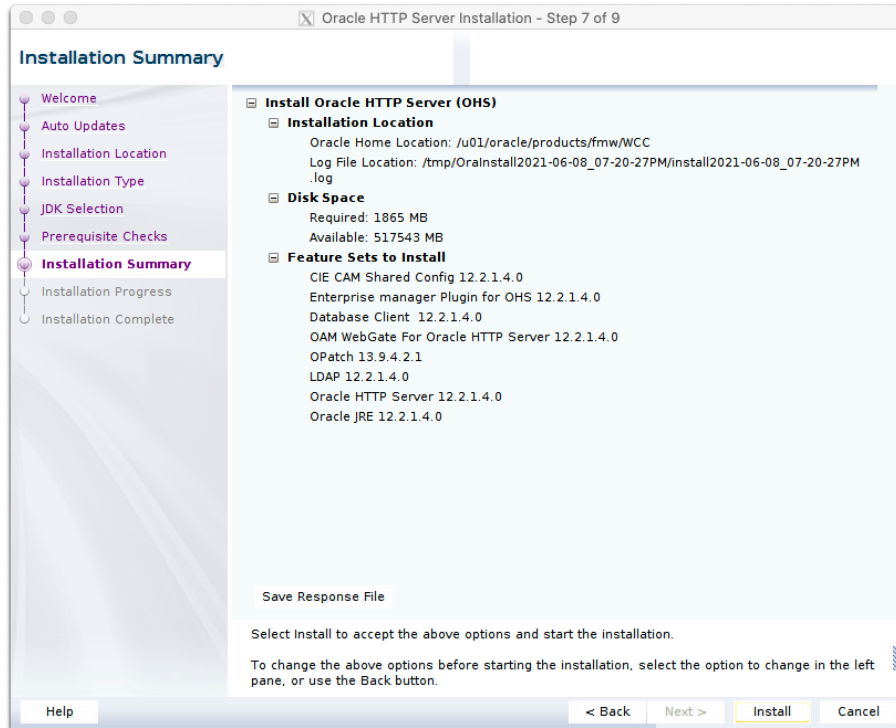
Instalación Oracle OHS:



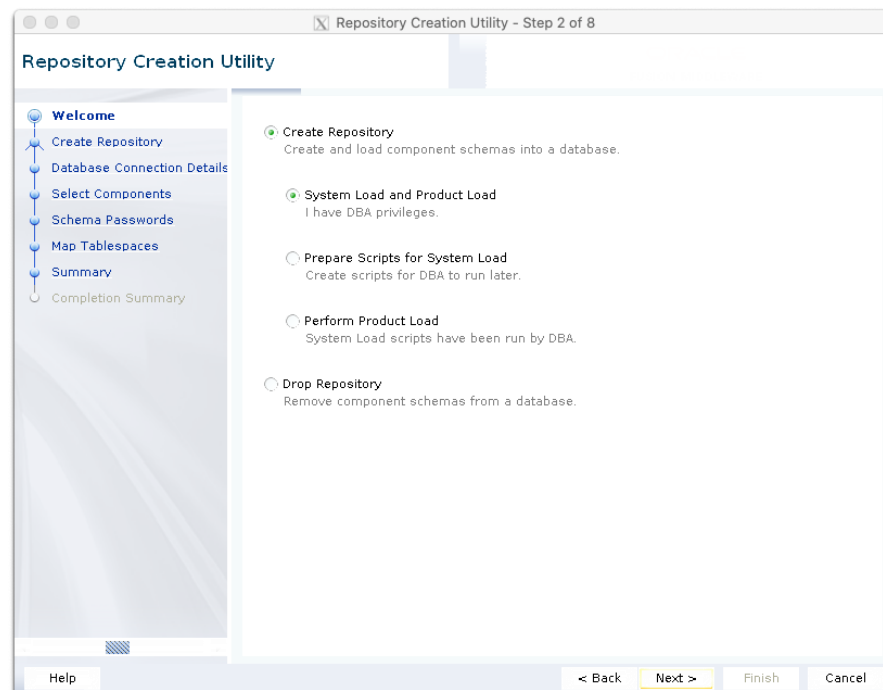
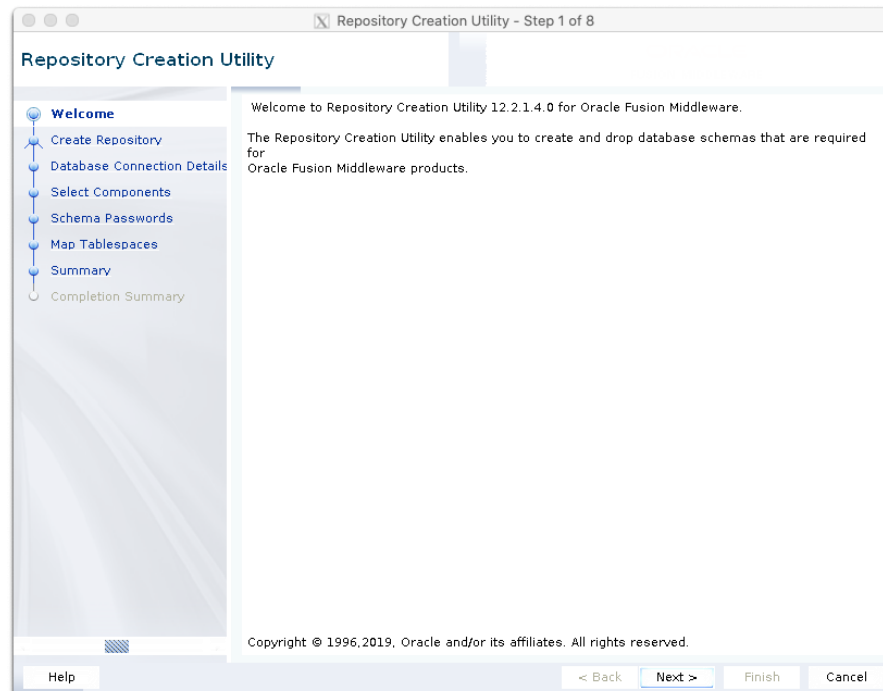








Ejecución RCU:



Repository Creation Utility - Step 3 of 8

Repository Creation Utility

Database Type: Oracle Database

Connection String Format: ☒ Connection Parameters ☐ Connection String

Connect String

Host Name: 10.160.4.48

Port: 1521

Service Name: wccinfra

Username: sys

Password:

Role: SYSDBA

Help < Back Next > Finish Cancel

Repository Creation Utility - Checking Prerequisites

Checking Global Prerequisites

- ✓ Initializing repository configuration metadata 00:06.620(sec)
- ✓ Obtain properties of the specified database 00:00.200(ms)
- ✓ Check requirement for specified database 00:01.904(sec)

Operation completed. Click OK to continue to next page.

OK

Repository Creation Utility - Step 4 of 8

Repository Creation Utility

Specify a unique prefix for all schemas created in this session, so you can easily locate, reference, and manage the schemas later.

☐ Select existing prefix

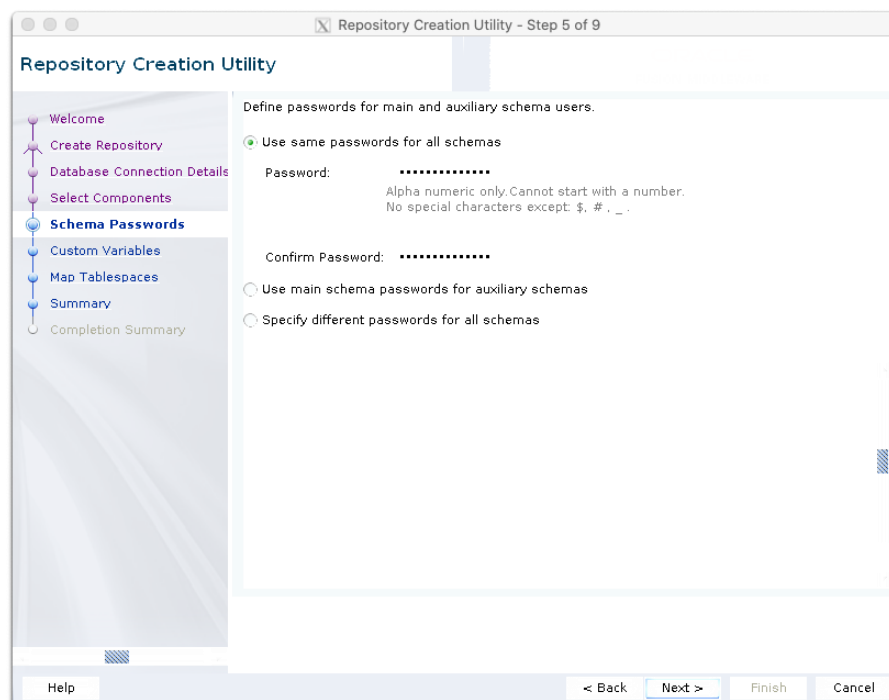
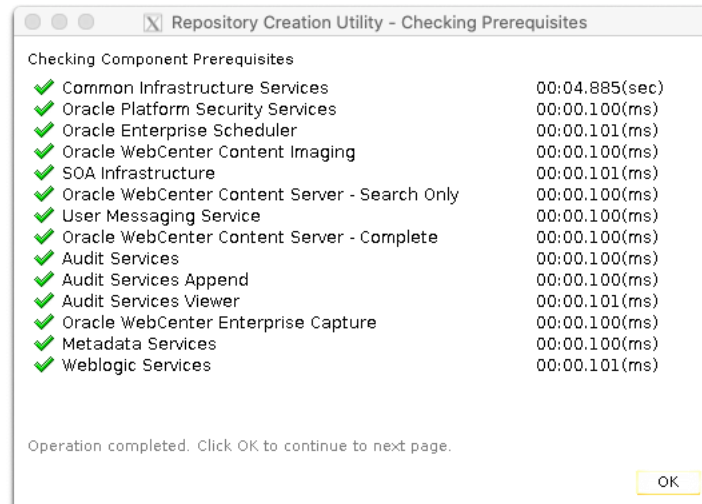
☒ Create new prefix: WCCQA

Alpha numeric only. Cannot start with a number. No special ...

Component	Schema Owner
☒ Common Infrastructure Services *	WCCQA_STB
☒ Oracle Enterprise Scheduler	WCCQA_ESS
☒ Oracle Platform Security Services	WCCQA_OPSS
☒ User Messaging Service	WCCQA_UMS
☒ Audit Services	WCCQA_IAU
☒ Audit Services Append	WCCQA_IAU_APPEND
☒ Audit Services Viewer	WCCQA_IAU_VIEWER
☒ Metadata Services	WCCQA_MDS
☒ Weblogic Services *	WCCQA_WLS
☒ SOA Suite	
☒ SOA Infrastructure	WCCQA_SOAINFRA
☒ WebCenter Content	
☒ Oracle WebCenter Content Imaging	WCCQA_IPM
☒ Oracle WebCenter Content Server - Search ...	WCCQA_OCSSEARCH
☒ Oracle WebCenter Content Server - Complete	WCCQA_OCS
☒ Oracle WebCenter Enterprise Capture	WCCQA_CAPTURE

* Mandatory component. Mandatory components cannot be deselected.

Help < Back Next > Finish Cancel



Repository Creation Utility - Step 6 of 9

Repository Creation Utility

Enter value for the following custom variables.

Component	Custom Variable	Medium	Value
SOA Infrastructure	Database Profile	Medium	No
	Healthcare Integration	No	

Help < Back Next > Finish Cancel

Repository Creation Utility - Step 7 of 9

Repository Creation Utility

Default and temporary tablespaces for the selected components appear in the table below. To create new tablespaces or modify existing tablespaces, use the Manage Tablespaces Button

Manage Tablespaces

Component	Schema Owner	Default Tablespace	Temp Tablespace
Common Infrastructu...	WCCQA_STB	*WCCQA_STB	*WCCQA_IAS_TEMP
Oracle Enterprise Sc...	WCCQA_ESS	*WCCQA_ESS	*WCCQA_IAS_TEMP
Oracle Platform Secu...	WCCQA_OPSS	*WCCQA_IAS_OPSS	*WCCQA_IAS_TEMP
Oracle WebCenter Co...	WCCQA_IPM	*WCCQA_IPM	*WCCQA_IPM_TEMP
SOA Infrastructure	WCCQA_SOAINFRA	*WCCQA_SOAINFRA	*WCCQA_IAS_TEMP
Oracle WebCenter Co...	WCCQA_OCSSEARCH	*WCCQA_OCSSEARCH	*WCCQA_OCSSEARCH...
User Messaging Serv...	WCCQA_UMS	*WCCQA_IAS_UMS	*WCCQA_IAS_TEMP
Oracle WebCenter Co...	WCCQA_OCS	*WCCQA_OCS	*WCCQA_OCS_TEMP
Audit Services	WCCQA_IAU	*WCCQA_IAU	*WCCQA_IAS_TEMP
Audit Services Append	WCCQA_IAU_APPEND	*WCCQA_IAU	*WCCQA_IAS_TEMP
Audit Services Viewer	WCCQA_IAU_VIEWER	*WCCQA_IAU	*WCCQA_IAS_TEMP
Oracle WebCenter En...	WCCQA_CAPTURE	*WCCQA_CAPTURE	*WCCQA_CAPTURE_TE...
Metadata Services	WCCQA_MDS	*WCCQA_MDS	*WCCQA_IAS_TEMP
Weblogic Services	WCCQA_WLS	*WCCQA_WLS	*WCCQA_IAS_TEMP

* Default tablespaces (specified in the configuration files) are to be created upon confirmation.

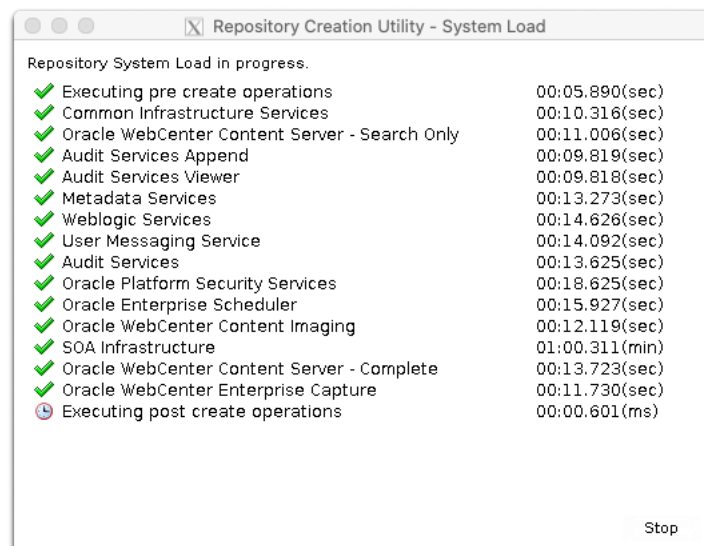
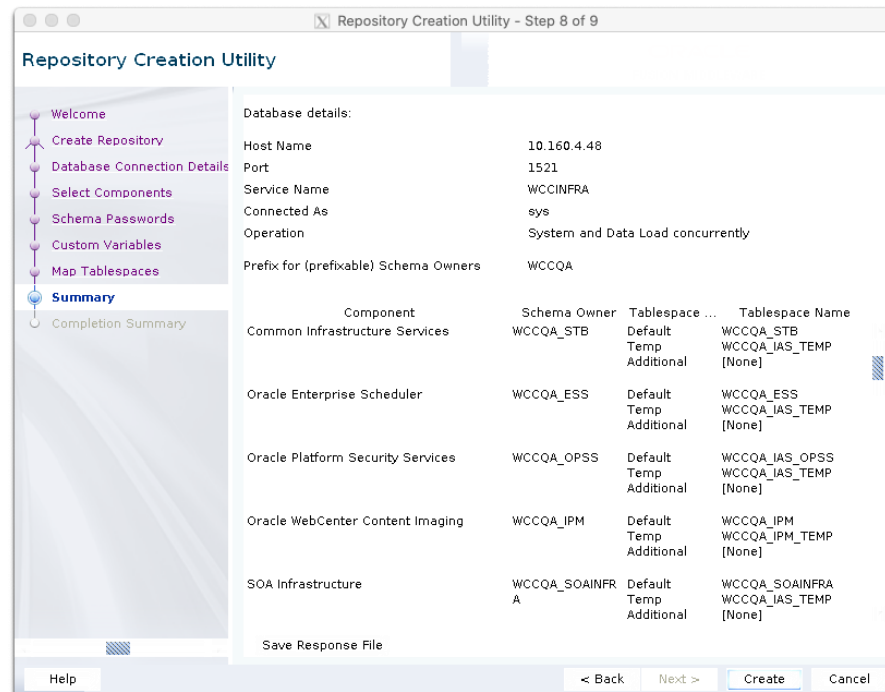
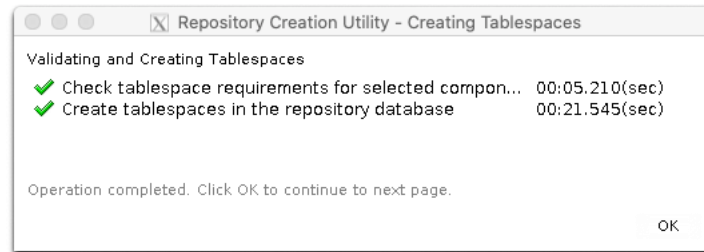
Help < Back Next > Finish Cancel

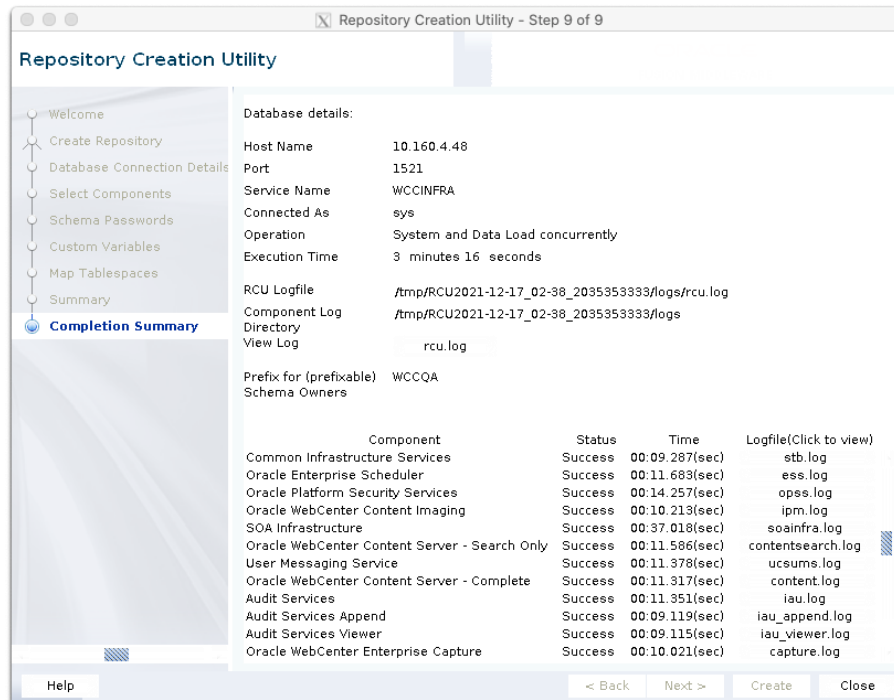
Repository Creation Utility - Confirmation

? Any tablespaces that do not already exist in the selected schemas will be created.

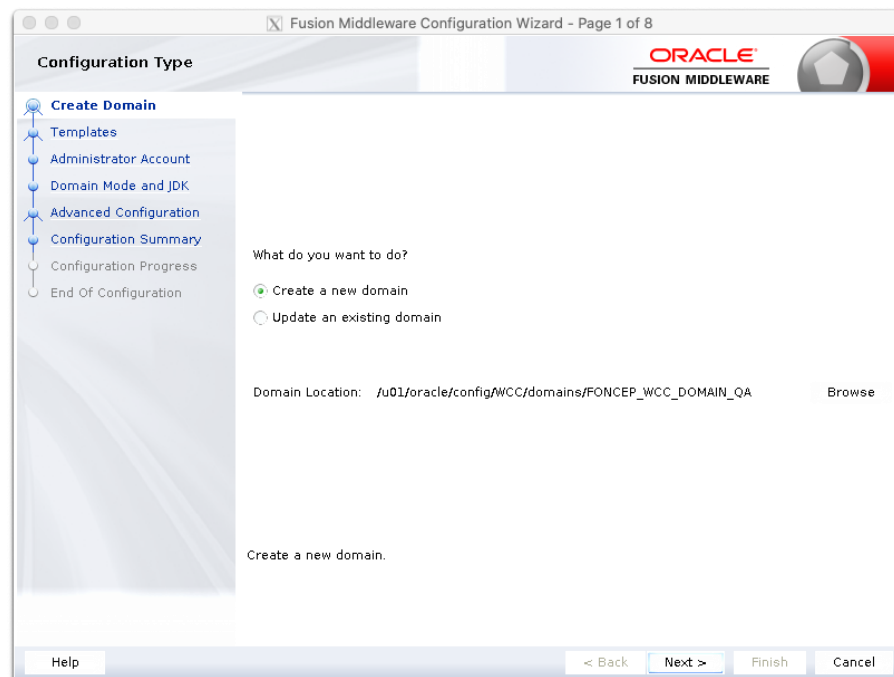
Click OK to create tablespaces.
Click Cancel to return to the wizard.

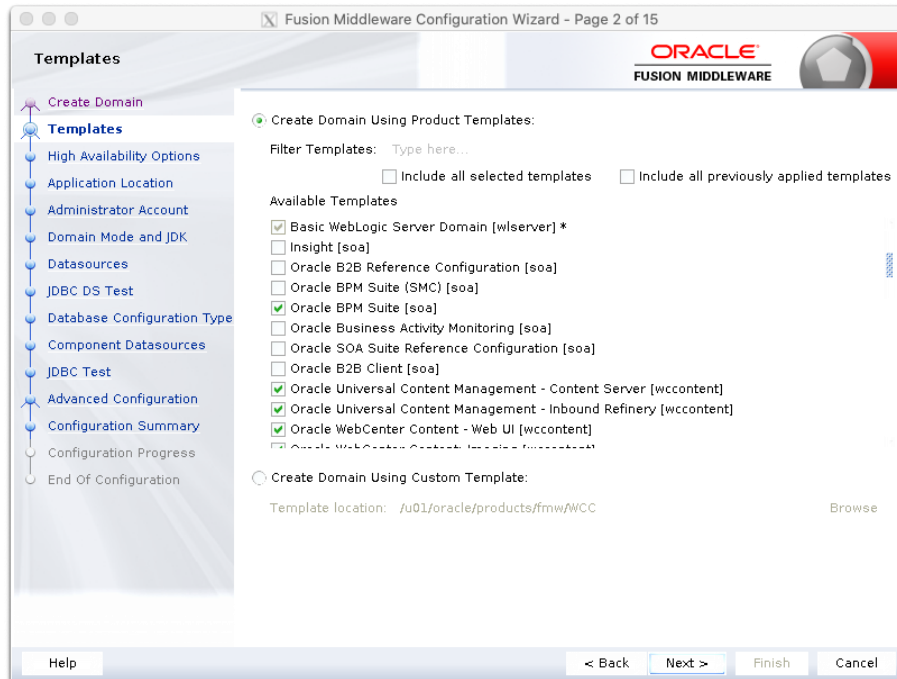
OK Cancel





Creación de Dominio WLS:





Fusion Middleware Configuration Wizard - Page 4 of 17

Application Location

ORACLE
FUSION MIDDLEWARE

- Create Domain
- Templates
- High Availability Options
- Application Location**
- Administrator Account
- Domain Mode and JDK
- Datasources
- JDBC DS Test
- Database Configuration Type
- Component Datasources
- JDBC Test
- Credentials
- Keystore
- Advanced Configuration
- Configuration Summary
- Configuration Progress
- End Of Configuration

Domain name: FONCEP_WCC_DOMAIN_QA

Domain location: /u01/oracle/config/WCC/domains

Application location: /u01/oracle/config/WCC/domains/applications Browse

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 4 of 12

Administrator Account

ORACLE
FUSION MIDDLEWARE

- Create Domain
- Templates
- Application Location
- Administrator Account**
- Domain Mode and JDK
- Database Configuration Type
- Component Datasources
- JDBC Test
- Advanced Configuration
- Configuration Summary
- Configuration Progress
- End Of Configuration

Name weblogic

Password

Confirm Password

Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 5 of 12

Domain Mode and JDK

Domain Mode

☐ Development
Utilize boot.properties for username and password, and poll for applications to deploy.

☒ Production
Require the entry of a username and password, and do not poll for applications to deploy.

JDK

☒ Oracle HotSpot 1.8.0_291 /u01/oracle/products/jdk

☐ Other JDK Location: Browse

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 7 of 17

JDBC Data Sources

Vendor: Oracle Driver: *Oracle's Driver (Thin) for Service connections; Ve

☒ Connection Parameters ☐ Connection URL String

Host Name: 10.160.4.48

DBMS/Service: wccinfra Port: 1521

Username: WCCQA_MDS Password:

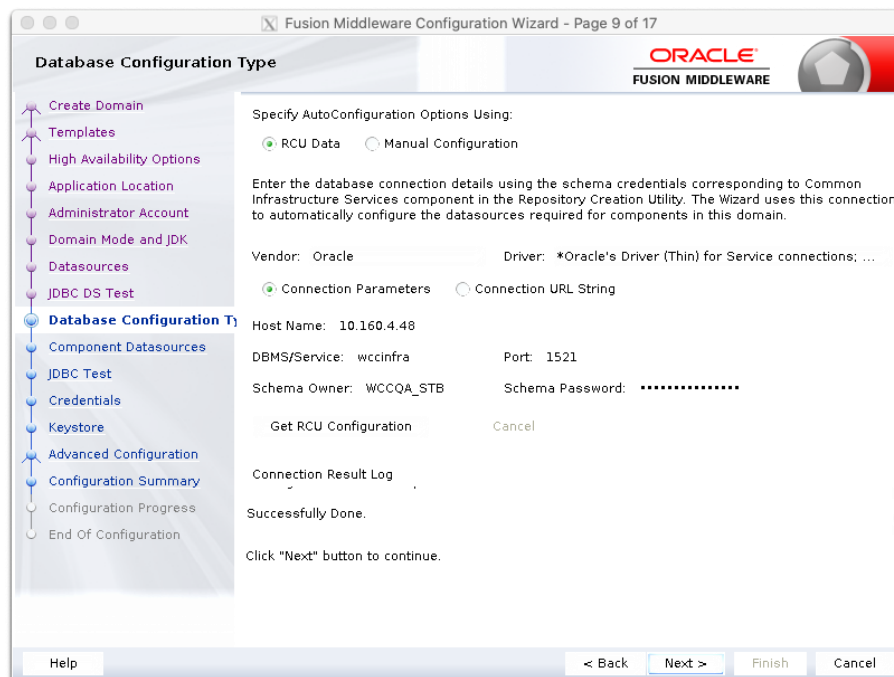
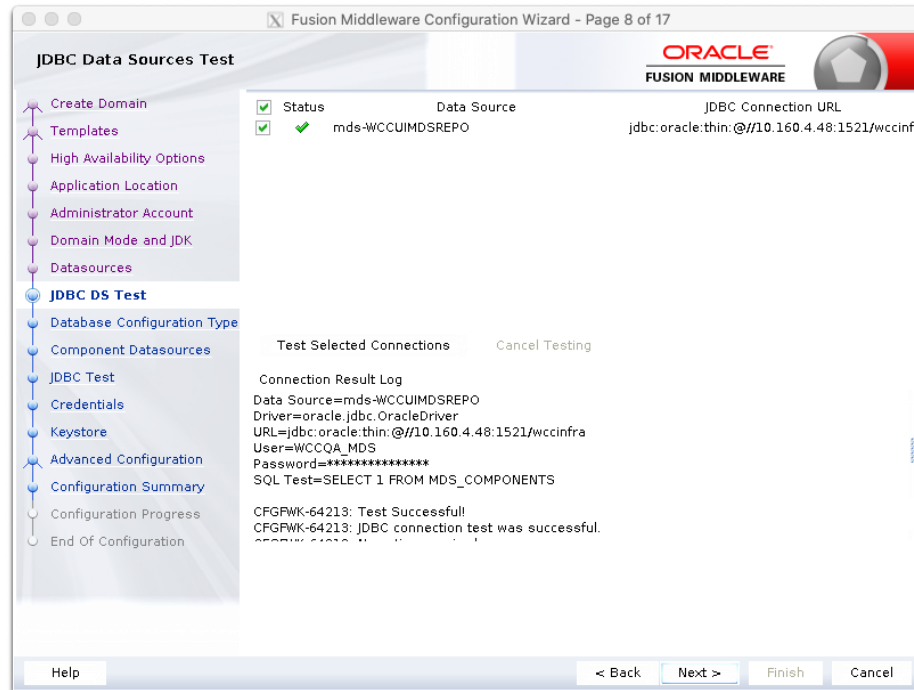
Oracle RAC configuration for data sources:

☐ Convert to GridLink ☐ Convert to RAC multi data source ☐ Don't convert

Edits to the data above will affect all checked rows in the table below.

	Data Source	DBMS/Service	Host Name	Port	Username	Password
☒	mds-WCCUIMDSREPO	wccinfra	10.160.4.48	1521	WCCQA_MDS	

Help < Back Next > Finish Cancel



Fusion Middleware Configuration Wizard - Page 10 of 17

JDBC Component Schema

Vendor: Driver:

☒ Connection Parameters ☐ Connection URL String

Host Name:

DBMS/Service: Port:

Schema Owner: Schema Password:

Oracle RAC configuration for component schemas:

☐ Convert to GridLink ☐ Convert to RAC multi data source ☐ Don't convert

Edits to the data above will affect all checked rows in the table below.

☐	Component Schema	DBMS/Service	Host Name	Port	Schema Ow...	Schema Pasw...
☐	UCM Schema	WCCINFRA	10.160.4.48	1521	WCCQA_OCS	
☐	SOA EDN (XA)	WCCINFRA	10.160.4.48	1521	WCCQA_SOAI	
☐	SOA EDN (Local)	WCCINFRA	10.160.4.48	1521	WCCQA_SOAI	
☐	IPM Schema	WCCINFRA	10.160.4.48	1521	WCCQA_IPM	
☐	LocalSvcTbl Schema	WCCINFRA	10.160.4.48	1521	WCCQA_STB	
☐	User Messaging Ser	WCCINFRA	10.160.4.48	1521	WCCQA_UMS	
☐	SOA (XA)	WCCINFRA	10.160.4.48	1521	WCCQA_SOAI	

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 11 of 17

JDBC Component Schema Test

☒ Status Component Schema JDBC Connection URL

☒	UCM Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA EDN (XA)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA EDN (Local)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	IPM Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	LocalSvcTbl Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	User Messaging Service	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA (XA)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	SOA (Local)	jdbc:oracle:thin:@//10.160.4.48:1521/W
☒	WLS Schema	jdbc:oracle:thin:@//10.160.4.48:1521/W

Test Selected Connections Cancel Testing

Connection Result Log

Component Schema=UCM Schema
Driver=oracle.jdbc.OracleDriver
URL=jdbc:oracle:thin:@//10.160.4.48:1521/WCCINFRA
User=WCCQA_OCS
Password=*****
SQL Test=select 1 from schema_version_registry where owner=(select user from dual) and mr_type

CFGFWK-64213: Test Successful!
CFGFWK-64213: JDBC connection test was successful
999999

Help < Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 12 of 17

Credentials

ORACLE
FUSION MIDDLEWARE

[+ Add](#) [X Delete](#) [Discard Changes](#)

Key Name	Username	Password	Store Name
wccadfConnectUser	weblogic	*****	oracle.wcc.security

Navigation: Create Domain, Templates, High Availability Options, Application Location, Administrator Account, Domain Mode and JDK, Datasources, JDBC DS Test, Database Configuration Type, Component Datasources, JDBC Test, **Credentials**, Keystore, Advanced Configuration, Configuration Summary, Configuration Progress, End Of Configuration

[Help](#) [< Back](#) [Next >](#) [Finish](#) [Cancel](#)

Fusion Middleware Configuration Wizard - Page 13 of 17

Keystore

ORACLE
FUSION MIDDLEWARE

[Discard Changes](#)

Store Key Name: ums/apns

Alias	Trusted Certificate
Alias	

Alias	Private Key	Password	Identity Certificate

Navigation: Create Domain, Templates, High Availability Options, Application Location, Administrator Account, Domain Mode and JDK, Datasources, JDBC DS Test, Database Configuration Type, Component Datasources, JDBC Test, Credentials, **Keystore**, Advanced Configuration, Configuration Summary, Configuration Progress, End Of Configuration

[Help](#) [< Back](#) [Next >](#) [Finish](#) [Cancel](#)

Fusion Middleware Configuration Wizard - Page 14 of 26

Advanced Configuration

ORACLE
FUSION MIDDLEWARE

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Administration Server
Node Manager
Managed Servers
Clusters
Server Templates
Coherence Clusters
Machines
Help

☒ **Administration Server**
Modify Settings

☐ **File Store**
Modify Settings

☒ **Node Manager**
Configure Node Manager

☒ **Topology**
Add, Delete or Modify Settings for Managed Servers, Clusters, Virtual Targets and Coherence

☒ **System Components**
Configure and Target System Components

☐ **Domain Frontend Host Capture**
Configure Domain Frontend Host

☐ **Deployments and Services**
Target to Servers or Clusters

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 15 of 26

Administration Server

ORACLE
FUSION MIDDLEWARE

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Administration Server
Node Manager
Managed Servers
Clusters
Server Templates
Coherence Clusters
Machines
Help

Server Name

Listen Address All Local Addresses

Listen Port 7001

Enable SSL ☐

SSL Listen Port

Server Groups Unspecified

The name must not be null or empty and may not contain any : , = * ? % / _ cloned.

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 16 of 26

Node Manager

Node Manager Type

☐ Per Domain Default Location

☒ Per Domain Custom Location

Node Manager Home: /u01/oracle/config/nodemanager Browse

☐ Manual Node Manager Setup

Node Manager Credentials

Username: weblogic

Password:

Confirm Password:

Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.

< Back **Next >** Finish Cancel

Fusion Middleware Configuration Wizard - Page 17 of 26

Managed Servers

Managed Servers

+ Add 📄 Clone ✗ Delete 🔄 Discard Changes

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WCCADF_server1	All Local Address...	16225	☐	Disabled	UCM-ADF...
UCM_server1	All Local Address...	16200	☐	Disabled	UCM-MGD...
IBR_server1	All Local Address...	16250	☐	Disabled	IBR-MGD...
IPM_server1	All Local Address...	16000	☐	Disabled	IPM-MGD...
SOA_server1	All Local Address...	9103	☐	Disabled	SOA-MGD...
CUST_server1	All Local Address...	9105	☐	Disabled	Unspecified

< Back **Next >** Finish Cancel

Fusion Middleware Configuration Wizard - Page 21 of 27

Machines

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Administration Server
Node Manager
Managed Servers
Clusters
Server Templates
Coherence Clusters
Machines
Help

Machine Unix Machine

+ Add X Delete Discard Changes

Name	Enable	Post Bind GID	Enable	Post Bind UID	Node Manager Listen Address	Node Manager
gestormdqa	☐	nobody	☐	nobody	gestormdqa	5556

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 22 of 27

Assign Servers to Machines

Create Domain
Templates
High Availability Options
Application Location
Administrator Account
Domain Mode and JDK
Datasources
JDBC DS Test
Database Configuration Type
Component Datasources
JDBC Test
Credentials
Keystore
Advanced Configuration
Administration Server
Node Manager
Managed Servers
Clusters
Server Templates
Coherence Clusters
Machines
Help

Servers

Machines

- UnixMachine
 - gestormdqa
 - AdminServer
 - CUST_server1
 - IBR_server1
 - IPM_server1
 - SOA_server1
 - UCM_server1
 - WCCADF_server1

Select **one or more** servers in the left pane and **one** machine in the right pane. Then use the right arrow button (>) to assign the server or servers to the machine.

< Back Next > Finish Cancel

Fusion Middleware Configuration Wizard - Page 25 of 29

System Components

+ Add - Delete Discard Changes

System Component	Component Type	Restart Interval Seconds	Restart Delay Seconds
ohs1	OHS	3600	0

Navigation: Help < Back Next > Finish Cancel

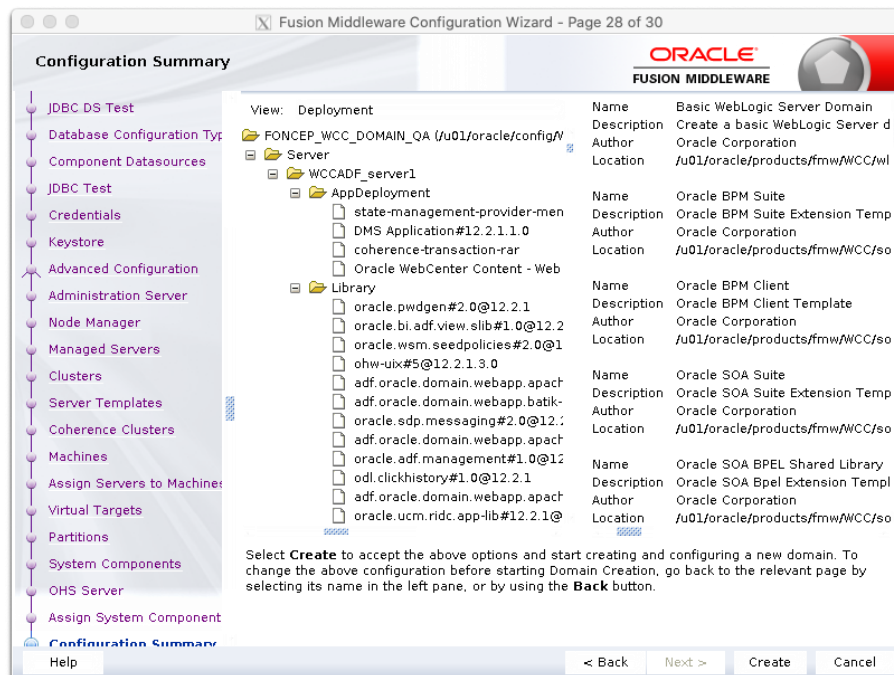
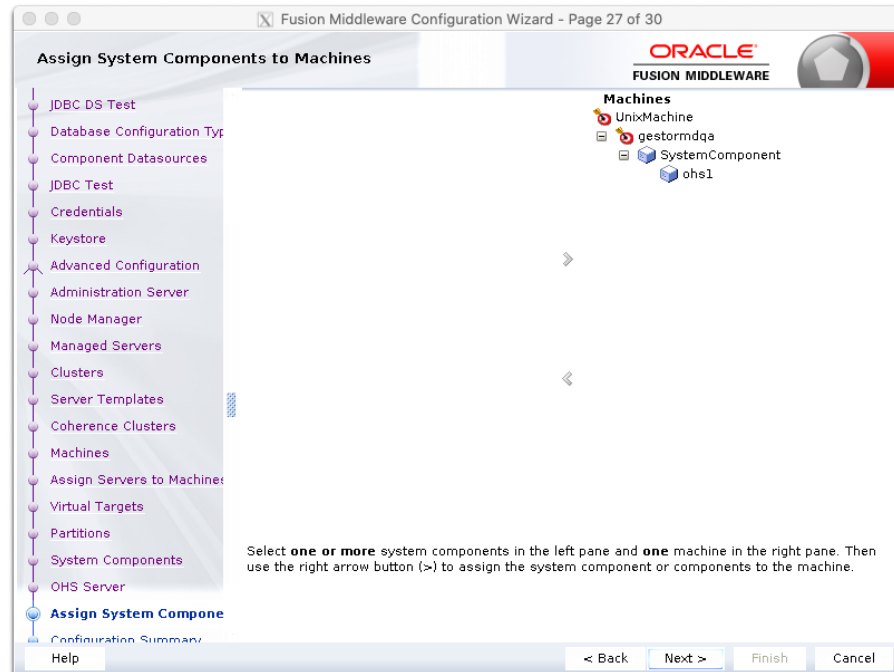
Fusion Middleware Configuration Wizard - Page 26 of 30

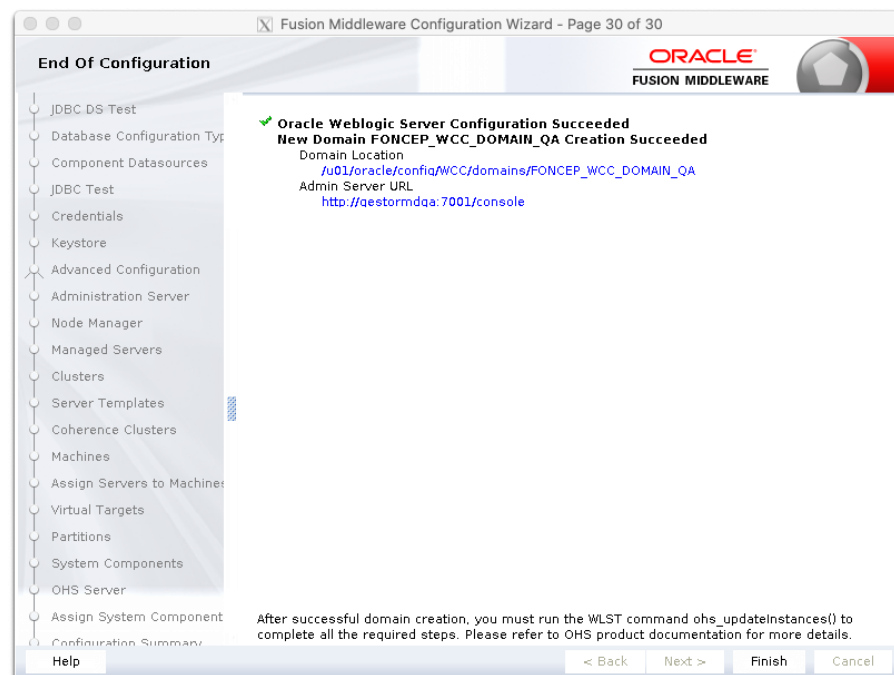
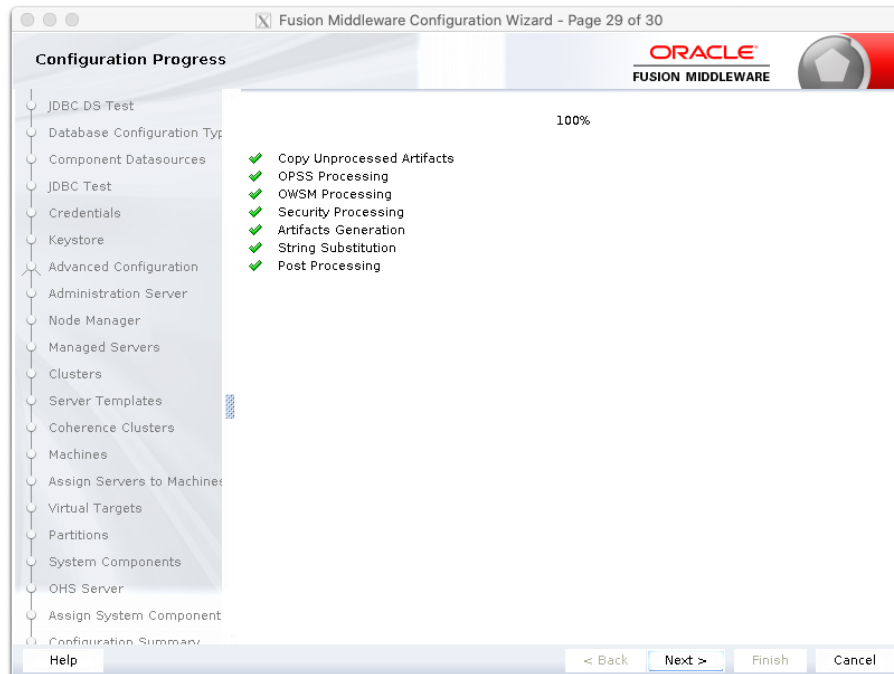
OHS Server

System Component ohs1

Admin Host	127.0.0.1
Admin Port	7779
Listen Address	
Listen Port	7777
SSL Listen Port	4443
Server Name	http://localhost:7777

Navigation: Help < Back Next > Finish Cancel





Consolas de Producto:

WebLogic Server - <http://gestormdqa:7001/console>

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: FONCEP_WCC_DOMAIN_QA

Home > Summary of Machines > gestormdqa > Summary of Servers

Summary of Servers

Configuration Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration. This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

Servers (Filtered - More Columns Exist)

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

New Clone Delete Showing 1 to 7 of 7 Previous Next

Name	Type	Cluster	Machine	State	Health	Listen Port
AdminServer(admin)	Configured		gestormdqa	RUNNING	OK	7001
CUST_server1	Configured		gestormdqa	RUNNING	OK	9105
IBR_server1	Configured		gestormdqa	RUNNING	OK	16250
IPM_server1	Configured		gestormdqa	RUNNING	OK	16000
SOA_server1	Configured		gestormdqa	RUNNING	OK	9103
UCM_server1	Configured		gestormdqa	RUNNING	OK	16200
WCCADF_server1	Configured		gestormdqa	RUNNING	OK	16225

New Clone Delete Showing 1 to 7 of 7 Previous Next

How do I...
 • Create Managed Servers
 • Clone servers
 • Delete Managed Servers
 • Delete the Administration Server
 • Start and stop servers
 • View objects in the JNDI tree

System Status

Enterprise Manager Fusion Middleware Control- <http://gestormdqa:7001/em>

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain weblogic

FONCEP_WCC_DOMAIN_QA

WebLogic Domain

Information
 Certain functionality on this page is available only when you own the edit session lock. To obtain the lock, click "Lock and Edit" in the Change Center menu.

Servers
 7 Up

Clusters
 0 Clusters

Deployments
 6 Down 25 Up

Administration Server

Name AdminServer
 Host gestormdqa.segqa.segdmz.oraclevcn.com
 Listen Port 7001

Servers

View Create Delete Control

Name	Status	Cluster	Machine	State	Health	Listen Port	C Usage
AdminServer(admin)	Running		gestormdqa	Running	OK	7001	0
CUST_server1	Running		gestormdqa	Running	OK	9105	Unavail
IBR_server1	Running		gestormdqa	Running	OK	16250	0
IPM_server1	Running		gestormdqa	Running	OK	16000	0
SOA_server1	Running		gestormdqa	Running	OK	9103	0

Columns Hidden 34 Servers 7 of 7

WebCenter Content - <http://gestormdqa:16200/cs>

WebCenter Content Configuration

Node Information

Cluster Node Identifier:  UCM_server1

*** Content Server Instance Folder:**  /u01/oracle/config/WCC/domains/FONCEP_WCC_

*** Native File Repository Location:**  /u01/oracle/config/WCC/domains/FONCEP_WCC_

*** Weblayout Folder:**  /u01/oracle/config/WCC/domains/FONCEP_WCC_

*** User Profile Folder:**  /u01/oracle/config/WCC/domains/FONCEP_WCC_

Content Server URL Prefix:  /cs/

Instance Information

Is New Content Server Instance:  ☒

Server Socket Port:  4444

Incoming Socket Connection Address Security Filter:  127.0.0.1|10.160.4.149|0:0:0:0:0:0:1

*** Web Server HTTP/HTTPS Address:**  gestormdqa.segqa.segdmz.oraclevcn.com:1620

Web Address Is HTTPS:  ☐

Company Mail Server:  mail

Administrator E-Mail Address:  sysadmin@example.com

*** Server Instance Name:**  gestormdqa_4444

*** Server Instance Label:**  gestormdqa_4444

*** Server Instance Description:**  Instance gestormdqa_4444

Is Auto Number Enabled:  ☒

Auto Number Prefix:  gestormdqa_444

SOA Suite - <http://gestormdqa:9103/soa-infra>

Welcome to the Oracle SOA/BPM Platform on WebLogic

SOA Version: v12.2.1.4.0 - MAIN_190828.0353.3300
WebLogic Server 12.2.1.4.0 (12.2.1.4.0)
Running on: SOA_server1

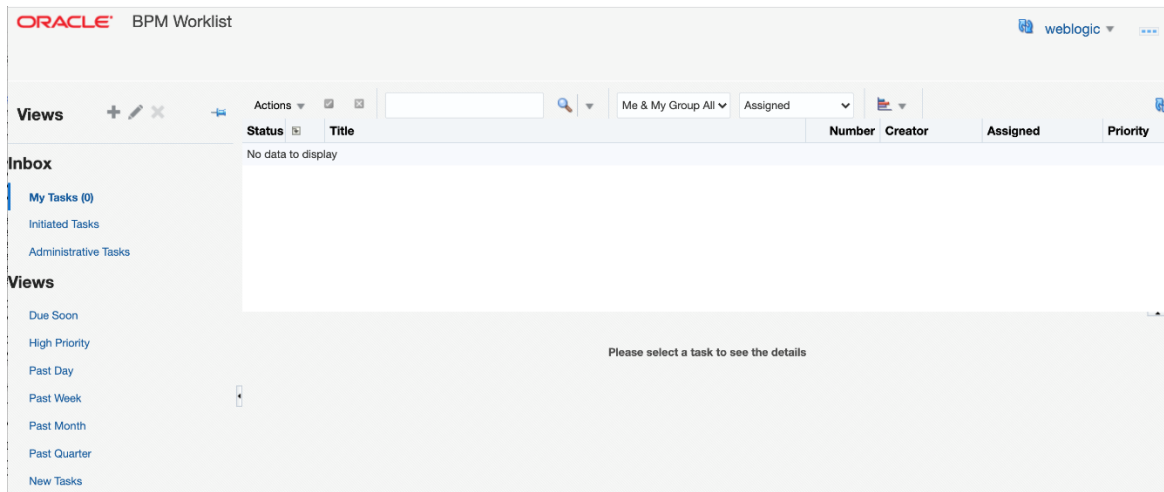
The following composites are currently deployed:

1. default/SimpleApproval!1.0*soa_6c7ecaaf-81ee-497b-81c9-29d8d0f320b9
 - [Test client](#)

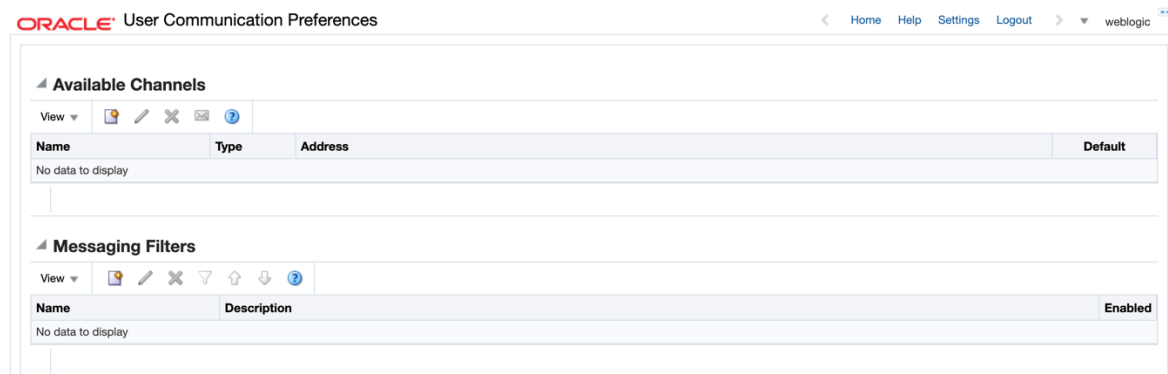
Links

[SOA Composer](#)
[BPM Worklist](#)
[Business Process Composer](#)
[Business Process Workspace](#)
[B2B Console](#)

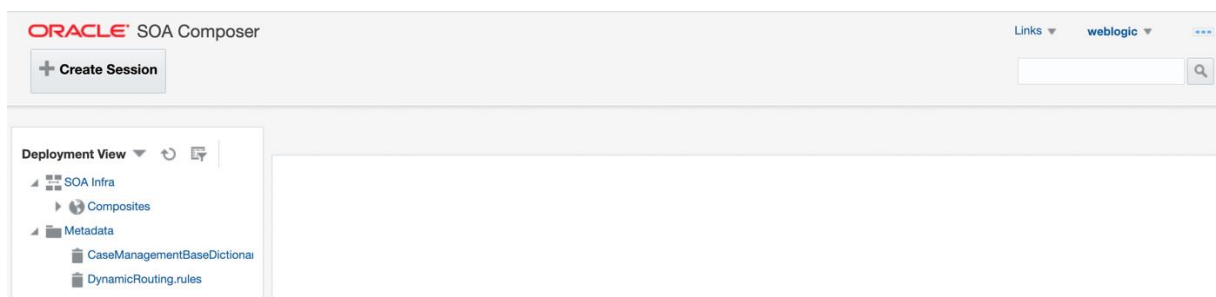
Oracle BPM - <http://gestormdqa:9103/integration/worklistapp>



User Communication Preference - <http://gestormdqa:9103/sdpmessaging/userprefs-ui>



SOA Composer - <http://gestormdqa:9103/soa/composer/>



WebServices Manager - <http://gestormdqa:9103/wsm-pm/>

[Validate Policy Manager](#)

Copyright © 2007, 2019, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Inbound Refinery - <http://gestormdqa:16250/ibr>

Inbound Refinery Configuration

Instance Information

Inbound Refinery Instance Identifier:	IBR_server1
* Inbound Refinery Instance Folder:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
* Native File Repository Location:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
* Weblayout Folder:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
* User Profile Folder:	/u01/oracle/config/WCC/domains/FONCEP_WCC_
Register Start Menu Actions:	☒
* Server Socket Port:	5555
Incoming Socket Connection Address Security Filter:	127.0.0.1 0:0:0:0:0:0:1
* Web Server HTTP/HTTPS Address:	gestormdqa.segqa.segdmz.oraclevcn.com:1625
Web Address Is HTTPS:	☐
Inbound Refinery URL Prefix:	/ibr/
* Server Instance Name:	gestormdqa379250cncom16250
* Server Instance Label:	gestormdqa379250cncom16250
* Server Instance Description:	Instance gestormdqa379250cncom16250

*** - Required**

Oracle Colombia,
Calle 100 No. 13 - 21 Piso 15
Bogotá, Colombia

Phone: +57 1 611 96 00
Fax: +57 1 611 96 00



Hardware and Software, Engineered to Work Together

CONNECT WITH US



Copyright © 2014, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0715

Información del Proyecto

Proyecto: **Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA**

Acta de Pruebas de Funcionalidad

Objetivo: Realización de un conjunto de pruebas técnicas para la verificación de la configuración y parametrización de los componentes de software Oracle que integran el Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA

1.1.

1.2. Especificación

Nombre de Prueba	Verificación instalación del SW		Número de Prueba	001	
Descripción Prueba	Acceso a la infraestructura tecnológica de la entidad para verificar los directorios donde fueron desplegados los componentes Oracle		Escenario Prueba	Verificación de la existencia de los directorios con los componentes de software Oracle	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso a las BD		Número de Prueba	002	
Descripción Prueba	Prueba de ingreso a las BD		Escenario Prueba	Ingreso correcto a las BD	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso WebLogic Server		Número de Prueba	003	
Descripción Prueba	Prueba de autenticación a la consola de WebLogic Server con un usuario con privilegios de administrador		Escenario Prueba	Autenticación exitosa en http://gestormdqa:7001/console	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso Enterprise Manager Fusion Middleware Control		Número de Prueba	004	
Descripción Prueba	Prueba de autenticación a la consola de Enterprise Manager Fusion Middleware Control		Escenario Prueba	Autenticación exitosa en http://gestormdqa:7001/em	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso WebCenter Content		Número de Prueba	005	
Descripción Prueba	Prueba de autenticación a la consola de WebCenter Content		Escenario Prueba	Autenticación exitosa en http://gestormdqa:16200/cs y validar la configuración	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso SOA Suite		Número de Prueba	006	
Descripción Prueba	Prueba de autenticación a la consola de SOA Suite		Escenario Prueba	Autenticación exitosa en http://gestormdqa:9103/soa-infra	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	15 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Acceso Oracle BPM		Número de Prueba	007	
Descripción Prueba	Prueba de autenticación a la consola de Oracle BPM		Escenario Prueba	Autenticación exitosa en http://gestormdqa:9103/integration/worklistapp	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a User Communication Preference		Número de Prueba	008	
Descripción Prueba	Ingreso correcto a User Communication Preference		Escenario Prueba	Es posible ingresar a http://gestormdqa:9103/sdpMessaging/userprefs-ui y administrar “Available Channels” y “Messaging Filters”	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	20 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a SOA Composer		Número de Prueba	009	
Descripción Prueba	Ingreso correcto a SOA Composer		Escenario Prueba	Es posible ingresar a http://gestormdqa:9103/soa/composer/ y administrar	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a WebServices Manager		Número de Prueba	010	
Descripción Prueba	Ingreso correcto a WebServices Manager		Escenario Prueba	Es posible ingresar a http://gestormdqa:9103/wsm-pm/ y ver Validate Policy Manager	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	30 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

Nombre de Prueba	Ingreso a Inbound Refinery		Número de Prueba	011	
Descripción Prueba	Ingreso correcto a Inbound Refinery		Escenario Prueba	Es posible ingresar a http://gestormdqa:16250/ibr y validar la configuración	
Organizador	Jorge García		Cargo	Coordinador de Infraestructura	
Duración	20 minutos	Hora Inicio		Hora Fin	
Lugar de la Prueba	Edificio Condominio Parque Santander				

1.3. Asistentes

Nombres y Apellidos	Cargo	Empresa	Correo Electrónico
Jorge García	Coordinador de Infraestructura	FONCEP	jmgarcia@foncep.gov.co
Oscar Hernán Rojas	Ingeniero Soporte Avanzado	ORACLE	oscar.hernan.rojas.rodriguez@oracle.com
Marcela Avendaño	Líder Técnico	OCP TECH	marcela.avendano@ocp.tech

1.4. Desarrollo de las Pruebas

2. Número de Prueba	001
Objetivo	Verificación instalación del software
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	002
Objetivo	Ingreso correcto a las BD
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	003
Objetivo	Autenticación exitosa en http://gestormdqa:7001/console
Resultados de la Prueba	Exitoso

Genero Error	No
Solución	N/A

Número de Prueba	004
Objetivo	Autenticación exitosa en http://gestormdqa:7001/em
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	005
Objetivo	Autenticación exitosa en http://gestormdqa:16200/cs y validar la configuración
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	006
Objetivo	Autenticación exitosa en http://gestormdqa:9103/soa-infra
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	007
Objetivo	Autenticación exitosa en http://gestormdqa:9103/integration/worklistapp

Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	008
Objetivo	Es posible ingresar a http://gestormdqa:9103/sdpMessaging/userprefs-ui y administrar "Available Channels" y "Messaging Filters"
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	009
Objetivo	Es posible ingresar a http://gestormdqa:9103/soa/composer/ y administrar
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	010
Objetivo	Es posible ingresar a http://gestormdqa:9103/wsm-pm/ y ver Validate Policy Manager
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

Número de Prueba	011

Objetivo	Es posible ingresar a http://gestormdqa:16250/ibr y validar la configuración
Resultados de la Prueba	Exitoso
Genero Error	No
Solución	N/A

1.4 Aceptación de las Pruebas

Funcionario Técnico FONCEP: Jorge García

Cargo: Coordinador de Infraestructura

Fecha de Aceptación: 17 de Diciembre 2021

Firma Aceptación:



Bogotá, Noviembre 30 de 2021

Señores

Fondo De Prestaciones Económicas Cesantías Y Pensiones Foncep
Ciudad

Para efectos exclusivamente informativos y en virtud de la orden de pedido presentada por nuestro distribuidor autorizado **NEXSYS DE COLOMBIA S.A.S.**, usted es titular de las siguientes licencias de programas Oracle:

Nombre del Programa	Tipo de Licencia	Cantidad
Oracle WebCenter Content - Processor Perpetual	Full Use	1
Oracle SOA Suite for Oracle Middleware – Processor Perpetual	Full Use	1
Oracle SOA Suite for Oracle Middleware – Named User Plus Perpetual	Full Use	10
Oracle WebLogic Server Enterprise Edition - Named User Plus Perpetual	Full Use	10
Oracle WebLogic Server Enterprise Edition - Processor Perpetual	Full Use	1
Oracle WebLogic Suite - Named User Plus Perpetual	Full Use	10
Oracle WebLogic Suite – Processor Perpetual	Full Use	1

Oracle Unified Business Process Management Suite – Named User Plus Perpetual	Full Use	10
Oracle Unified Business Process Management Suite – Processor Perpetual	Full Use	1
Oracle WebCenter Content - Named User Plus Perpetual	Full Use	10

Sin otro particular, aprovechamos la ocasión de enviarle un cordial saludo.

Atentamente,
ORACLE COLOMBIA LTDA.

DocuSigned by:

31F395AF344E446...
German Mayorga
Alliances & Channels Manager



Bogotá, 03 de diciembre 2021

OCP TECH CO-124/2021

NIT 900222314-5

Señores

Fondo de Prestaciones Económicas Cesantías y Pensiones Foncep

Carrera 6 Nro 14 98 piso 6

Ciudad

Ref.: Orden de compra 80732

Asunto: Adquisición, instalación y puesta en funcionamiento de un sistema de gestión de documentos electrónicos de archivo- SGDEA

Cordial Saludo,

Nos es grato haber sido adjudicados del proceso de acuerdo con la orden de compra de la referencia, correspondiente a la contratación de servicios y licencias de Oracle en el marco del contrato Instrumento de generación de demanda de CCE.

Por medio de la presente, cumplimos en brindar mayor detalle sobre los servicios ACS de Oracle adquiridos.

En relación a los ítems 1 y 2 de la orden de compra referente a la contratación de servicios de ACS Oracle, los mismos corresponden a 25 jornadas del perfil Gerente Técnico y 335 jornadas del perfil Ingeniero Soporte Avanzado, donde cada jornada equivale a 8 horas, estos servicios serán utilizados en el proyecto Sistema de Gestión Documental de Archivos de FONCEP a partir del acta de inicio correspondiente.

Sin otro particular,

A handwritten signature in black ink, appearing to be 'MH', written over a horizontal line.

Marcelo Herrera

Representante legal

OCP TECH COLOMBIA SAS NIT 900222314-5

Info.co@ocp.tech

Tel + 601 4423209 + 57 3134653030

AK 9 #115-06 Oficina 701 Edificio Tierra Firme

DOCUMENTACIÓN DE PRODUCTOS DEL FABRICANTE ORACLE

- ▶ Guía de Instalación y Configuración de Oracle Webcenter Content

Oracle® Fusion Middleware - Installing and Configuring Oracle WebCenter Content

<https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/inecm/installing-and-configuring-oracle-webcenter-content.pdf>

- ▶ Guía para el Despliegue Empresarial de Oracle Webcenter Content

Oracle® Fusion Middleware - Enterprise Deployment Guide for Oracle WebCenter Content

<https://docs.oracle.com/middleware/1221/core/CMEDG/CMEDG.pdf>

<https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.3/cmedg/enterprise-deployment-guide-oracle-webcenter-content.pdf>

- ▶ Guía de Iniciación y documentación de Oracle Webcenter Content

<https://docs.oracle.com/en/middleware/webcenter/content/12.2.1.4/index.html>

- ▶ Documentación de otros componentes de la infraestructura de software Oracle

Oracle Business Process Management

<https://docs.oracle.com/en/middleware/fusion-middleware/bpm/12.2.1.4/index.html>

Oracle SOA Suite

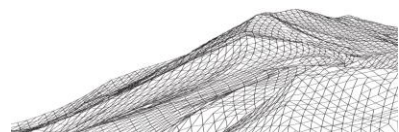
<https://docs.oracle.com/en/middleware/soa-suite/index.html>

Oracle Weblogic Server

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/index.html>

Oracle Database

<https://docs.oracle.com/en/database/oracle/oracle-database/index.html>



Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle WebCenter Content



Release 12.2.1.3
E95487-04
June 2021

ORACLE®

Copyright © 2018, 2021, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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 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" or "commercial computer software documentation" 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 and Java 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

Preface

Audience	xvi
Documentation Accessibility	xvi
Conventions	xvi

Part I Understanding an Enterprise Deployment

1 Enterprise Deployment Overview

About the Enterprise Deployment Guide	1-1
When to Use the Enterprise Deployment Guide	1-2

2 About a Typical Enterprise Deployment

Diagram of a Typical Enterprise Deployment	2-1
About the Typical Enterprise Deployment Topology Diagram	2-2
Understanding the Firewalls and Zones of a Typical Enterprise Deployment	2-3
Understanding the Elements of a Typical Enterprise Deployment Topology	2-3
Receiving Requests Through Hardware Load Balancer	2-4
Purpose of the Hardware Load Balancer (LBR)	2-4
Summary of the Typical Load Balancer Virtual Server Names	2-6
HTTPS Versus HTTP Requests to the External Virtual Server Name	2-7
Understanding the Web Tier	2-7
Benefits of Using Oracle HTTP Server Instances to Route Requests	2-7
Configuration of Oracle HTTP Server in the Web Tier	2-8
About Mod_WL_OHS	2-9
Understanding the Application Tier	2-9
Configuration of the Administration Server and Managed Servers Domain Directories	2-9
About the Node Manager Configuration in a Typical Enterprise Deployment	2-10
About Using Unicast for Communications within the Application Tier	2-11
Understanding OPSS and Requests to the Authentication and Authorization Stores	2-12

3 Understanding the WebCenter Content Enterprise Deployment Topology

Diagram of the WebCenter Content Enterprise Topology	3-2
Understanding the WebCenter Content Enterprise Topology Diagram	3-2
Summary of Oracle WebCenter Content Load Balancer Virtual Server Names	3-3
Summary of the Managed Servers and Clusters on the WebCenter Content Application Tier	3-4
Flow Chart and Roadmap for Implementing the WebCenter Content Enterprise Topology	3-4
Flow Chart of the Steps to Install and Configure the WebCenter Content Enterprise Topology	3-4
Roadmap Table for Planning and Preparing for an Enterprise Deployment	3-7
Roadmap Table for Configuring the Oracle WebCenter Content Topology	3-7

Part II Preparing for an Enterprise Deployment

4 Using the Enterprise Deployment Workbook

Introduction to the Enterprise Deployment Workbook	4-1
Typical Use Case for Using the Workbook	4-2
Using the Oracle WebCenter Content Enterprise Deployment Workbook	4-2
Locating the Oracle WebCenter Content Enterprise Deployment Workbook	4-2
Understanding the Contents of the Oracle WebCenter Content Enterprise Deployment Workbook	4-2
Using the Start Tab	4-3
Using the Hardware - Host Computers Tab	4-3
Using the Network - Virtual Hosts & Ports Tab	4-4
Using the Storage - Directory Variables Tab	4-4
Using the Database - Connection Details Tab	4-5
Who Should Use the Enterprise Deployment Workbook?	4-5

5 Procuring Resources for an Enterprise Deployment

Hardware and Software Requirements for the Enterprise Deployment Topology	5-1
Hardware Load Balancer Requirements	5-1
Host Computer Hardware Requirements	5-2
General Considerations for Enterprise Deployment Host Computers	5-3
Reviewing the Oracle Fusion Middleware System Requirements	5-3

Typical Memory, File Descriptors, and Processes Required for an Enterprise Deployment	5-4
Typical Disk Space Requirements for an Enterprise Deployment	5-5
Operating System Requirements for an Enterprise Deployment Topology	5-5
Reserving the Required IP Addresses for an Enterprise Deployment	5-6
What is a Virtual IP (VIP) Address?	5-6
Why Use Virtual Host Names and Virtual IP Addresses?	5-7
Physical and Virtual IP Addresses Required by the Enterprise Topology	5-7
Identifying and Obtaining Software Distributions for an Enterprise Deployment	5-8

6 Preparing the Load Balancer and Firewalls for an Enterprise Deployment

Configuring Virtual Hosts on the Hardware Load Balancer	6-1
Overview of the Hardware Load Balancer Configuration	6-1
Typical Procedure for Configuring the Hardware Load Balancer	6-2
Summary of the Virtual Servers Required for an Enterprise Deployment	6-2
Additional Instructions for admin.example.com	6-3
Additional Instructions for wcc.example.com	6-3
Additional Instructions for wccinternal.example.com	6-3
Configuring the Firewalls and Ports for an Enterprise Deployment	6-4

7 Preparing the File System for an Enterprise Deployment

Overview of Preparing the File System for an Enterprise Deployment	7-1
Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment	7-2
Understanding the Recommended Directory Structure for an Enterprise Deployment	7-3
File System and Directory Variables Used in This Guide	7-7
About Creating and Mounting the Directories for an Enterprise Deployment	7-11
Summary of the Shared Storage Volumes in an Enterprise Deployment	7-12

8 Preparing the Host Computers for an Enterprise Deployment

Verifying the Minimum Hardware Requirements for Each Host	8-1
Verifying Linux Operating System Requirements	8-2
Setting Linux Kernel Parameters	8-2
Setting the Open File Limit and Number of Processes Settings on UNIX Systems	8-3
Viewing the Number of Currently Open Files	8-3
Setting the Operating System Open File and Processes Limits	8-3
Verifying IP Addresses and Host Names in DNS or hosts File	8-4

Setting the DNS Settings	8-4
Configuring Operating System Users and Groups	8-4
Enabling Unicode Support	8-5
Mounting the Required Shared File Systems on Each Host	8-5
Enabling the Required Virtual IP Addresses on Each Host	8-7

9 Preparing the Database for an Enterprise Deployment

Overview of Preparing the Database for an Enterprise Deployment	9-1
About Database Requirements	9-2
Supported Database Versions	9-2
Additional Database Software Requirements	9-2
Installing and Validating Oracle Text	9-3
Creating Database Services	9-3
Using SecureFiles for Large Objects (LOBs) in an Oracle Database	9-5
About Database Backup Strategies	9-6

Part III Configuring the Enterprise Deployment

10 Creating the Initial Infrastructure Domain for an Enterprise Deployment

Variables Used When Creating the Infrastructure Domain	10-1
Understanding the Initial Infrastructure Domain	10-2
About the Infrastructure Distribution	10-2
Characteristics of the Initial Infrastructure Domain	10-2
Installing the Oracle Fusion Middleware Infrastructure on WCCHOST1	10-3
Installing a Supported JDK	10-3
Locating and Downloading the JDK Software	10-3
Installing the JDK Software	10-4
Starting the Infrastructure Installer on WCCHOST1	10-5
Navigating the Infrastructure Installation Screens	10-5
Installing Oracle Fusion Middleware Infrastructure on the Other Host Computers	10-7
Checking the Directory Structure	10-7
Disabling the Derby Database	10-8
Creating the Database Schemas	10-8
Installing and Configuring a Certified Database	10-9
Starting the Repository Creation Utility (RCU)	10-9
Navigating the RCU Screens to Create the Schemas	10-9
Verifying Schema Access	10-12
Configuring the Infrastructure Domain	10-13

Starting the Configuration Wizard	10-13
Navigating the Configuration Wizard Screens to Configure the Infrastructure Domain	10-13
Starting the Administration Server	10-20
Starting the Node Manager in the Administration Server Domain Home on WCCHOST1	10-21
Creating the boot.properties File	10-21
Starting the Administration Server Using the Node Manager	10-22
Validating the Administration Server	10-23
Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group	10-23
About the Supported Authentication Providers	10-24
About the Enterprise Deployment Users and Groups	10-24
About Using Unique Administration Users for Each Domain	10-25
About the Domain Connector User	10-25
About Adding Users to the Central LDAP Directory	10-25
About Product-Specific Roles and Groups for Oracle WebCenter Content	10-26
Example Users and Groups Used in This Guide	10-26
Prerequisites for Creating a New Authentication Provider and Provisioning Users and Groups	10-27
Backing up the Configuration	10-27
Enabling Authentication Provider Virtualization	10-27
Provisioning a Domain Connector User in the LDAP Directory	10-28
Creating the New Authentication Provider	10-30
Provisioning an Enterprise Deployment Administration User and Group	10-33
Adding the Administration Role to the New Administration Group	10-35
Updating the boot.properties File and Restarting the System	10-36

11 Configuring the Web Tier for an Enterprise Deployment

Variables Used When Configuring the Web Tier	11-1
About the Web Tier Domains	11-2
Installing a Supported JDK	11-2
Locating and Downloading the JDK Software	11-2
Installing the JDK Software	11-2
Installing Oracle HTTP Server on WEBHOST1	11-3
Starting the Installer on WEBHOST1	11-3
Navigating the Oracle HTTP Server Installation Screens	11-4
Verifying the Oracle HTTP Server Installation	11-5
Creating a Web Tier Domain on WEBHOST1	11-6
Starting the Configuration Wizard on WEBHOST1	11-6
Navigating the Configuration Wizard Screens for an Oracle HTTP Server Domain	11-6

Installing and Configuring a Web Tier Domain on WEBHOST2	11-9
Starting the Node Manager and Oracle HTTP Server Instances on WEBHOST1 and WEBHOST2	11-9
Starting the Node Manager on WEBHOST1 and WEBHOST2	11-9
Starting the Oracle HTTP Server Instances	11-9
Configuring Oracle HTTP Server to Route Requests to the Application Tier	11-10
About the Oracle HTTP Server Configuration for an Enterprise Deployment	11-10
Purpose of the Oracle HTTP Server Virtual Hosts	11-11
Recommended Structure of the Oracle HTTP Server Configuration Files	11-11
Modifying the httpd.conf File to Include Virtual Host Configuration Files	11-11
Creating the Virtual Host Configuration Files	11-12
Validating the Virtual Server Configuration on the Load Balancer	11-13
Configuring Routing to the Administration Server	11-13
Turning On the WebLogic Server Plug-In Enabled Flag	11-15
Setting the Front-End URL for the Administration Console and Setting Redirection Preferences	11-16
Validating Access to the Management Consoles and Administration Server	11-16

12 Extending the Domain to Include Oracle WebCenter Content

Installing WebCenter Content for an Enterprise Deployment	12-2
Starting the Installation Program	12-2
Navigating the Installation Screens	12-2
Installing Oracle WebCenter Content on the Other Host Computers	12-3
Verifying the Installation	12-3
Reviewing the Installation Log Files	12-3
Checking the Directory Structure	12-3
Viewing the Contents of Your Oracle Home	12-4
Creating the Oracle WebCenter Content Database Schemas	12-4
Starting the Repository Creation Utility (RCU)	12-4
Navigating the RCU Screens to Create the Schemas	12-5
Extending the Domain for WebCenter Content	12-7
Starting the Configuration Wizard	12-7
Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Content	12-8
Extending the Domain with Static Clusters	12-8
Extending the Domain with Dynamic Clusters	12-16
Completing Postconfiguration and Verification Tasks for WebCenter Content	12-23
Propagating the Extended Domain to the Domain Directories and Machines	12-24
Packing Up the Extended Domain on WCCHOST1	12-24
Unpacking the Domain in Managed Server Domain Home on WCCHOST1	12-25
Unpacking the Domain on WCCHOST2	12-26

Starting the Node Manager in the Managed Server Domain Directory on WCCHOST1	12-27
Starting the WLS_WCC1 Managed Server	12-28
Configuring the Content Server on WLS_WCC1 Managed Server	12-28
Updating the cwallet File in the Administration Server	12-29
Starting the Node Manager in the Managed Server Domain Directory WCCHOST2	12-30
Starting the WLS_WCC2 Managed Server	12-31
Configuring the Content Server on WLS_WCC2 Managed Server	12-31
Validating GridLink Data Sources	12-32
Verifying the Configuration of a GridLink Data Source for WebCenter Content	12-32
Verifying the Configuration of ONS for a GridLink Data Source	12-32
Configuring Additional Parameters	12-33
Configuring Service Retries for Oracle WebCenter Content	12-33
Granting user administrative access to Oracle WebCenter Content	12-34
Granting the WebCenter Content Administrative Roles through Credential Map	12-34
Configuring Content Server for the WebCenter Content User Interface	12-36
Configuring Oracle HTTP Server for the WebCenter Content Cluster	12-37
Configuring Oracle HTTP Server for the WLS_WCC Managed Servers	12-37
Enabling Access for Content Server Admin Applets	12-38
Validating Access Through the Load Balancer	12-39
Verifying the URLs	12-39
Verifying the Cluster Nodes	12-39
Enabling JDBC Persistent Stores	12-40
Enabling Automatic Service Migration	12-40

13 Extending the Domain with Oracle SOA Suite

Variables Used When Configuring Oracle SOA Suite	13-2
Support for Dynamic Clusters in Oracle SOA Suite	13-3
Synchronizing the System Clocks	13-3
Installing the Software for an Enterprise Deployment	13-4
Starting the Oracle SOA Suite Installer on WCCHOST1	13-4
Navigating the Installation Screens	13-4
Installing Oracle SOA Suite on the Other Host Computers	13-5
Verifying the Installation	13-5
Reviewing the Installation Log Files	13-5
Checking the Directory Structure	13-5
Viewing the Contents of Your Oracle Home	13-6
Creating the Oracle SOA Suite Database Schemas	13-6
Starting the Repository Creation Utility (RCU)	13-6

Navigating the RCU Screens to Create the Schemas	13-7
Verifying Schema Access	13-9
Configuring SOA Schemas for Transactional Recovery	13-10
Extending the Enterprise Deployment Domain with Oracle SOA Suite	13-10
Starting the Configuration Wizard	13-11
Navigating the Configuration Wizard Screens to Extend the Domain with Oracle SOA Suite	13-11
Extending the Domain with Static Clusters	13-12
Extending the Domain with Dynamic Clusters	13-19
Targeting Adapters Manually	13-25
Propagating the Extended Domain to the Domain Directories and Machines	13-27
Packing Up the Extended Domain on WCCHOST1	13-27
Unpacking the Domain in the Managed Servers Domain Directory on WCCHOST1	13-28
Unpacking the Domain on WCCHOST2	13-29
Updating the NodeManager Configuration After Unpacking the Domain	13-31
Modifying the Upload and Stage Directories to an Absolute Path in an Enterprise Deployment	13-32
Configuring Listen Addresses When Using Dynamic Clusters	13-34
Starting and Validating the WLS_SOA1 Managed Server	13-34
Starting the WLS_SOA1 Managed Server	13-34
Adding the SOAAdmin Role to the Administrators Group	13-35
Validating the Managed Server by Logging in to the SOA Infrastructure	13-35
Starting and Validating the WLS_SOA2 Managed Server	13-36
Configuring Oracle HTTP Server for the Extended Domain	13-36
Configuring Oracle HTTP Server for SOA in an Oracle WebCenter Content Enterprise Deployment	13-36
Validating the Oracle SOA Suite URLs Through the Load Balancer	13-40
Post-Configuration Steps for Oracle SOA Suite	13-40
Configuring Oracle Adapters for Oracle SOA Suite	13-40
Enabling High Availability for Oracle File and FTP Adapters	13-41
Enabling High Availability for Oracle JMS Adapters	13-45
Enabling High Availability for the Oracle Database Adapter	13-46
Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer	13-47
Considerations for Sync-Async Interactions in a SOA Cluster	13-47
Updating FusionAppsFrontendHostUrl	13-47
Enabling JDBC Persistent Stores	13-48
Enabling Automatic Service Migration	13-49

14 Extending the Domain to Include Inbound Refinery

Overview of Extending the Domain to Include Inbound Refinery	14-1
Extending the Domain for Inbound Refinery	14-2
Starting the Configuration Wizard	14-2
Navigating the Configuration Wizard Screens to Extend the Domain	14-2
Completing Postconfiguration and Verification Tasks for Inbound Refinery	14-7
Propagate the Domain Configuration Updates for Inbound Refinery	14-7
Starting the Node Manager in the Managed Server Domain Directory	14-8
Starting the Inbound Refinery Managed Servers	14-8
Configuring the Inbound Refinery Managed Servers	14-9
Configuring Inbound Refinery Settings	14-9
Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion	14-12
Creating an Outgoing Provider	14-12
Enabling Components for Inbound Refinery on Content Server	14-13
Selecting File Formats To Be Converted	14-13
Validating the Configuration of the Inbound Refinery Managed Servers	14-14

15 Extending the Domain to Include Capture

Overview of Extending the Domain to Include Capture	15-1
Extending the Domain for Capture	15-1
Starting the Configuration Wizard	15-2
Navigating the Configuration Wizard Screens to Extend the Domain	15-2
Extending the Domain with Static Clusters	15-2
Extending the Domain with Dynamic Clusters	15-9
Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2	15-14
Configuring Oracle HTTP Server for the Capture Cluster	15-15
Configuring Oracle HTTP Server for the WLS_CPT Managed Servers	15-15
Setting the Front-End HTTP Host and Port for the Capture Cluster	15-16
Validating Access Through the Load Balancer	15-16

16 Extending the Domain to Include Imaging

Overview of Extending the Domain to Include Imaging	16-1
Extending the Domain for Imaging	16-1
Navigating the Configuration Wizard Screens to Extend the Domain	16-2
Extending the Domain with Static Clusters	16-2
Extending the Domain with Dynamic Clusters	16-8
Propagating the Domain Configuration to WLS_IPM1 and WLS_IPM2	16-14
Configuring Oracle HTTP Server for the Imaging Cluster	16-15
Configuring Oracle HTTP Server for the WLS_IPM Managed Servers	16-15

Setting the Front-End HTTP Host and Port for the Imaging Cluster	16-16
Validating Access Through the Load Balancer	16-16

17 Extending the Domain to Include WebCenter Content User Interface

Extending the Domain for WebCenter Content User Interface	17-1
Starting the Configuration Wizard	17-2
Navigating the Configuration Wizard Screens to Extend the Domain	17-2
Extending the Domain with Static Clusters	17-2
Extending the Domain with Dynamic Clusters	17-8
Propagating the Domain Configuration to WLS_WCCUI1 and WLS_WCCUI2	17-13
Modifying System-Level Settings Through MBeans	17-14
Configuring Oracle HTTP Server with the WebCenter Content User Interface Cluster	17-15
Configuring Oracle HTTP Server for the WLS_WCCUI Managed Servers	17-16
Setting the Front-End HTTP Host and Port for the WebCenter Content User Interface Cluster	17-16
Validating Access Through the Load Balancer	17-16
Completing the Workflow Configuration	17-17

Part IV Common Configuration and Management Procedures for an Enterprise Deployment

18 Common Configuration and Management Tasks for an Enterprise Deployment

Verifying Appropriate Sizing and Configuration for the WLSSchemaDataSource	18-2
Verifying Manual Failover of the Administration Server	18-2
Failing Over the Administration Server to a Different Host	18-3
Validating Access to the Administration Server on WCCHOST2 Through Oracle HTTP Server	18-5
Failing the Administration Server Back to WCCHOST1	18-5
Configuring Listen Addresses in Dynamic Cluster Server Templates	18-6
Configuring Server Template Listen Addresses Using the Machine Name	18-7
Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer	18-8
When is SSL Communication Between the Middle Tier and Load Balancer Necessary?	18-9
Generating Self-Signed Certificates Using the utils.CertGen Utility	18-9
Creating an Identity Keystore Using the utils.ImportPrivateKey Utility	18-10
Creating a Trust Keystore Using the Keytool Utility	18-12
Importing the Load Balancer Certificate into the Truststore	18-13

Adding the Updated Trust Store to the Oracle WebLogic Server Start Scripts	18-13
Configuring Node Manager to Use the Custom Keystores	18-14
Configuring WebLogic Servers to Use the Custom Keystores	18-15
Testing Composites Using SSL Endpoints	18-16
Configuring Roles for Administration of an Enterprise Deployment	18-17
Summary of Products with Specific Administration Roles	18-17
Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group	18-18
Using Persistent Stores for TLOGs and JMS in an Enterprise Deployment	18-18
Products and Components that use JMS Persistence Stores and TLOGs	18-19
JDBC Persistent Stores vs. File Persistent Stores	18-20
About JDBC Persistent Stores for JMS and TLOGs	18-20
Performance Considerations for TLOGs and JMS Persistent Stores	18-20
Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment	18-22
Recommendations for TLOGs and JMS Datasource Consolidation	18-23
Roadmap for Configuring a JDBC Persistent Store for TLOGs	18-23
Roadmap for Configuring a JDBC Persistent Store for JMS	18-24
Creating a User and Tablespace for TLOGs	18-24
Creating a User and Tablespace for JMS	18-24
Creating GridLink Data Sources for TLOGs and JMS Stores	18-25
Assigning the TLOGs JDBC Store to the Managed Servers	18-28
Creating a JDBC JMS Store	18-28
Assigning the JMS JDBC store to the JMS Servers	18-29
Creating the Required Tables for the JMS JDBC Store	18-29
Using File Persistent Stores for TLOGs and JMS in an Enterprise Deployment	18-30
Configuring TLOGs File Persistent Store in a Shared Folder	18-30
Configuring JMS File Persistent Store in a Shared Folder	18-33
Performing Backups and Recoveries for an Enterprise Deployment	18-33
Modifying the Upload and Stage Directories to an Absolute Path in an Enterprise Deployment	18-34
Starting and Stopping Servers in Dynamic Clusters	18-36
Expanding or Reducing Dynamic Clusters	18-36

19 Using Whole Server Migration and Service Migration in an Enterprise Deployment

About Whole Server Migration and Automatic Service Migration in an Enterprise Deployment	19-1
Understanding the Difference between Whole Server and Service Migration	19-1
Implications of Using Whole Server Migration or Service Migration in an Enterprise Deployment	19-2

Understanding Which Products and Components Require Whole Server Migration and Service Migration	19-3
Creating a GridLink Data Source for Leasing	19-3
Configuring Whole Server Migration for an Enterprise Deployment	19-6
Editing the Node Manager's Properties File to Enable Whole Server Migration	19-6
Setting Environment and Superuser Privileges for the wlsifconfig.sh Script	19-7
Setting the PATH Environment Variable for the wlsifconfig.sh Script	19-8
Granting Privileges to the wlsifconfig.sh Script	19-8
Configuring Server Migration Targets	19-8
Testing Whole Server Migration	19-9
Configuring Automatic Service Migration in an Enterprise Deployment	19-11
Setting the Leasing Mechanism and Data Source for an Enterprise Deployment Cluster	19-11
Changing the Migration Settings for the Managed Servers in the Cluster	19-12
About Selecting a Service Migration Policy	19-12
Setting the Service Migration Policy for Each Managed Server in the Cluster	19-13
Validating Automatic Service Migration in Static Clusters	19-14
Failing Back Services After Automatic Service Migration	19-15

20 Configuring Single Sign-On for an Enterprise Deployment

About Oracle HTTP Server Webgate	20-1
General Prerequisites for Configuring Oracle HTTP Server WebGate	20-2
Enterprise Deployment Prerequisites for Configuring OHS 12c Webgate	20-2
Configuring Oracle HTTP Server 12c WebGate for an Enterprise Deployment	20-3
Registering the Oracle HTTP Server WebGate with Oracle Access Manager	20-4
Locating and Preparing the RREG Tool	20-4
About RREG In-Band and Out-of-Band Mode	20-5
Updating the Standard Properties in the OAM11gRequest.xml File	20-6
Updating the Protected, Public, and Excluded Resources for an Enterprise Deployment	20-10
Running the RREG Tool	20-11
Running the RREG Tool in In-Band Mode	20-11
Running the RREG Tool in Out-Of-Band Mode	20-12
Files and Artifacts Generated by RREG	20-13
Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location	20-14
Insert OHS SimpleCA Certificate into the Wallet Artifact	20-15
Enable MD5 Certificate Signatures for the Oracle HTTP Server Instances	20-16
Restarting the Oracle HTTP Server Instance	20-17
Setting Up the WebLogic Server Authentication Providers	20-17
Backing Up Configuration Files	20-17

Setting Up the Oracle Access Manager Identity Assertion Provider	20-18
Updating the Default Authenticator and Setting the Order of Providers	20-18
Configuring Oracle ADF and OPSS Security with Oracle Access Manager	20-19

A Using Multi Data Sources with Oracle RAC

About Multi Data Sources and Oracle RAC	A-1
Typical Procedure for Configuring Multi Data Sources for an Enterprise Deployment	A-1

Preface

This guide explains how to install, configure, and manage a highly available Oracle Fusion Middleware enterprise deployment..

- [Audience](#)
- [Documentation Accessibility](#)
- [Conventions](#)

Audience

In general, this document is intended for administrators of Oracle Fusion Middleware, who are assigned the task of installing and configuring Oracle Fusion Middleware software for production deployments.

Specific tasks can also be assigned to specialized administrators, such as database administrators (DBAs) and network administrators, where applicable.

Documentation Accessibility

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

Access to Oracle Support

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

Conventions

The following text conventions are used in this document:

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

 Note:

This guide focuses on the implementation of the enterprise deployment reference topology on Oracle Linux systems.

The topology can be implemented on any certified, supported operating system, but the examples in this guide typically show the commands and configuration steps as they should be performed using the bash shell on Oracle Linux.

Part I

Understanding an Enterprise Deployment

It is important to understand the concept and general characteristics of a typical enterprise deployment, before you configure the Oracle WebCenter Content enterprise deployment topology.

This part of the Enterprise Deployment Guide contains the following topics.

- [Enterprise Deployment Overview](#)
The Enterprise Deployment Guide provides detailed, validated instructions that help you plan, prepare, install, and configure a multi-host, secure, highly available, production topology for selected Oracle Fusion Middleware products.
- [About a Typical Enterprise Deployment](#)
It is essential to understand the components of a typical enterprise deployment topology.
- [Understanding the WebCenter Content Enterprise Deployment Topology](#)
The Oracle WebCenter Content enterprise deployment topology represents a specific reference implementation of the concepts described in [Understanding a Typical Enterprise Deployment](#).

1

Enterprise Deployment Overview

The Enterprise Deployment Guide provides detailed, validated instructions that help you plan, prepare, install, and configure a multi-host, secure, highly available, production topology for selected Oracle Fusion Middleware products.

This chapter introduces the concept of an Oracle Fusion Middleware enterprise deployment. It also provides information on when to use the Enterprise Deployment guide.

- [About the Enterprise Deployment Guide](#)
An Enterprise Deployment Guide provides a comprehensive, scalable example for installing, configuring, and maintaining a secure, highly available, production-quality deployment of selected Oracle Fusion Middleware products. The resulting environment is known as an **enterprise deployment topology**.
- [When to Use the Enterprise Deployment Guide](#)
This guide describes one of the three primary installation and configuration options for Oracle Fusion Middleware. Use this guide to help you plan, prepare, install, and configure a multi-host, secure, highly available, production topology for selected Oracle Fusion Middleware products.

About the Enterprise Deployment Guide

An Enterprise Deployment Guide provides a comprehensive, scalable example for installing, configuring, and maintaining a secure, highly available, production-quality deployment of selected Oracle Fusion Middleware products. The resulting environment is known as an **enterprise deployment topology**.

For example, the enterprise deployment topology introduces key concepts and best practices that you can use to implement a similar Oracle Fusion Middleware environment for your organization.

Each Enterprise Deployment Guide provides detailed, validated instructions for implementing the reference topology. Along the way, the guide also offers links to supporting documentation that explains concepts, reference material, and additional options for an Oracle Fusion Middleware enterprise deployment.

Note that the enterprise deployment topologies described in the enterprise deployment guides cannot meet the exact requirements of all Oracle customers. In some cases, you can consider alternatives to specific procedures in this guide, depending on whether the variations to the topology are documented and supported by Oracle.

Oracle recommends customers use the Enterprise Deployment Guides as a first option for deployment. If variations are required, then those variations should be verified by reviewing the related Oracle documentation or by working with Oracle Support.

When to Use the Enterprise Deployment Guide

This guide describes one of the three primary installation and configuration options for Oracle Fusion Middleware. Use this guide to help you plan, prepare, install, and configure a multi-host, secure, highly available, production topology for selected Oracle Fusion Middleware products.

Alternatively, you can use the other primary installation and configuration options:

- Review *Planning an Installation of Oracle Fusion Middleware*, which provides additional information to help you prepare for any Oracle Fusion Middleware installation.

2

About a Typical Enterprise Deployment

It is essential to understand the components of a typical enterprise deployment topology.

This chapter provides information on the Enterprise Deployment Topology diagram.

- [Diagram of a Typical Enterprise Deployment](#)
This diagram shows all the components of a typical enterprise deployment, including the Web tier, Application tier, and Data tier. All enterprise deployments are based on these basic principles.
- [About the Typical Enterprise Deployment Topology Diagram](#)
A typical enterprise deployment topology consists of a Hardware Load Balancer (LBR), web tier, an application tier, and data tier. This section provides detailed information on these components.

Diagram of a Typical Enterprise Deployment

This diagram shows all the components of a typical enterprise deployment, including the Web tier, Application tier, and Data tier. All enterprise deployments are based on these basic principles.

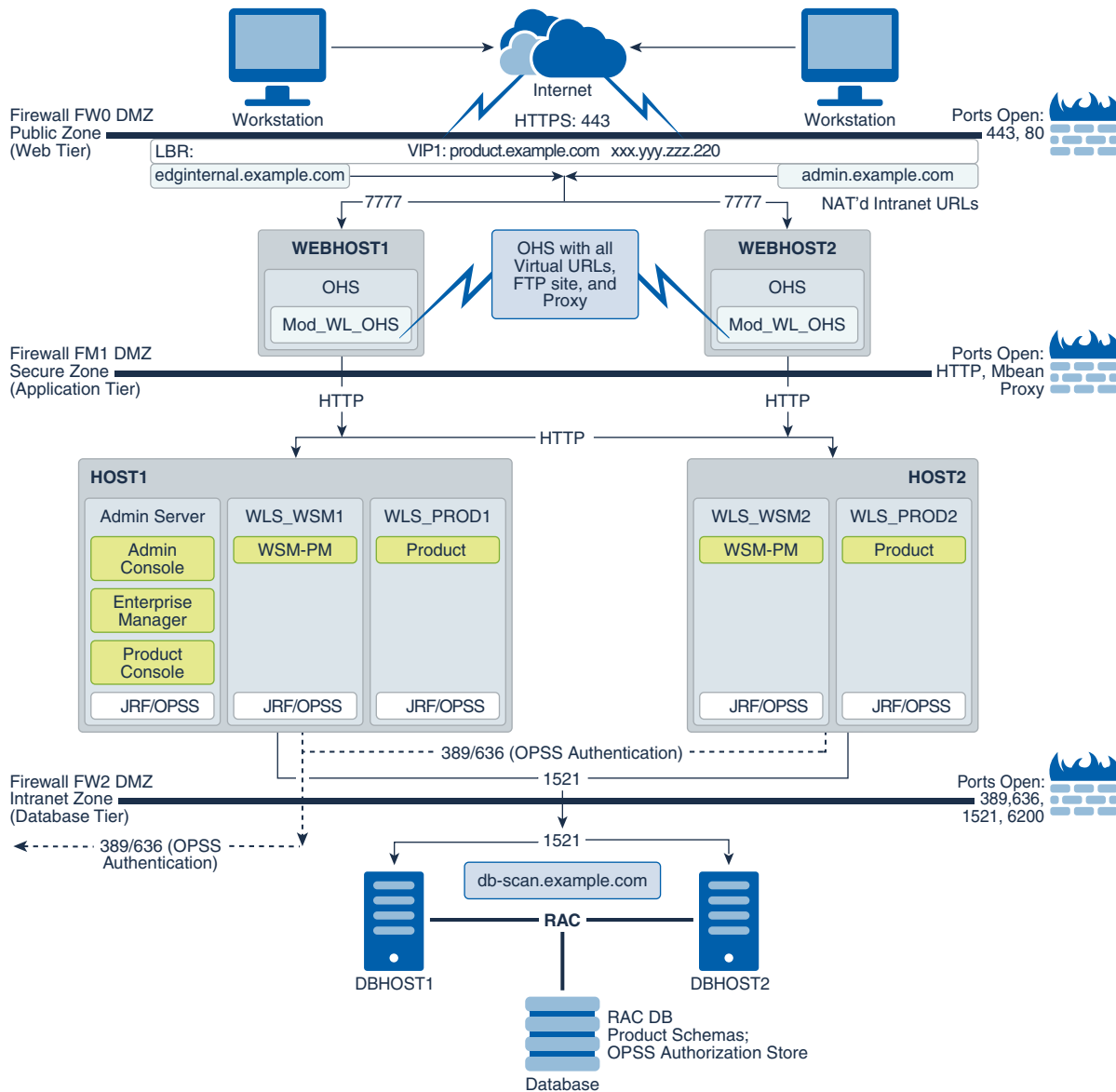
All Oracle Fusion Middleware enterprise deployments are designed to demonstrate the best practices for installing and configuring an Oracle Fusion Middleware production environment.

A best practices approach starts with the basic concept of a multi-tiered deployment and standard communications between the different software tiers.

[Figure 2-1](#) shows a typical enterprise deployment, including the Web tier, Application tier, and Data tier. All enterprise deployments are based on these basic principles.

For a description of each tier and the standard protocols used for communications within a typical Oracle Fusion Middleware enterprise deployment, see [About the typical Enterprise Deployment Topology Diagram](#).

Figure 2-1 Typical Enterprise Deployment Topology Diagram



About the Typical Enterprise Deployment Topology Diagram

A typical enterprise deployment topology consists of a Hardware Load Balancer (LBR), web tier, an application tier, and data tier. This section provides detailed information on these components.

- [Understanding the Firewalls and Zones of a Typical Enterprise Deployment](#)
- [Understanding the Elements of a Typical Enterprise Deployment Topology](#)
- [Receiving Requests Through Hardware Load Balancer](#)
- [Understanding the Web Tier](#)
- [Understanding the Application Tier](#)

- [About the Data Tier](#)

Understanding the Firewalls and Zones of a Typical Enterprise Deployment

The topology is divided into several security zones, which are separated by firewalls:

- The web tier (or DMZ), which is used for the hardware load balancer and Web servers (in this case, Oracle HTTP Server instances) that receive the initial requests from users. This zone is accessible only through a single virtual server name that is defined on the load balancer.
- The application tier, which is where the business and application logic resides.
- The data tier, which is not accessible from the Internet and reserved in this topology for the highly available database instances.

The firewalls are configured to allow data to be transferred only through specific communication ports. Those ports (or in some cases, the protocols that need open ports in the firewall) are shown on each firewall line in the diagram.

For example:

- On the firewall protecting the web tier, only the HTTP ports are open: 443 for HTTPS and 80 for HTTP.
- On the firewall protecting an application tier, HTTP ports, and MBean proxy port are open.

Applications that require external HTTP access can use the Oracle HTTP Server instances as a proxy. Note that this port for outbound communications only and the proxy capabilities on the Oracle HTTP Server must be enabled.

- On the firewall protecting the data tier, the database listener port (typically, 1521) must be open.

The LDAP ports (typically, 389 and 636) are also required to be open for communication between the authorization provider and the LDAP-based identity store.

The ONS port (typically, 6200) is also required so that the application tier can receive notifications about workload and events in the Oracle RAC Database. These events are used by the Oracle WebLogic Server connection pools to adjust quickly (creating or destroying connections), depending on the availability and workload on the Oracle RAC database instances.

For a complete list of the ports that you must open for a specific Oracle Fusion Middleware enterprise deployment topology, see the chapter that describes the topology that you want to implement, or refer to the *Enterprise Deployment Workbook* for the topology that you want to implement. See [Using the Enterprise Deployment Workbook](#).

Understanding the Elements of a Typical Enterprise Deployment Topology

The enterprise deployment topology consists of the following high-level elements:

- A hardware load balancer that routes requests from the Internet to the web servers in the web tier. It also routes requests from internal clients or other components that perform internal invocations within the corporate network.
- A web tier, consisting of a hardware load balancer and two or more physical computers that host the web server instances (for high availability).

The web server instances are configured to authenticate users (through an external identity store and a single sign-on server) and then route the HTTP requests to the Oracle Fusion Middleware products and components that are running in the Application tier.

The web server instances also host static web content that does not require the application logic to be delivered. Placing such content in the web tier reduces the overhead on the application servers and eliminates unnecessary network activity.

- An application tier, consisting of two or more physical computers that are hosting a cluster of Oracle WebLogic Server Managed Servers, and the Administration Server for the domain. The Managed Servers are configured to run the various Oracle Fusion Middleware products, such as Oracle SOA Suite, Oracle Service Bus, Oracle WebCenter Content, and Oracle WebCenter Portal, depending on your choice of products in the enterprise deployment.
- A data tier, consisting of two or more physical hosts that are hosting an Oracle RAC Database.

Receiving Requests Through Hardware Load Balancer

The following topics describe the hardware load balancer and its role in an enterprise deployment.

- [Purpose of the Hardware Load Balancer \(LBR\)](#)
- [Summary of the Typical Load Balancer Virtual Server Names](#)
- [HTTPS Versus HTTP Requests to the External Virtual Server Name](#)

Purpose of the Hardware Load Balancer (LBR)

There are two types of load balancers, Local Load Balancers and Global Load Balancers. Load balancers can either be hardware devices such as Big IP, Cisco, Brocade, and so on—or they can be software applications such as Oracle Traffic Director. Most load balancer appliances can be configured for both local and global load balancers.

Load balancers should always be deployed in pairs to ensure that no single load balancer is a single point of failure. Most load balancers do this in an active-passive way. You should consult your load balancer documentation on how best to achieve this.



Note:

Oracle does not certify against specific load balancers. The configuration information of load balancers given in the Enterprise Deployment guide are for guidance only and you should consult with your load balancer vendor about the best practices that are associated with the configuration of the device that you are using.

A local load balancer is used to distribute traffic within a site. It can distribute both HTTP and TCP traffic and the requirements of your deployment dictates which options you should use. Local load balancers often provide acceleration for SSL encryption and decryption as well as the ability to terminate or off-load SSL requests. SSL termination at the load balancer provides a significant performance gain to applications, ensuring that traffic to and from a site remains encrypted without the overhead of on the fly software encryption inside the deployment itself. Enterprise Deployment guide environments always utilize a local load balancer.

A global load balancer is used when you have multiple sites that need to function as the same logical environment. Its purpose is to distribute requests between the sites based on a pre-determined set of rules. Global load balancers are typically used in Disaster Recovery (DR) deployments or Active/Active Multi-Data Center (MDC) deployments.

The following topics describe the types of requests that are handled by the hardware load balancer in an Enterprise Deployment:

- [HTTP Requests From the Internet to the Web Server Instances in the Web Tier](#)
- [Specific Internal-Only Communications Between the Components of the Application Tier](#)
- [Load Balancer Considerations for Disaster Recovery and Multi-Data Center Topologies](#)

HTTP Requests From the Internet to the Web Server Instances in the Web Tier

The hardware load balancer balances the load on the web tier by receiving requests to a single virtual host name and then routing each request to one of the web server instances, based on a load balancing algorithm. In this way, the load balancer ensures that no one web server is overloaded with HTTP requests.

For more information about the purpose of specific virtual host names on the hardware load balancer, see [Summary of the Typical Load Balancer Virtual Server Names](#).

Note that in the reference topology, only HTTP requests are routed from the hardware load balancer to the web tier. Secure Socket Layer (SSL) requests are terminated at the load balancer and only HTTP requests are forwarded to the Oracle HTTP Server instances. This guide does not provide instructions for SSL configuration between the load balancer and the Oracle HTTP Server instances or between the web tier and the application tier.

The load balancer provides high availability by ensuring that if one web server goes down, requests are routed to the remaining web servers that are up and running.

Further, in a typical highly available configuration, the hardware load balancers are configured such that a hot standby device is ready to resume service in case a failure occurs in the main load balancing appliance. This is important because for many types of services and systems, the hardware load balancer becomes the unique point of access to make invocations and, as a result, becomes a single point of failure (SPOF) for the whole system if it is not protected.

Specific Internal-Only Communications Between the Components of the Application Tier

In addition, the hardware load balancer routes specific communications between the Oracle Fusion Middleware components and applications on the application tier. The

internal-only requests are also routed through the load balancer by using a unique virtual host name.

Load Balancer Considerations for Disaster Recovery and Multi-Data Center Topologies

In addition to the load-balancing features for local site traffic as described in the previous topics, many LBR also include features for configuring global load-balancing across multiple sites in DR or active/active MDC topologies.

A global load balancer configuration uses conditional DNS to direct traffic to local load balancers at different sites. A global load balancer for Oracle Fusion Middleware is typically configured for DR or MDC topologies:

- Active/Passive DR: Always send requests to site 1 unless site 1 is unavailable in which case send traffic to site 2.
- Active/Active MDC: Always send requests to both site 1 and site 2, often based on the geographic location of the source request in relation to the physical geographical location of the sites. Active/Active deployments are available only to those applications which support it.

For example:

Application entry point: `app.example.com`

Site 1 - Local Load Balancer Virtual Host: `site1app.example.com`

Site 2 - Local Load Balancer Virtual Host: `site2app.example.com`

When a request for `app.example.com` is received, the global load balancer would:

- If the topology is active/passive DR:
Change the IP address of `app.example.com` in DNS to resolve as the IP address of the local load balancer Virtual Host for the active site. For example: `site1app.example.com` (assuming that is the active site).
- If the topology is active/active MDC:
Change the IP address of `app.example.com` in DNS to resolve as either the IP address of `site1app.example.com` or `site2app.example.com` depending on which site is nearest to the client making the request.

For information on Disaster Recovery, see *Oracle Fusion Middleware Disaster Recovery Guide*.

For more information on Multi-Data Center topologies for various Fusion Middleware products, see the [MAA Best Practices for Fusion Middleware](#) page on the Oracle Technology Network website.

Summary of the Typical Load Balancer Virtual Server Names

In order to balance the load on servers and to provide high availability, the hardware load balancer is configured to recognize a set of virtual server names. By using the naming convention in [Figure 2-1](#), the following virtual server names are recognized by the hardware load balancer in this topology:

- `product.example.com`: This virtual server name is used for all incoming traffic.

Users enter this URL to access the Oracle Fusion Middleware product that you have deployed and the custom applications that are available on this server. The load balancer then routes these requests (by using a load balancing algorithm) to one of the servers in the web tier. In this way, the single virtual server name can be used to route traffic to multiple servers for load balancing and high availability of the web servers instances.

- `productinternal.example.com`: This virtual server name is for internal communications only.

The load balancer uses its **Network Address Translation (NAT)** capabilities to route any internal communication from the application tier components that are directed to this URL. This URL is not exposed to external customers or users on the Internet. Each product has specific uses for the internal URL, so in the deployment instructions, the virtual server name is prefixed with the product name.

- `admin.example.com`: This virtual server name is for administrators who need to access the Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server Administration Console interfaces.

This URL is known only to internal administrators. It also uses the NAT capabilities of the load balancer to route administrators to the active Administration Server in the domain.

For a complete set of virtual server names that you must define for your topology, see the chapter that describes the product-specific topology.

HTTPS Versus HTTP Requests to the External Virtual Server Name

Note that when you configure the hardware load balancer, a best practice is to assign the main external URL (for example, `http://myapplication.example.com`) to port 80 and port 443.

Any request on port 80 (non-SSL protocol) should be redirected to port 443 (SSL protocol). Exceptions to this rule include requests from public WSDLs. See [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Understanding the Web Tier

The Web tier of the reference topology consists of the Web servers that receive requests from the load balancer. In the typical enterprise deployment, at least two Oracle HTTP Server instances are configured in the Web tier. The following topics provide more detail.

- [Benefits of Using Oracle HTTP Server Instances to Route Requests](#)
- [Configuration of Oracle HTTP Server in the Web Tier](#)
- [About Mod_WL_OHS](#)

Benefits of Using Oracle HTTP Server Instances to Route Requests

A Web tier with Oracle HTTP Server is not a requirement for many of the Oracle Fusion Middleware products. You can route traffic directly from the hardware load balancer to the WLS servers in the Application Tier. However, a Web tier does provide several advantages, which is why it is recommended as part of the reference topology:

- The Web tier provides DMZ public zone, which is a common requirement in security audits. If a load balancer routes directly to the WebLogic Server, requests move from the load balancer to the application tier in one single HTTP jump, which can cause security concerns.
- The Web tier allows the WebLogic Server cluster membership to be reconfigured (new servers added, others removed) without having to change the Web server configuration (as long as at least some of the servers in the configured list remain alive).
- Oracle HTTP Server delivers static content more efficiently and faster than WebLogic Server; it also provides FTP services, which are required for some enterprise deployments, as well as the ability to create virtual hosts and proxies via the Oracle HTTP Server configuration files.
- Oracle HTTP Server provides HTTP redirection over and above what WebLogic Server provides. You can use Oracle HTTP Server as a front end against many different WebLogic Server clusters, and in some cases, control the routing via content based routing.
- Oracle HTTP Server provides the ability to integrate single sign-on capabilities into your enterprise deployment. For example, you can later implement single sign-on for the enterprise deployment, using Oracle Access Manager, which is part of the Oracle Identity and Access Management family of products.
- Oracle HTTP Server provides support for WebSocket connections deployed within WebLogic Server.

For more information about Oracle HTTP Server, see Introduction to Oracle HTTP Server in *Oracle Fusion Middleware Administering Oracle HTTP Server*.

Configuration of Oracle HTTP Server in the Web Tier

Starting with Oracle Fusion Middleware 12c, the Oracle HTTP Server software can be configured in one of two ways: as part of an existing Oracle WebLogic Server domain or in its own standalone domain. Each configuration offers specific benefits.

When you configure Oracle HTTP Server instances as part of an existing WebLogic Server domain, you can manage the Oracle HTTP Server instances, including the wiring of communications between the web servers and the Oracle WebLogic Server Managed Servers by using Oracle Enterprise Manager Fusion Middleware Control. When you configure Oracle HTTP Server in a standalone configuration, you can configure and manage the Oracle HTTP Server instances independently of the application tier domains.

For this enterprise deployment guide, the Oracle HTTP Server instances are configured as separate standalone domains, one on each Web tier host. You can choose to configure the Oracle HTTP Server instances as part of the application tier domain, but this enterprise deployment guide does not provide specific steps to configure the Oracle HTTP Server instances in that manner.

See About Oracle HTTP Server in *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.

About Mod_WL_OHS

As shown in the diagram, the Oracle HTTP Server instances use the WebLogic Proxy Plug-In (mod_wl_ohs) for proxying HTTP requests from Oracle HTTP Server to the Oracle WebLogic Server Managed Servers in the Application tier.

See What are Oracle WebLogic Server Proxy Plug-Ins? in *Oracle Fusion Middleware Using Oracle WebLogic Server Proxy Plug-Ins 12.2.1.1*.

Understanding the Application Tier

The application tier consists of two physical host computers, where Oracle WebLogic Server and the Oracle Fusion Middleware products are installed and configured. The application tier computers reside in the secured zone between firewall 1 and firewall 2.

The following topics provide more information:

- [Configuration of the Administration Server and Managed Servers Domain Directories](#)
- [About the Node Manager Configuration in a Typical Enterprise Deployment](#)
- [About Using Unicast for Communications within the Application Tier](#)
- [Understanding OPSS and Requests to the Authentication and Authorization Stores](#)

Configuration of the Administration Server and Managed Servers Domain Directories

Unlike the Managed Servers in the domain, the Administration Server uses an active-passive high availability configuration. This is because only one Administration Server can be running within an Oracle WebLogic Server domain.

In the topology diagrams, the Administration Server on HOST1 is in the active state and the Administration Server on HOST2 is in the passive (inactive) state.

To support the manual fail over of the Administration Server in the event of a system failure, the typical enterprise deployment topology includes:

- A Virtual IP Address (VIP) for the routing of Administration Server requests.
- The configuration of the Administration Server domain directory on a shared storage device.

In the event of a system failure (for example a failure of HOST1), you can manually reassign the Administration Server VIP address to another host in the domain, mount the Administration Server domain directory on the new host, and then start the Administration Server on the new host.

However, unlike the Administration Server, there is no benefit to storing the Managed Servers on shared storage. In fact, there is a potential performance impact when Managed Server configuration data is not stored on the local disk of the host computer.

As a result, in the typical enterprise deployment, after you configure the Administration Server domain on shared storage, a copy of the domain configuration is placed on the local storage device of each host computer, and the Managed Servers are started

from this copy of the domain configuration. You create this copy by using the Oracle WebLogic Server pack and unpack utilities.

The resulting configuration consists of separate domain directories on each host: one for the Administration Server (on shared storage) and one for the Managed Servers (on local storage). Depending upon the action required, you must perform configuration tasks from one domain directory or the other.

For more information about structure of the Administration Server domain directory and the Managed Server domain directory, as well as the variables used to reference these directories, see [Understanding the Recommended Directory Structure for an Enterprise Deployment](#).

There is an additional benefit to the multiple domain directory model. It allows you to isolate the Administration Server from the Managed Servers. By default, the primary enterprise deployment topology assumes the Administration Server domain directory is on one of the application tier hosts, but if necessary, you could isolate the Administration Server further by running it from its own host, for example in cases where the Administration Server is consuming high CPU or RAM. Some administrators prefer to configure the Administration Server on a separate, dedicated host, and the multiple domain directory model makes that possible.

About the Node Manager Configuration in a Typical Enterprise Deployment

Starting with Oracle Fusion Middleware 12c, you can use either a per domain Node Manager or a per host Node Manager. The following sections of this topic provide more information on the impact of the Node Manager configuration on a typical enterprise deployment.



Note:

For general information about these two types of Node Managers, see Overview in *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

About Using a Per Domain Node Manager Configuration

In a per domain Node Manager configuration—as opposed to a per host Node Manager configuration—you actually start two Node Manager instances on the Administration Server host: one from the Administration Server domain directory and one from the Managed Servers domain directory. In addition, a separate Node Manager instance runs on each of the other hosts in the topology.

The Node Manager that controls the Administration Server uses the listen address of the virtual host name created for the Administration Server. The Node Manager that controls the Managed Servers uses the listen address of the physical host. When the Administration Server fails over to another host, an additional instance of Node Manager is started to control the Administration Server on the failover host.

The key advantages of the per domain configuration are an easier and simpler initial setup of the Node Manager and the ability to set Node Manager properties that are unique to the Administration Server. This last feature was important in previous releases because some features, such as Crash Recovery, applied only to

the Administration Server and not to the Managed servers. In the current release, the Oracle SOA Suite products can be configured for Automated Service Migration, rather than Whole Server Migration. This means the Managed Servers, as well as the Administration Server, can take advantage of Crash Recovery, so there is no need to apply different properties to the Administration Server and Managed Server domain directories.

Another advantage is that the per domain Node Manager provides a default SSL configuration for Node Manager-to-Server communication, based on the Demo Identity store created for each domain.

About Using a Per Host Node Manager Configuration

In a per host Node Manager configuration, you start a single Node Manager instance to control the Administration Server and all Managed Servers on a host, even those that reside in different domains. This reduces the footprint and resource utilization on the Administration Server host, especially in those cases where multiple domains coexist on the same computer.

A per host Node Manager configuration allows all Node Managers to use a listen address of ANY, so they listen on all addresses available on the host. This means that when the Administration Server fails over to a new host, no additional configuration is necessary. The per host configuration allows for simpler maintenance, because you can update and maintain a single Node Manager properties file on each host, rather than multiple node manager property files.

The per host Node Manager configuration requires additional configuration steps. If you want SSL for Node Manager-to-Server communication, then you must configure an additional Identity and Trust store, and it also requires using Subject Alternate Names (SAN), because the Node Manager listens on multiple addresses. Note that SSL communications are typically not required for the application tier, because it is protected by two firewalls.

About Using Unicast for Communications within the Application Tier

Oracle recommends the unicast communication protocol for communication between the Managed Servers and hosts within the Oracle WebLogic Server clusters in an enterprise deployment. Unlike multicast communication, unicast does not require cross-network configuration and it reduces potential network errors that can occur from multicast address conflicts as well.

When you consider using the multicast or unicast protocol for your own deployment, consider the type of network, the number of members in the cluster, and the reliability requirements for cluster membership. Also consider the following features of each protocol.

Features of unicast in an enterprise deployment:

- Uses a group leader that every server sends messages directly to. This leader is responsible for retransmitting the message to every other group member and other group leaders, if applicable.
- Works out of the box in most network topologies
- Requires no additional configuration, regardless of the network topology.
- Uses a single missed heartbeat to remove a server from the cluster membership list.

Features of multicast in an enterprise deployment:

- Multicast uses a more scalable peer-to-peer model, where a server sends each message directly to the network once and the network makes sure that each cluster member receives the message directly from the network.
- Works out of the box in most modern environments, where the cluster members are in a single subnet.
- Requires additional configuration in the routers and WebLogic Server (that is, Multicast TTL) if the cluster members span more than one subnet.
- Uses three consecutive missed heartbeats to remove a server from the cluster membership list.

Depending on the number of servers in your cluster and on whether the cluster membership is critical for the underlying application (for example, in session-replication intensive applications or clusters with intensive RMI invocations across the cluster), each model may act better.

Consider whether your topology is going to be part of an active-active disaster recovery system or if the cluster is going to traverse multiple subnets. In general, unicast acts better in those cases.

For more information about multicast and unicast communication types, see the following resources:

- [Configuring Multicast Messaging for WebLogic Server Clusters in *Oracle Fusion Middleware High Availability Guide*](#)
- [One-to-Many Communication Using Unicast in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*](#)

Understanding OPSS and Requests to the Authentication and Authorization Stores

Many of the Oracle Fusion Middleware products and components require an Oracle Platform Security Services (OPSS) security store for authentication providers (an identity store), policies, credentials, keystores, and for audit data. As a result, communications must be enabled so the application tier can send requests to and from the security providers.

For authentication, this communication is to an LDAP directory, such as Oracle Internet Directory (OID) or Oracle Unified Directory (OUD), which typically communicates over port 389 or 636. When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Server Authentication provider. However, for an enterprise deployment, you must use a dedicated, centralized LDAP-compliant authentication provider.

For authorization (and the policy store), the location of the security store varies, depending upon the tier:

- For the application tier, the authorization store is database-based, so frequent connections from the Oracle WebLogic Server Managed Servers to the database are required for the purpose of retrieving the required OPSS data.
- For the web tier, the authorization store is file-based, so connections to the database are not required.

For more information about OPSS security stores, see the following sections of *Oracle Fusion Middleware Securing Applications with Oracle Platform Security Services*:

- Authentication Basics
- The Security Model

About the Data Tier

In the data tier, an Oracle RAC database runs on the two hosts (DBHOST1 and DBHOST2). The database contains the schemas required by the Oracle WebCenter Content components and the Oracle Platform Security Services (OPSS) policy store.

You can define multiple services for the different products and components in an enterprise deployment to isolate and prioritize throughput and performance accordingly. In this guide, one database service is used as an example. Furthermore, you can use other high availability database solutions to protect the database:

- Oracle Data Guard: See Introduction to Oracle Data Guard in *Oracle Data Guard Concepts and Administration*.
- Oracle RAC One Node: See Overview of Oracle RAC One Node in *Oracle Real Application Clusters Administration and Deployment Guide*.

These solutions above provide protection for the database beyond the information provided in this guide, which focuses on using an Oracle RAC Database, given the scalability and availability requirements that typically apply to an enterprise deployment.

For more information about using Oracle Databases in a high availability environment, see Database Considerations in *Oracle Fusion Middleware High Availability Guide*.

3

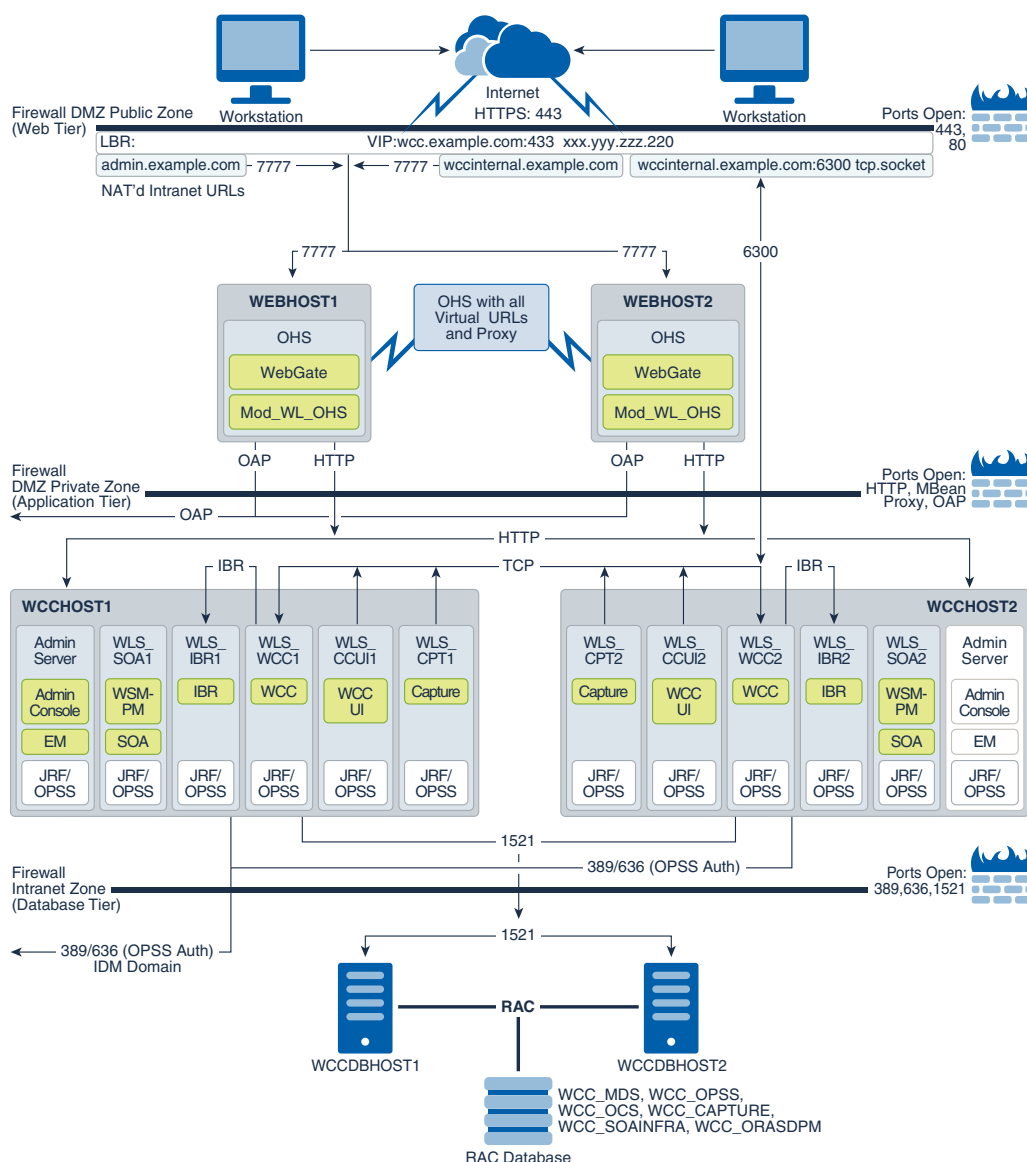
Understanding the WebCenter Content Enterprise Deployment Topology

The Oracle WebCenter Content enterprise deployment topology represents a specific reference implementation of the concepts described in [Understanding a Typical Enterprise Deployment](#).

- [Diagram of the WebCenter Content Enterprise Topology](#)
The below diagram shows the primary Oracle WebCenter Content enterprise deployment topologies.
- [Understanding the WebCenter Content Enterprise Topology Diagram](#)
Although most of the elements of Oracle WebCenter Content topology represent standard features of any enterprise topology, there are some elements that are unique to the WebCenter Content topology.
- [Flow Chart and Roadmap for Implementing the WebCenter Content Enterprise Topology](#)
It is essential to understand the steps that you need to perform to install and configure the WebCenter Content enterprise topology.

Diagram of the WebCenter Content Enterprise Topology

The below diagram shows the primary Oracle WebCenter Content enterprise deployment topologies.



Understanding the WebCenter Content Enterprise Topology Diagram

Although most of the elements of Oracle WebCenter Content topology represent standard features of any enterprise topology, there are some elements that are unique to the WebCenter Content topology.

Most of the elements of Oracle WebCenter Content topologies represent standard features of any enterprise topology that follows the Oracle-recommended best practices. These elements are described detail in [Understanding a Typical Enterprise Deployment](#).

Before you review the information in the following topics, it is assumed you have reviewed the information in [Understanding a Typical Enterprise Deployment](#) and that you are familiar with the general concepts of an enterprise deployment topology.

- [Summary of Oracle WebCenter Content Load Balancer Virtual Server Names](#)
- [Summary of the Managed Servers and Clusters on the WebCenter Content Application Tier](#)

Summary of Oracle WebCenter Content Load Balancer Virtual Server Names

In order to balance the load on servers and to provide high availability, the hardware load balancer is configured to recognize a set of virtual server names.

For information about the purpose of each of these server names, see [Summary of the Typical Load Balancer Virtual Server Names](#).

The following virtual server names are recognized by the hardware load balancer in Oracle WebCenter Content topologies:

- `wcc.example.com` - This virtual server name is used for all incoming traffic. It acts as the access point for all HTTP traffic to the runtime Oracle WebCenter Content components. The load balancer routes all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

`wcc.example.com:443`

- `wccinternal.example.com` - This virtual server name is for internal communications between the application tier components only and is not exposed to the Internet.

The traffic from clients to this URL is not SSL-enabled. Clients access this service using the following address and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

`wccinternal.example.com:80`

Note that this URL can also be set as the URL to be used for internal service invocations while modeling composites or at runtime with the appropriate Enterprise Manager MBeans.

This virtual server name also acts as the access point for all internal Remote Intradoc Client (RIDC) TCP traffic to the runtime Oracle WebCenter Content components. Applications like Imaging and Capture access this service using the address `ucminternal.example.com:6300` for RIDC connections, and the requests are forwarded to port 4444 on WCCHOST1 and WCCHOST2.

- `admin.example.com` - This virtual server name is for administrators who need to access the Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server Administration Console interfaces.

Information later in this guide provide instructions so you can:

- Configure the hardware load balancer to recognize and route requests to the virtual host names
- Configure the Oracle HTTP Server instances on the Web Tier to recognize and properly route requests to these virtual host names to the correct host computers.

Summary of the Managed Servers and Clusters on the WebCenter Content Application Tier

The Application tier hosts the Administration Server and Managed Servers in the Oracle WebLogic Server domain.

Depending upon the topology you select, the Oracle WebLogic Server domain for the Oracle WebCenter Content domain consists of the clusters shown in [Table 3-1](#). These clusters function as active-active high availability configurations.

Table 3-1 Summary of the Clusters in the Oracle WebCenter Content Enterprise Deployment Topology

Cluster	Managed Servers
Oracle WebCenter Content Cluster	WLS_WCC1, WLS_WCC2
Oracle SOA Suite Cluster	WLS_SOA1, WLS_SOA2
Oracle Inbound Refinery Cluster	WLS_IBR1, WLS_IBR2
Oracle WebCenter Enterprise Capture Cluster	WLS_CPT1, WLS_CPT2
WebCenter Content user interface Cluster	WLS_WCCUI1, WLS_WCCUI2

Flow Chart and Roadmap for Implementing the WebCenter Content Enterprise Topology

It is essential to understand the steps that you need to perform to install and configure the WebCenter Content enterprise topology.

- [Flow Chart of the Steps to Install and Configure the WebCenter Content Enterprise Topology](#)
- [Roadmap Table for Planning and Preparing for an Enterprise Deployment](#)
- [Roadmap Table for Configuring the Oracle WebCenter Content Topology](#)

Flow Chart of the Steps to Install and Configure the WebCenter Content Enterprise Topology

[Figure 3-1](#) shows a flow chart of the steps required to install and configure the primary enterprise deployment topologies described in this chapter. The sections following the flow chart explain each step in the flow chart.

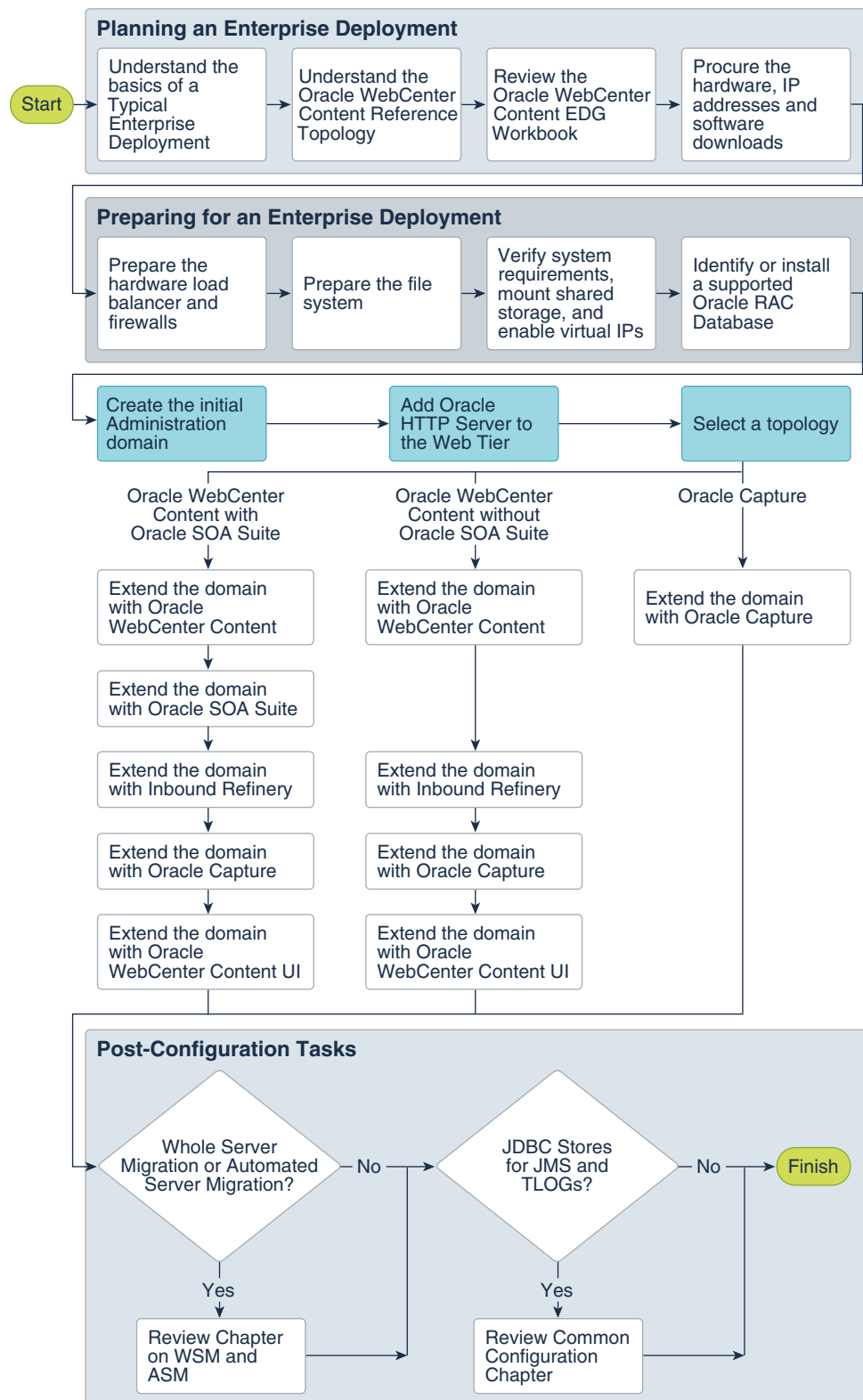
This guide is designed so you can start with a working WebCenter Content domain and then later extend the domain to add additional capabilities.

This modular approach to building the topology allows you to make strategic decisions, based on your hardware and software resources, as well as the Oracle WebCenter Content features that are most important to your organization.

It also allows you to validate and troubleshoot each individual product or component as they are configured.

This does not imply that configuring multiple products in one Configuration Wizard session is not supported; it is possible to group various extensions like the ones presented in this guide in one Configuration Wizard execution. However, the instructions in this guide focus primarily on the modular approach to building an enterprise deployment.

Figure 3-1 Flow Chart of the Enterprise Topology Configuration Steps



Roadmap Table for Planning and Preparing for an Enterprise Deployment

The following table describes each of the planning and preparing steps shown in the enterprise topology flow chart.

Flow Chart Step	More Information
Understand the basics of a Typical Enterprise Deployment	Understanding a Typical Enterprise Deployment
Understand the specific reference topology for the products that you plan to deploy	Review the product-specific topologies and the description of the topologies, including the virtual servers required and the summary of clusters and Managed Servers recommended for the product-specific deployment.
Review the Oracle WebCenter Content EDG Workbook	Using the Enterprise Deployment Workbook
Procure the hardware, IP addresses, and software downloads	Procuring Resources for an Enterprise Deployment
Prepare the hardware load balancer and firewalls	Preparing the Load Balancer and Firewalls for an Enterprise Deployment
Prepare the file system	Preparing the File System for an Enterprise Deployment
Verify system requirements, mount shared storage, and enable virtual IPs	Preparing the Host Computers for an Enterprise Deployment
Identify or install a supported Oracle RAC Database	Preparing the Database for an Enterprise Deployment

Roadmap Table for Configuring the Oracle WebCenter Content Topology

The following table describes each of the configuration steps required when configuring the topology shown in [Diagram of the WebCenter Content Enterprise Deployment Topology](#).

These steps correspond to the steps shown in the flow chart.

Flow Chart Step	More Information
Create the initial Infrastructure domain	Creating the Initial Infrastructure Domain for an Enterprise Deployment
Extend the domain to Include the Web Tier	Configuring the Web Tier for an Enterprise Deployment
Extend the domain with Oracle WebCenter Content	Extending the Domain to Include Oracle WebCenter Content
Extend the domain with Oracle SOA Suite	Extending the Domain with Oracle SOA Suite
Extend the domain with Inbound Refinery	Extending the Domain to Include Inbound Refinery
Extend the domain with Oracle WebCenter Enterprise Capture	Extending the Domain to Include Capture
Extend the domain with WebCenter Content user interface	Extending the Domain to Include WebCenter Content User Interface
Integrate the Enterprise Deployment with Oracle Identity Management	Configuring Single Sign-On for an Enterprise Deployment

Part II

Preparing for an Enterprise Deployment

It is important to understand the tasks that need to be performed to prepare for an enterprise deployment.

This part of the enterprise deployment guide contains the following topics.

- [Using the Enterprise Deployment Workbook](#)
The Enterprise Deployment workbook enables you to plan an enterprise deployment for your organization.
- [Procuring Resources for an Enterprise Deployment](#)
It is essential to procure the required hardware, software, and network settings before you configure the Oracle WebCenter Content reference topology.
- [Preparing the Load Balancer and Firewalls for an Enterprise Deployment](#)
It is important to understand how to configure the hardware load balancer and ports that must be opened on the firewalls for an enterprise deployment.
- [Preparing the File System for an Enterprise Deployment](#)
Preparing the file system for an enterprise deployment involves understanding the requirements for local and shared storage, as well as the terminology that is used to reference important directories and file locations during the installation and configuration of the enterprise topology.
- [Preparing the Host Computers for an Enterprise Deployment](#)
It is important to perform a set of tasks on each computer or server before you configure the enterprise deployment topology. This involves verifying the minimum hardware and operating system requirements for each host, configuring operating system users and groups, enabling Unicode support, mounting the required shared storage systems to the host and enabling the required virtual IP addresses on each host.
- [Preparing the Database for an Enterprise Deployment](#)
Preparing the database for an enterprise deployment involves ensuring that the database meets specific requirements, creating database services, using SecureFiles for large objects in the database, and creating database backup strategies.

4

Using the Enterprise Deployment Workbook

The Enterprise Deployment workbook enables you to plan an enterprise deployment for your organization.

This chapter provides an introduction to the Enterprise Deployment workbook, use cases, and information on who should use the Enterprise Deployment workbook.

- [Introduction to the Enterprise Deployment Workbook](#)
The Enterprise Deployment workbook is a spreadsheet that is used by architects, system engineers, database administrators, and others to plan and record all the details for an environment installation (such as server names, URLs, port numbers, installation paths, and other resources).
- [Typical Use Case for Using the Workbook](#)
It is important to understand the roles and tasks involved in a typical use case of the Enterprise Deployment workbook.
- [Using the Oracle WebCenter Content Enterprise Deployment Workbook](#)
Locating and understanding the Oracle WebCenter Content Enterprise Deployment workbook enables you to use it efficiently.
- [Who Should Use the Enterprise Deployment Workbook?](#)
The details of the Enterprise Deployment workbook are filled in by the individual or a team that is responsible for planning, procuring, or setting up each category of resources.

Introduction to the Enterprise Deployment Workbook

The Enterprise Deployment workbook is a spreadsheet that is used by architects, system engineers, database administrators, and others to plan and record all the details for an environment installation (such as server names, URLs, port numbers, installation paths, and other resources).

The Enterprise Deployment workbook serves as a single document that you can use to track input variables for the entire process, allowing for:

- Separation of tasks between architects, system engineers, database administrators, and other key organizational roles.
- Comprehensive planning before the implementation.
- Validation of planned decisions before the actual implementation.
- Consistency during implementation.
- A record of the environment for future use.

Typical Use Case for Using the Workbook

It is important to understand the roles and tasks involved in a typical use case of the Enterprise Deployment workbook.

A typical use case for the Enterprise Deployment workbook involves the following roles and tasks, in preparation for an Oracle Fusion Middleware Enterprise Deployment:

- Architects read through the first five chapters of this guide, and fill in the corresponding sections of the workbook.
- The workbook is validated by other architects and system engineers.
- The architect uses the validated workbook to initiate network and system change requests with the system engineering departments.
- The Administrators and System Integrators who install and configure the software refer to the workbook and the subsequent chapters of this guide to perform the installation and configuration tasks.

Using the Oracle WebCenter Content Enterprise Deployment Workbook

Locating and understanding the Oracle WebCenter Content Enterprise Deployment workbook enables you to use it efficiently.

The following sections provide an introduction to the location and contents of the Oracle WebCenter Content Enterprise Deployment workbook:

- [Locating the Oracle WebCenter Content Enterprise Deployment Workbook](#)
- [Understanding the Contents of the Oracle WebCenter Content Enterprise Deployment Workbook](#)

Locating the Oracle WebCenter Content Enterprise Deployment Workbook

The Oracle WebCenter Content Enterprise Deployment workbook is available as a Microsoft Excel spreadsheet in the Oracle Fusion Middleware documentation library. It is available as a link on the Install, Patch, and Upgrade page of the library.

Understanding the Contents of the Oracle WebCenter Content Enterprise Deployment Workbook

The following sections describe the contents of the Oracle WebCenter Content Enterprise Deployment workbook. The workbook is divided into tabs, each containing a set of related variables and values that you need to install and configure the Enterprise Deployment topologies.

- [Using the Start Tab](#)
- [Using the Hardware - Host Computers Tab](#)
- [Using the Network - Virtual Hosts & Ports Tab](#)

- [Using the Storage - Directory Variables Tab](#)
- [Using the Database - Connection Details Tab](#)

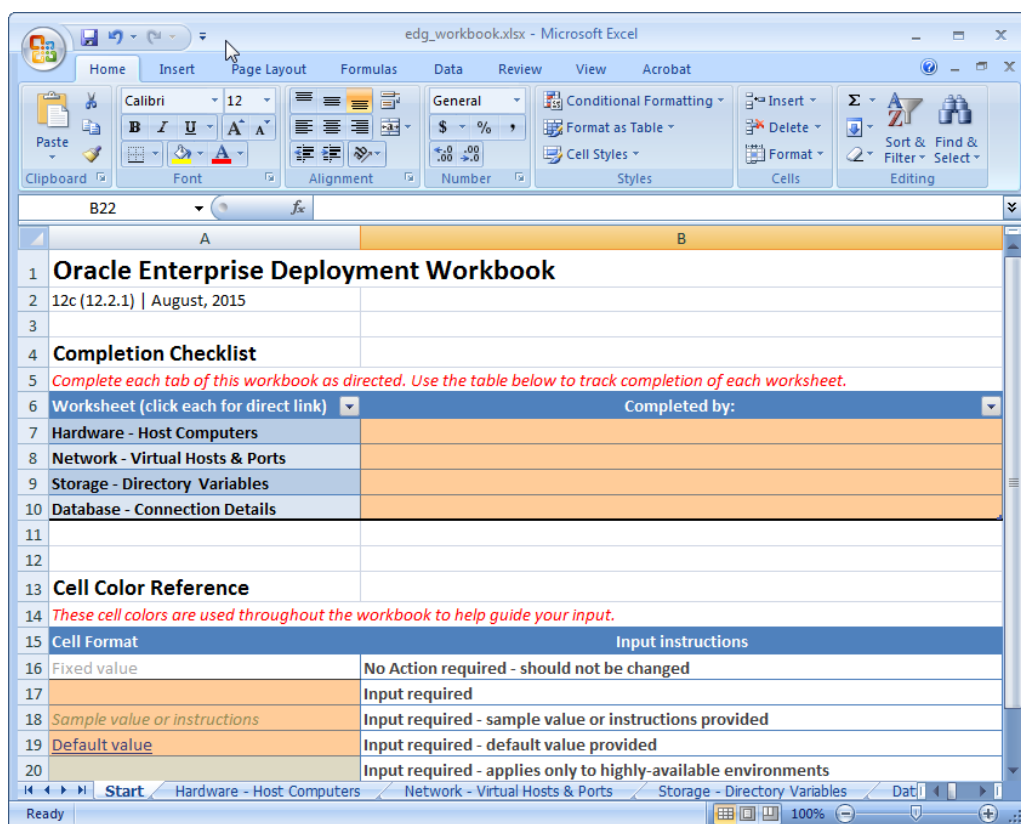
Using the Start Tab

The Start tab of the Enterprise Deployment workbook serves as a table of contents for the rest of the workbook. You can also use it to identify the people who will be completing the spreadsheet.

The Start tab also provides a key to identify the colors used to identify workbook fields that need values, as well as those that are provided for informational purposes.

The following image shows the Start tab of the Enterprise Deployment workbook.

Figure 4-1 Start Tab of the Enterprise Deployment workbook



Using the Hardware - Host Computers Tab

The Hardware - Host Computers tab lists the host computers that are required to install and configure the Oracle WebCenter Content Enterprise Deployment topology.

The reference topologies typically require a minimum of six host computers: two for the web tier, two for the application tier, and two for the Oracle RAC database on the data tier. If you decide to expand the environment to include more systems, add a row for each additional host computer.

The **Abstract Host Name** is the name used throughout this guide to reference the host. For each row, procure a host computer, and enter the **Actual Host Name**. You can then use the actual host name when any of the abstract names is referenced in this guide.

For example, if a procedure in this guide references WCCHOST1, you can then replace the WCCHOST1 variable with the actual name provided on the Hardware - Host Computers tab of the workbook.

**Note:**

If two domains share the same node, for example, if you set up the Oracle SOA suite, and then create MFT with its own domain, you have two domains on the same node. In this case, you use WCCHOST1 and MFTHOST1 at the same time, one for each domain.

For easy reference, Oracle also recommends that you include the IP address, Operating System (including the version), number of CPUs, and the amount of RAM for each host. This information can be useful during the installation, configuration, and maintenance of the enterprise deployment. See [Preparing the Host Computers for an Enterprise Deployment](#).

Using the Network - Virtual Hosts & Ports Tab

The Network - Virtual Hosts & Ports tab lists the virtual hosts that must be defined by your network administrator before you can install and configure the enterprise deployment topology.

The port numbers are important for several reasons. You must have quick reference to the port numbers so that you can access the management consoles; the firewalls must also be configured to allow network traffic through specific ports.

Each virtual host, virtual IP address, and each network port serves a distinct purpose in the deployment. See [Preparing the Load Balancer and Firewalls for an Enterprise Deployment](#).

In the Network - Virtual Hosts table, review the items in the **Abstract Virtual Host or Virtual IP Name** column. These are the virtual host and virtual IP names that are used in the procedures in this guide. For each abstract name, enter the actual virtual host name that is defined by your network administrator. Whenever this guide references one of the abstract virtual host or virtual IP names, replace that value with the actual corresponding value in this table.

Similarly, in many cases, this guide assumes that you are using default port numbers for the components or products you install and configure. However, in reality, you are likely to use different port numbers. Use the Network - Port Numbers table to map the default port values to the actual values that are used in your specific installation.

Using the Storage - Directory Variables Tab

As part of preparing for an enterprise deployment, it is assumed you are using a standard directory structure, which is recommended for Oracle enterprise deployments.

In addition, procedures in this book reference specific directory locations. Within the procedures, each directory is assigned a consistent variable, which you should replace with the actual location of the directory in your installation.

For each of the directory locations listed on this tab, provide the actual directory path in your installation.

In addition, for the application tier, it is recommended that many of these standard directories be created on a shared storage device. For those directories, the table also provides fields so you can enter the name of the shared storage location and the mount point that is used when you mounted the shared location. See [Preparing the File System for an Enterprise Deployment](#).

Using the Database - Connection Details Tab

When you install and configure the enterprise deployment topology, you often have to make connections to a highly available Oracle Real Application Clusters (RAC) database. In this guide, the procedures reference a set of variables that identify the information you need to provide to connect to the database from tools, such as the Configuration Wizard and the Repository Creation Utility.

To be sure that you have these values handy, use this tab to enter the actual values for these variables in your database installation. See [Preparing the Database for an Enterprise Deployment](#).

Who Should Use the Enterprise Deployment Workbook?

The details of the Enterprise Deployment workbook are filled in by the individual or a team that is responsible for planning, procuring, or setting up each category of resources.

The information in the Enterprise Deployment workbook is divided into categories. Depending on the structure of your organization and roles that are defined for your team, you can assign specific individuals in your organization to fill in the details of the workbook. Similarly, the information in each category can be assigned to the individual or team that is responsible for planning, procuring, or setting up each category of resources.

For example, the workbook can be filled in, reviewed, and used by people in your organization that fill the following roles:

- Information Technology (IT) Director
- Architect
- System Administrator
- Network Engineer
- Database Administrator

5

Procuring Resources for an Enterprise Deployment

It is essential to procure the required hardware, software, and network settings before you configure the Oracle WebCenter Content reference topology.

This chapter provides information on how to reserve the required IP addresses and identify and obtain software downloads for an enterprise deployment.

- [Hardware and Software Requirements for the Enterprise Deployment Topology](#)
It is important to understand the hardware load balancer requirements, host computer hardware requirements, and operating system requirements for the enterprise deployment topology.
- [Reserving the Required IP Addresses for an Enterprise Deployment](#)
You have to obtain and reserve a set of IP addresses before you install and configure the enterprise topology. The set of IP addresses that need to be reserved are listed in this section.
- [Identifying and Obtaining Software Distributions for an Enterprise Deployment](#)
Before you begin to install and configure the enterprise topology, you must obtain the software distributions that you need to implement the topology.

Hardware and Software Requirements for the Enterprise Deployment Topology

It is important to understand the hardware load balancer requirements, host computer hardware requirements, and operating system requirements for the enterprise deployment topology.

This section includes the following sections.

- [Hardware Load Balancer Requirements](#)
The section lists the wanted features of the external load balancer.
- [Host Computer Hardware Requirements](#)
This section provides information to help you procure host computers that are configured to support the enterprise deployment topologies.
- [Operating System Requirements for an Enterprise Deployment Topology](#)
This section provides details about the operating system requirements.

Hardware Load Balancer Requirements

The section lists the wanted features of the external load balancer.

The enterprise topology uses an external load balancer. The features of the external load balancer are:

- Ability to load-balance traffic to a pool of real servers through a virtual host name: Clients access services by using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.
- Port translation configuration should be possible so that incoming requests on the virtual host name and port are directed to a different port on the backend servers.
- Monitoring of ports on the servers in the pool to determine availability of a service.
- Ability to configure names and ports on your external load balancer. The virtual server names and ports must meet the following requirements:
 - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle HTTP Server in the web tier, the load balancer needs to be configured with a virtual server and ports for HTTP and HTTPS traffic.
 - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the backend services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.
- Ability to maintain sticky connections to components. Examples of this include cookie-based persistence, IP-based persistence, and so on.
- The load balancer should be able to terminate SSL requests at the load balancer and forward traffic to the backend real servers by using the equivalent non-SSL protocol (for example, HTTPS to HTTP).
- SSL acceleration (this feature is recommended, but not required for the enterprise topology).
- The ability to route TCP/IP requests; this is a requirement for Oracle SOA Suite for healthcare integration, which uses the Minimum Lower Layer Protocol (MLLP) over TCP.

Host Computer Hardware Requirements

This section provides information to help you procure host computers that are configured to support the enterprise deployment topologies.

It includes the following topics.

- [General Considerations for Enterprise Deployment Host Computers](#)
This section specifies the general considerations that are required for the enterprise deployment host computers.
- [Reviewing the Oracle Fusion Middleware System Requirements](#)
This section provides reference to the system requirements information to help you ensure that the environment meets the necessary minimum requirements.

- [Typical Memory, File Descriptors, and Processes Required for an Enterprise Deployment](#)
This section specifies the typical memory, number of file descriptors, and operating system processes and tasks details required for an enterprise deployment.
- [Typical Disk Space Requirements for an Enterprise Deployment](#)
This section specifies the disk space that is typically required for this enterprise deployment.

General Considerations for Enterprise Deployment Host Computers

This section specifies the general considerations that are required for the enterprise deployment host computers.

Before you start the process of configuring an Oracle Fusion Middleware enterprise deployment, you must perform the appropriate capacity planning to determine the number of nodes, CPUs, and memory requirements for each node depending on the specific system's load as well as the throughput and response requirements. These requirements vary for each application or custom Oracle WebCenter Content system being used.

The information in this chapter provides general guidelines and information that helps you determine the host computer requirements. It does not replace the need to perform capacity planning for your specific production environment.

Note:

As you obtain and reserve the host computers in this section, note the host names and system characteristics in the Enterprise Deployment workbook. You will use these addresses later when you enable the IP addresses on each host computer. See [Using the Enterprise Deployment Workbook](#).

Reviewing the Oracle Fusion Middleware System Requirements

This section provides reference to the system requirements information to help you ensure that the environment meets the necessary minimum requirements.

Review the [Oracle Fusion Middleware System Requirements and Specifications](#) to ensure that your environment meets the minimum installation requirements for the products that you are installing.

The Requirements and Specifications document contains information about general Oracle Fusion Middleware hardware and software requirements, minimum disk space and memory requirements, database schema requirements, and the required operating system libraries and packages.

It also provides some general guidelines for estimating the memory requirements for your Oracle Fusion Middleware deployment.

Typical Memory, File Descriptors, and Processes Required for an Enterprise Deployment

This section specifies the typical memory, number of file descriptors, and operating system processes and tasks details required for an enterprise deployment.

The following table summarizes the memory, file descriptors, and processes required for the Administration Server and each of the Managed Servers computers in a typical Oracle WebCenter Content enterprise deployment. These values are provided as an example only, but they can be used to estimate the minimum amount of memory required for an initial enterprise deployment.

The example in this topic reflects the minimum requirements for configuring the Managed Servers and other services required on WCCHOST1, as depicted in the reference topologies.

When you are procuring machines, use the information in the **Approximate Top Memory** column as a guide when determining the minimum physical memory each host computer should have available.

After you procure the host computer hardware and verify the operating system requirements, review the software configuration to be sure the operating system settings are configured to accommodate the number of open files listed in the **File Descriptors** column and the number processes listed in the **Operating System Processes and Tasks** column. See [Setting the Open File Limit and Number of Processes Settings on UNIX Systems](#).

Managed Server, Utility, or Service	Approximate Top Memory	Number of File Descriptors	Operating System Processes and Tasks
Administration Server	3.5 GB	3500	165
WLS_WCC	4.0 GB	3100	240
WLS_WCCUI	4.0 GB	3100	100
WLS_CPT	3.0 GB	1300	100
WLS_IBR	3.0 GB	1300	100
WLS_SOA	4.0 GB	3100	240
WLST (connection to the Node Manager)	1.5 GB	910	20
Configuration Wizard	1.5 GB	700	20
Node Manager	1.0 GB	720	15
TOTAL	11.5 GB*	TBD	TBD

* Approximate total, with consideration for Operating System and other additional memory requirements.

Typical Disk Space Requirements for an Enterprise Deployment

This section specifies the disk space that is typically required for this enterprise deployment.

For the latest disk space requirements for the Oracle Fusion Middleware 12c (12.2.1.3.0) products, including the Oracle WebCenter Content products, review the [Oracle Fusion Middleware System Requirements and Specifications](#).

In addition, the following table summarizes the disk space that is typically required for an Oracle WebCenter Content enterprise deployment.

Use the this information and the information in [Preparing the File System for an Enterprise Deployment](#) to determine the disk space requirements required for your deployment.

Server	Disk
Database	nXm n = number of disks, at least 4 (striped as one disk) m = size of the disk (minimum of 30 GB)
WEBHOSTn	10 GB
WCCHOSTn	20 GB*

* For a shared storage Oracle home configuration, two installations suffice by making a total of 20 GB.

Operating System Requirements for an Enterprise Deployment Topology

This section provides details about the operating system requirements.

The Oracle Fusion Middleware software products and components that are described in this guide are certified on various operating systems and platforms, which are listed in *Oracle Fusion Middleware System Requirements and Specifications*.

Note:

This guide focuses on the implementation of the enterprise deployment reference topology on Oracle Linux systems.

The topology can be implemented on any certified, supported operating system, but the examples in this guide typically show the commands and configuration steps as they should be performed by using the bash shell on Oracle Linux.

Reserving the Required IP Addresses for an Enterprise Deployment

You have to obtain and reserve a set of IP addresses before you install and configure the enterprise topology. The set of IP addresses that need to be reserved are listed in this section.

Before you begin installing and configuring the enterprise topology, you must obtain and reserve a set of IP addresses:

- Physical IP (IP) addresses for each of the host computers that you have procured for the topology
- A virtual IP (VIP) address for the Administration Server
- Additional VIP addresses for each Managed Server that is configured for Whole Server Migration

For Fusion Middleware 12c products that support Automatic Service Migration, VIPs for the Managed Servers are typically not necessary.

- A unique virtual host name to be mapped to each VIP.

You can then work with your network administrator to be sure that these required VIPs are defined in your DNS server. Alternatively, for non-production environments, you can use the `/etc/hosts` file to define these virtual hosts.

For more information, see the following topics.

- [What is a Virtual IP \(VIP\) Address?](#)
This section defines the virtual IP address and specifies its purpose.
- [Why Use Virtual Host Names and Virtual IP Addresses?](#)
For an enterprise deployment, in particular, it is important that a set of VIPs--and the virtual host names to which they are mapped--are reserved and enabled on the corporate network.
- [Physical and Virtual IP Addresses Required by the Enterprise Topology](#)
This section describes the physical IP (IP) and virtual IP (VIP) addresses that are required for the Administration Server and each of the Managed Servers in a typical Oracle WebCenter Content enterprise deployment topology.

What is a Virtual IP (VIP) Address?

This section defines the virtual IP address and specifies its purpose.

A virtual IP address is an unused IP Address that belongs to the same subnet as the host's primary IP address. It is assigned to a host manually. If a host computer fails, the virtual address can be assigned to a new host in the topology. For the purposes of this guide, *virtual* IP addresses are referenced, which can be reassigned from one host to another, and *physical* IP addresses are referenced, which are assigned permanently to hardware host computer.

Why Use Virtual Host Names and Virtual IP Addresses?

For an enterprise deployment, in particular, it is important that a set of VIPs--and the virtual host names to which they are mapped--are reserved and enabled on the corporate network.

Alternatively, host names can be resolved through appropriate `/etc/hosts` file propagated through the different nodes.

In the event of the failure of the host computer where the IP address is assigned, the IP address can be assigned to another host in the same subnet, so that the new host can take responsibility for running the Managed Servers that are assigned to it.

The reassignment of virtual IP address for the Administration Server must be performed manually, but the reassignment of virtual IP addresses for Managed Servers can be performed automatically by using the Whole Server Migration feature of Oracle WebLogic Server.

Whether you should use Whole Server Migration or not depends upon the products that you are deploying and whether they support Automatic Service Migration.

Physical and Virtual IP Addresses Required by the Enterprise Topology

This section describes the physical IP (IP) and virtual IP (VIP) addresses that are required for the Administration Server and each of the Managed Servers in a typical Oracle WebCenter Content enterprise deployment topology.

Before you begin to install and configure the enterprise deployment, reserve a set of host names and IP addresses that correspond to the VIPs in [Table 5-1](#).

You can assign any unique host name to the VIPs, but in this guide, each VIP is referenced by using the suggested host names in the table.

Note:

As you obtain and reserve the IP addresses and their corresponding virtual host names in this section, note the values of the IP addresses and host names in the Enterprise Deployment workbook. You will use these addresses later when you enable the IP addresses on each host computer. See [Using the Enterprise Deployment Workbook](#).

Table 5-1 Summary of the Virtual IP Addresses Required for the Enterprise Deployment

Virtual IP	VIP Maps to...	Description
VIP1	ADMINVHN	ADMINVHN is the virtual host name used as the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running.

Identifying and Obtaining Software Distributions for an Enterprise Deployment

Before you begin to install and configure the enterprise topology, you must obtain the software distributions that you need to implement the topology.

The following table lists the distributions used in this guide.

For general information about how to obtain Oracle Fusion Middleware software, see *Obtaining Product Distributions* in *Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware*.

For more specific information about locating and downloading specific Oracle Fusion Middleware products, see the *Oracle Fusion Middleware Download, Installation, and Configuration Readme Files* on OTN.



Note:

The information in this guide is meant to complement the information contained in the [Oracle Fusion Middleware certification matrixes](#). If there is a conflict of information between this guide and the certification matrixes, then the information in the certification matrixes must be considered the correct version, as they are frequently updated.

Distribution	Description
Oracle Fusion Middleware 12c (12.2.1.3.0) Infrastructure	Download this distribution to install the Oracle Fusion Middleware Infrastructure, which includes Oracle WebLogic Server and Java Required Files software required for Oracle Fusion Middleware products. This distribution also installs the Repository Creation Utility (RCU), which in previous Oracle Fusion Middleware releases was packaged in its own distribution.
Oracle HTTP Server 12c (12.2.1.3.0)	Download this distribution to install the Oracle HTTP Server software on the Web Tier.
Oracle Fusion Middleware 12c (12.2.1.3.0) WebCenter Content	Download this distribution to install the Oracle WebCenter Content.

Distribution	Description
Oracle Fusion Middleware 12c (12.2.1.3.0) SOA Suite	Download this distribution if you plan to install and configure Oracle SOA Suite as part of the Oracle WebCenter Content enterprise topology.

6

Preparing the Load Balancer and Firewalls for an Enterprise Deployment

It is important to understand how to configure the hardware load balancer and ports that must be opened on the firewalls for an enterprise deployment.

- [Configuring Virtual Hosts on the Hardware Load Balancer](#)
The hardware load balancer configuration facilitates to recognize and route requests to several virtual servers and associated ports for different types of network traffic and monitoring.
- [Configuring the Firewalls and Ports for an Enterprise Deployment](#)
As an administrator, it is important that you become familiar with the port numbers used by various Oracle Fusion Middleware products and services. This ensures that the same port number is not used by two services on the same host, and that the proper ports are open on the firewalls in the enterprise topology.

Configuring Virtual Hosts on the Hardware Load Balancer

The hardware load balancer configuration facilitates to recognize and route requests to several virtual servers and associated ports for different types of network traffic and monitoring.

The following topics explain how to configure the hardware load balancer, provide a summary of the virtual servers that are required, and provide additional instructions for these virtual servers:

- [Overview of the Hardware Load Balancer Configuration](#)
- [Typical Procedure for Configuring the Hardware Load Balancer](#)
- [Summary of the Virtual Servers Required for an Enterprise Deployment](#)
- [Additional Instructions for admin.example.com](#)
- [Additional Instructions for wcc.example.com](#)
- [Additional Instructions for wccinternal.example.com](#)

Overview of the Hardware Load Balancer Configuration

As shown in the topology diagrams, you must configure the hardware load balancer to recognize and route requests to several virtual servers and associated ports for different types of network traffic and monitoring.

In the context of a load-balancing device, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. It is typically represented by an IP address and a service, and it is used to distribute incoming client requests to the servers in the server pool.

The virtual servers should be configured to direct traffic to the appropriate host computers and ports for the various services that are available in the enterprise deployment.

In addition, you should configure the load balancer to monitor the host computers and ports for availability so that the traffic to a particular server is stopped as soon as possible when a service is down. This ensures that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

Note that after you configure the load balancer, you can later configure the web server instances in the web tier to recognize a set of virtual hosts that use the same names as the virtual servers that you defined for the load balancer. For each request coming from the hardware load balancer, the web server can then route the request appropriately, based on the server name included in the header of the request. See [Configuring Oracle HTTP Server for Administration and Oracle Web Services Manager](#).

Typical Procedure for Configuring the Hardware Load Balancer

The following procedure outlines the typical steps for configuring a hardware load balancer for an enterprise deployment.

Note that the actual procedures for configuring a specific load balancer will differ, depending on the specific type of load balancer. There may also be some differences depending on the type of protocol that is being load balanced. For example, TCP virtual servers and HTTP virtual servers use different types of monitors for their pools. Refer to the vendor-supplied documentation for actual steps.

1. Create a pool of servers. This pool contains a list of servers and the ports that are included in the load-balancing definition.

For example, for load balancing between the web hosts, create a pool of servers that would direct requests to hosts WEBHOST1 and WEBHOST2 on port 7777.
2. Create rules to determine whether a given host and service is available and assign it to the pool of servers that are described in Step 1.
3. Create the required virtual servers on the load balancer for the addresses and ports that receive requests for the applications.

For a complete list of the virtual servers required for the enterprise deployment, see [Summary of the Virtual Servers Required for an Enterprise Deployment](#).

When you define each virtual server on the load balancer, consider the following:

- a. If your load balancer supports it, specify whether the virtual server is available internally, externally, or both. Ensure that internal addresses are only resolvable from inside the network.
- b. Configure SSL Termination, if applicable, for the virtual server.
- c. Assign the pool of servers created in Step 1 to the virtual server.

Summary of the Virtual Servers Required for an Enterprise Deployment

This topic provides details of the virtual servers that are required for an enterprise deployment.

The following table provides a list of the virtual servers that you must define on the hardware load balancer for the Oracle WebCenter Content enterprise topology:

Virtual Host	Server Pool	Protocol	SSL Termination?	External?
admin.example.com:80	WEBHOST1.example.com:7777 WEBHOST2.example.com:7777	HTTP	No	No
wcc.example.com:443	WEBHOST1.example.com:7777 WEBHOST2.example.com:7777	HTTPS	Yes	Yes
wccinternal.example.com:800	WEBHOST1.example.com:7777 WEBHOST2.example.com:7777	HTTP	No	No
wccinternal.example.com:6300	WCCHOST1.example.com:4444 WCCHOST2.example.com:4444	TCP	No	No

Additional Instructions for admin.example.com

This section provides additional instructions that are required for the virtual server-admin.example.com.

When you configure this virtual server on the hardware load balancer:

- Enable address and port translation.
- Enable reset of connections when services or hosts are down.

Additional Instructions for wcc.example.com

The address wcc.example.com is a virtual server name that acts as the access point for all HTTP traffic to the runtime Oracle WebCenter Content components. Traffic to SSL is configured. Clients access this service using the address wcc.example.com:443 for HTTP. When you configure this virtual server on the hardware load balancer:

- Use port 80 and port 443. Any request that goes to port 80 (non-SSL protocol) should be redirected to port 443 (SSL protocol).
- Specify ANY as the protocol (non-HTTP protocols are required for B2B).
- Enable address and port translation.
- Enable reset of connections when services and/or nodes are down.
- Create rules to filter out access to /console and /em on this virtual server.

These context strings direct requests to Oracle WebLogic Server Administration Console and to Oracle Enterprise Manager Fusion Middleware Control and should be used only when accessing the system from admin.example.com.

Additional Instructions for wccinternal.example.com

The address wccinternal.example.com is a virtual server name used for internal invocations of WebCenter Content and SOA services. This URL is not exposed to the Internet and is accessible only from the intranet. The incoming traffic from clients is not SSL enabled.

This address is used for both HTTP and Remote Intradoc Client (RIDC) traffic using different ports:

- HTTP traffic is routed via ports 7777 and 80.
- RIDC traffic is routed via ports 6300 and 4400 over TCP.

HTTP traffic goes to goes to Web tier hosts pool (WEBHOST1 and WEBHOST2) pool.

The end-user RIDC traffic (such as from the WebCenter Content ADF UI) goes directly to the WebCenter Content hosts pool (WCCHOST1 and WCCHOST2). The RIDC traffic uses port 6300 on the load balancer (6300 is mainly for masking), but the traffic ultimately routes to the RIDC port (4444) on the WebCenter hosts.

For Oracle SOA Suite systems, users can set this URL while modeling composites or at runtime with the appropriate MBean through Fusion Middleware Control, as the URL to be used for invoking internal services. You can use this URL for any service callback to WebCenter Content components from Oracle SOA Suite. Clients access this service using the address `wccinternal.example.com:80`, and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2.

When you configure this virtual server on the hardware load balancer:

- Enable address and port translation.
- Enable reset of connections when services or nodes are down.
- As with `wcc.example.com`, create rules to filter out access to `/console` and `/em` on this virtual server.

Configuring the Firewalls and Ports for an Enterprise Deployment

As an administrator, it is important that you become familiar with the port numbers used by various Oracle Fusion Middleware products and services. This ensures that the same port number is not used by two services on the same host, and that the proper ports are open on the firewalls in the enterprise topology.

The following tables lists the ports that you must open on the firewalls in the topology:

Firewall notation:

- FW0 refers to the outermost firewall.
- FW1 refers to the firewall between the web tier and the application tier.
- FW2 refers to the firewall between the application tier and the data tier.

Table 6-1 Firewall Ports Common to All Fusion Middleware Enterprise Deployments

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	80	HTTP / Load Balancer	Inbound	Timeout depends on the size and type of HTML content.

Table 6-1 (Cont.) Firewall Ports Common to All Fusion Middleware Enterprise Deployments

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	443	HTTPS / Load Balancer	Inbound	Timeout depends on the size and type of HTML content.
Browser request	FW1	80	HTTP / Load Balancer	Outbound (for intranet clients)	Timeout depends on the size and type of HTML content.
Browser request	FW1	443	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on the size and type of HTML content.
Callbacks and Outbound invocations	FW1	80	HTTP / Load Balancer	Outbound	Timeout depends on the size and type of HTML content.
Callbacks and Outbound invocations	FW1	443	HTTPS / Load Balancer	Outbound	Timeout depends on the size and type of HTML content.
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	n/a
OHS registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
OHS management by Administration Server	FW1	OHS Admin Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period (5-10 seconds).
Session replication within a WebLogic Server cluster	n/a	n/a	n/a	n/a	By default, this communication uses the same port as the server's listen address.

Table 6-1 (Cont.) Firewall Ports Common to All Fusion Middleware Enterprise Deployments

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Administration Console access	FW1	7001	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the admin console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Database access	FW2	1521	SQL*Net	Both	Timeout depends on database content and on the type of process model used for SOA.
Coherence for deployment	n/a	8088 Range: 8000 - 8090		n/a	n/a
Oracle Unified Directory access	FW2	389 636 (SSL)	LDAP or LDAP/ssl	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
Oracle Notification Server (ONS)	FW2	6200	ONS	Both	Required for Gridlink. An ONS server runs on each database server.

Table 6-2 Firewall Ports for Product-specific Components in Oracle Fusion Middleware Enterprise Deployments

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Oracle SOA Suite and WSM Server access	FW1	8001 Range: 8000 - 8080	HTTP / WLS_SOAn	Inbound	Timeout varies based on the type of process model used for SOA.
Oracle WebCenter Content Access	FW1	16200	HTTP / WLS_WCCn	Inbound	Browser-based access. Configurable session timeouts.
RIDC API requests	FW1	6300	TCP/WLS_WCCn	Inbound	n/a
Oracle WebCenter Enterprise Capture access	FW1	16400	HTTP / WLS_CPTn	Inbound	Browser-based access. Configurable session timeouts.
Communication between SOA_Cluster members	n/a	8001	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between WCC_Cluster members	n/a	16200	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between CPT_Cluster members	n/a	16400	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.

Preparing the File System for an Enterprise Deployment

Preparing the file system for an enterprise deployment involves understanding the requirements for local and shared storage, as well as the terminology that is used to reference important directories and file locations during the installation and configuration of the enterprise topology.

This chapter describes how to prepare the file system for an Oracle Fusion Middleware enterprise deployment.

- [Overview of Preparing the File System for an Enterprise Deployment](#)
It is important to set up your storage in a way that makes the enterprise deployment easy to understand, configure, and manage.
- [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#)
Oracle recommends that you implement certain guidelines regarding shared storage when you install and configure an enterprise deployment.
- [Understanding the Recommended Directory Structure for an Enterprise Deployment](#)
The diagrams in this section show the recommended directory structure for a typical Oracle Fusion Middleware enterprise deployment.
- [File System and Directory Variables Used in This Guide](#)
Understanding the file system directories and the directory variables used to reference these directories is essential for installing and configuring the enterprise deployment topology.
- [About Creating and Mounting the Directories for an Enterprise Deployment](#)
Oracle recommends that you implement certain best practices when you create or mount the top-level directories in an enterprise deployment.
- [Summary of the Shared Storage Volumes in an Enterprise Deployment](#)
It is important to understand the shared volumes and their purpose in a typical Oracle Fusion Middleware enterprise deployment.

Overview of Preparing the File System for an Enterprise Deployment

It is important to set up your storage in a way that makes the enterprise deployment easy to understand, configure, and manage.

This chapter provides an overview of the process of preparing the file system for an enterprise deployment. Oracle recommends setting up your storage according to information in this chapter. The terminology defined in this chapter is used in the diagrams and procedures throughout the guide.

Use this chapter as a reference to understand the directory variables that are used in the installation and configuration procedures.

Other directory layouts are possible and supported, but the model adopted in this guide was designed for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment

Oracle recommends that you implement certain guidelines regarding shared storage when you install and configure an enterprise deployment.

Before you implement the detailed recommendations in this chapter, be sure to review the recommendations and general information about using shared storage in the *Oracle Fusion Middleware High Availability Guide*.

The recommendations in this chapter are based on the concepts and guidelines described in the *Oracle Fusion Middleware High Availability Guide*.

[Table 7-1](#) lists the key sections that you should review and how those concepts apply to an enterprise deployment.

Table 7-1 Shared Storage Resources in the High Availability Guide

Section in <i>High Availability Guide</i>	Importance to an Enterprise Deployment
Shared Storage Prerequisites	Describes guidelines for disk format and the requirements for hardware devices that are optimized for shared storage.
Using Shared Storage for Binary (Oracle Home) Directories	Describes your options for storing the Oracle home on a shared storage device that is available to multiple hosts. For an enterprise deployment, Oracle recommends that you use redundant Oracle homes on separate storage volumes. If a separate volume is not available, a separate partition on the shared disk should be used to provide redundant Oracle homes to application tier hosts.
Using Shared Storage for Domain Configuration Files	Describes the concept of creating separate domain homes for the Administration Server and the Managed Servers in the domain. For an enterprise deployment, the Administration Server domain home location is referenced by the <code>ASERVER_HOME</code> variable.
Shared Storage Requirements for JMS Stores and JTA Logs	Provides instructions for setting the location of the transaction logs and JMS stores for an enterprise deployment.
Introduction to Zero Downtime Patching	Describes the Zero Downtime feature and the procedure to configure and monitor workflows.

 Note:

Zero Downtime Patching (ZDT Patching) provides an automated mechanism to orchestrate the rollout of patches while avoiding downtime or loss of sessions. ZDT reduces risks and downtime of mission-critical applications that require availability and predictability while applying patches.

By using the workflows that you define, you can patch or update any number of nodes in a domain with little or no manual intervention. Changes are rolled out to one node at a time. This preemptively allows for session data to be migrated to compatible servers in the cluster and allows service migration of singleton services, such as JTA and JMS.

When you patch the Oracle home, the current Oracle home must be installed locally on each node that is included in the workflow. Although it is not required, Oracle also recommends that the Oracle home be in the same location on each node.

Understanding the Recommended Directory Structure for an Enterprise Deployment

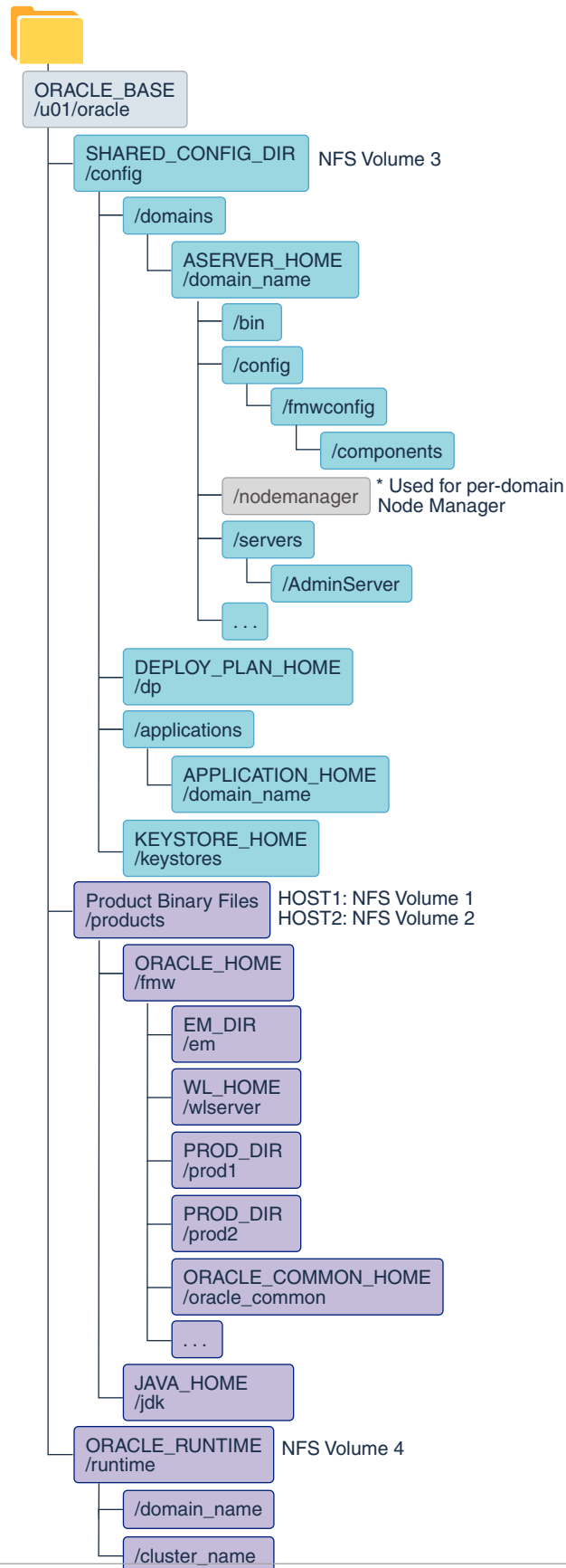
The diagrams in this section show the recommended directory structure for a typical Oracle Fusion Middleware enterprise deployment.

The directories shown in the diagrams contain binary files that are installed on disk by the Oracle Fusion Middleware installers, domain-specific files generated via the domain configuration process, as well as domain configuration files that are propagated to the various host computers via the Oracle WebLogic Server pack and unpack commands:

- [Figure 7-1](#) shows the resulting directory structure on the shared storage device after you have installed and configured a typical Oracle Fusion Middleware enterprise deployment. The shared storage directories are accessible by the application tier host computers.
- [Figure 7-2](#) shows the resulting directory structure on the local storage device for a typical application tier host after you have installed and configured an Oracle Fusion Middleware enterprise deployment. The Managed Servers in particular are stored on the local storage device for the application tier host computers.
- [Figure 7-3](#) shows the resulting directory structure on the local storage device for a typical Web tier host after you have installed and configured an Oracle Fusion Middleware enterprise deployment. Note that the software binaries (in the Oracle home) are installed on the local storage device for each Web tier host.

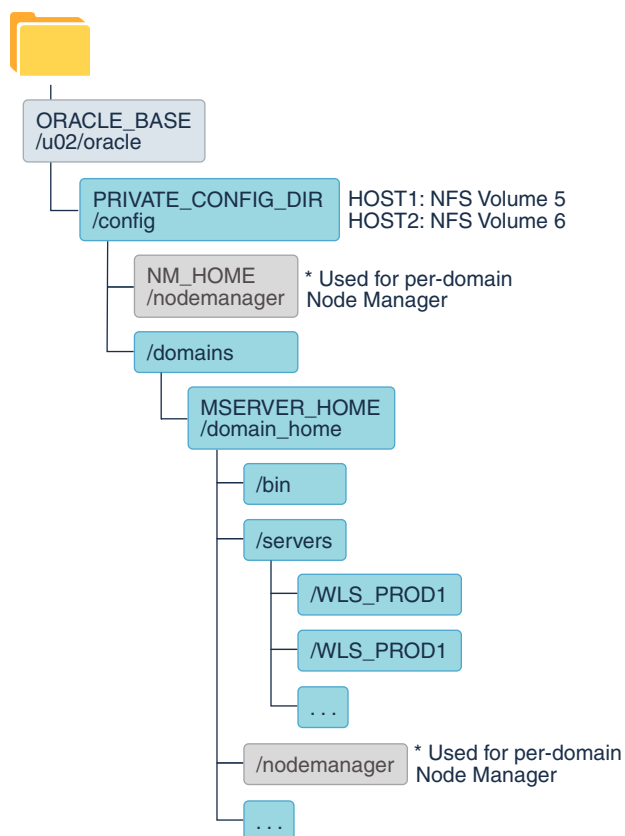
Where applicable, the diagrams also include the standard variables used to reference the directory locations in the installation and configuration procedures in this guide.

Figure 7-1 Recommended Shared Storage Directory Structure for an Enterprise Deployment



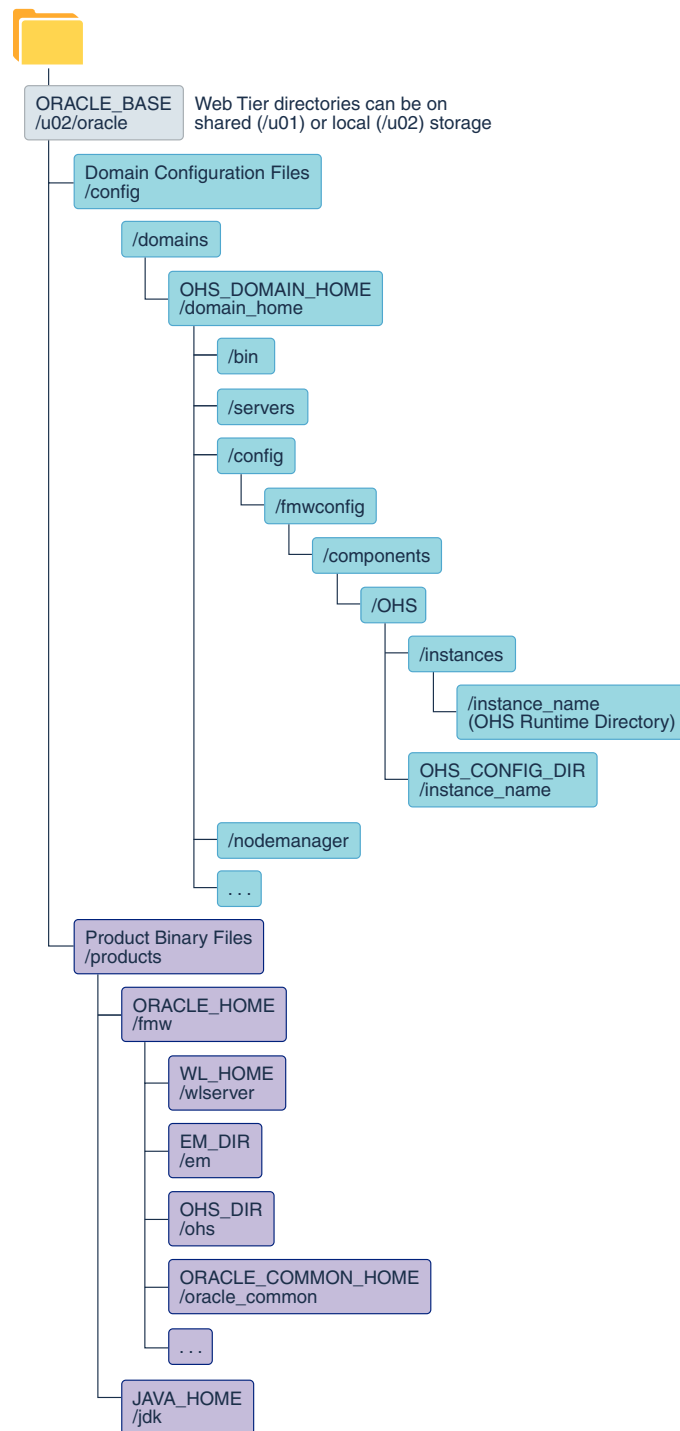
* See [About the Node Manager Configuration in a Typical Enterprise Deployment](#).

Figure 7-2 Recommended Local Storage Directory Structure for an Application Tier Host Computer in an Enterprise Deployment



* See [About the Node Manager Configuration in a Typical Enterprise Deployment](#).

Figure 7-3 Recommended Local Storage Directory Structure for a Web Tier Host Computer in an Enterprise Deployment



File System and Directory Variables Used in This Guide

Understanding the file system directories and the directory variables used to reference these directories is essential for installing and configuring the enterprise deployment topology.

[Table 7-2](#) lists the file system directories and the directory variables that are used to reference the directories on the application tier. [Table 7-3](#) lists the file system directories and variables that are used to reference the directories on the web tier.

For additional information about mounting these directories when you use shared storage, see [About Creating and Mounting the Directories for an Enterprise Deployment](#).

Throughout this guide, the instructions for installing and configuring the topology refer to the directory locations that use the variables shown here.

You can also define operating system variables for each of the directories listed in this section. If you define system variables for the particular UNIX shell that you are using, you can then use the variables as they are used in this document, without having to map the variables to the actual values for your environment.

Note:

As you configure your storage devices to accommodate the recommended directory structure, note the actual directory paths in the Enterprise Deployment workbook. You will use these addresses later when you enable the IP addresses on each host computer.

See [Using the Enterprise Deployment Workbook](#).

Table 7-2 Sample Values for Key Directory Variables on the Application Tier

Directory Variable	Description	Relative Path	Sample Value on the Application Tier
<i>ORACLE_BASE</i>	The base directory, under which Oracle products are installed.	N/A	/u01/oracle
<i>ORACLE_HOME</i>	The read-only location for the product binaries. For the application tier host computers, it is stored on shared disk. The Oracle home is created when you install the Oracle Fusion Middleware Infrastructure software. You can then install additional Oracle Fusion Middleware products into the same Oracle home.	<i>ORACLE_BASE</i> /products/fmw	/u01/oracle/products/fmw

Table 7-2 (Cont.) Sample Values for Key Directory Variables on the Application Tier

Directory Variable	Description	Relative Path	Sample Value on the Application Tier
<i>ORACLE_COMMON_HOME</i>	The directory within the Oracle Fusion Middleware Oracle home where common utilities, libraries, and other common Oracle Fusion Middleware products are stored.	<i>ORACLE_HOME/oracle_common</i>	<i>/u01/oracle/products/fmw/oracle_common</i>
<i>WL_HOME</i>	The directory within the Oracle home where the Oracle WebLogic Server software binaries are stored.	<i>ORACLE_HOME/wlserver</i>	<i>/u01/oracle/products/fmw/wlserver</i>
<i>PROD_DIR</i>	Individual product directories for each Oracle Fusion Middleware product that you install.	<i>ORACLE_HOME/prod_dir</i>	<i>/u01/oracle/products/fmw/prod_dir</i> The product can be soa, wcc, idm, bi, or another value, depending on your enterprise deployment.
<i>EM_DIR</i>	The product directory used to store the Oracle Enterprise Manager Fusion Middleware Control software binaries.	<i>ORACLE_HOME/em</i>	<i>/u01/oracle/products/fmw/em</i>
<i>JAVA_HOME</i>	The location where you install the supported Java Development Kit (JDK).	<i>ORACLE_BASE/products/jdk</i>	<i>/u01/oracle/products/jdk</i>
<i>SHARED_CONFIG_DIR</i>	The shared parent directory for shared environment configuration files, including domain configuration, keystores, runtime artifacts, and application deployments	<i>ORACLE_BASE/config</i>	<i>/u01/oracle/config</i>
<i>PRIVATE_CONFIG_DIR</i>	The local or nfs-mounted private configuration directory unique to a given host containing the machine-specific domain directory (MSERVER_HOME). Directory variable: PRIVATE_CONFIG_DIR	<i>/u02/oracle/config</i>	<i>/u02/oracle/config</i>
<i>ASERVER_HOME</i>	The Administration Server domain home, which is installed on a shared disk.	<i>SHARED_CONFIG_DIR/domains/domain_name</i>	<i>/u01/oracle/config/domains/domain_name</i> In this example, replace <i>domain_name</i> with the name of the WebLogic Server domain.

Table 7-2 (Cont.) Sample Values for Key Directory Variables on the Application Tier

Directory Variable	Description	Relative Path	Sample Value on the Application Tier
<i>MSERVER_HOME</i>	The Managed Server domain home, which is created by using the unpack command on the local disk of each application tier host.	<i>PRIVATE_CONFIG_DIR</i> / <i>domains/domain_name</i>	<i>/u02/oracle/config/</i> <i>domains/domain_name</i> In this example, replace <i>domain_name</i> with the name of the WebLogic Server domain.
<i>APPLICATION_HOME</i>	The Application home directory, which is installed on shared disk, so the directory is accessible by all the application tier host computers.	<i>SHARED_CONFIG_DIR</i> / <i>applications/domain_name</i>	<i>/u01/oracle/config/</i> <i>applications/</i> <i>domain_name</i> In this example, replace <i>domain_name</i> with the name of the WebLogic Server domain.
<i>ORACLE_RUNTIME</i>	This directory contains the Oracle runtime artifacts, such as the JMS logs and TLogs. Typically, you mount this directory as a separate shared file system, which is accessible by all hosts in the domain. When you run the Configuration Wizard or perform post-configuration tasks, and you identify the location of JMS stores or tlogs persistent stores, then you can use this directory, qualified with the name of the domain, the name of the cluster, and the purpose of the directory. For example: <i>ORACLE_RUNTIME/</i> <i>cluster_name/jms</i>	<i>ORACLE_BASE</i> / <i>runtime</i>	<i>/u01/oracle/runtime/</i>
<i>NM_HOME</i>	The directory used by the Per Machine Node Manager start script and configuration files. Note: This directory is necessary only if you are using a Per Machine Node Manager configuration. See About the Node Manager Configuration in a Typical Enterprise Deployment .	<i>PRIVATE_CONFIG_DIR</i> / <i>node_manager</i>	<i>/u02/oracle/config/</i> <i>node_manager</i>

Table 7-2 (Cont.) Sample Values for Key Directory Variables on the Application Tier

Directory Variable	Description	Relative Path	Sample Value on the Application Tier
<i>DEPLOY_PLAN_HOME</i>	The deployment plan directory, which is used as the default location for application deployment plans. Note: This directory is required only when you are deploying custom applications to the application tier.	<i>SHARED_CONFIG_DIR</i> /dp	/u01/oracle/config/dp
<i>KEYSTORE_HOME</i>	The shared location for custom certificates and keystores.	<i>SHARED_CONFIG_DIR</i> /keystores	/u01/oracle/config/keystores

Table 7-3 Sample Values for Key Directory Variables on the Web Tier

Directory Variable	Description	Sample Value on the Web Tier
<i>WEB_ORACLE_HOME</i>	The read-only location for the Oracle HTTP Server product binaries. For the web tier host computers, this directory is stored on the local disk. The Oracle home is created when you install the Oracle HTTP Server software .	/u02/oracle/products/fmw
<i>ORACLE_COMMON_HOME</i>	The directory within the Oracle HTTP Server Oracle home where common utilities, libraries, and other common Oracle Fusion Middleware products are stored.	/u02/oracle/products/fmw/oracle_common
<i>WL_HOME</i>	The directory within the Oracle home where the Oracle WebLogic Server software binaries are stored.	/u02/oracle/products/fmw/wlserver
<i>PROD_DIR</i>	Individual product directories for each Oracle Fusion Middleware product that you install.	/u02/oracle/products/fmw/ohs
<i>JAVA_HOME</i>	The location where you install the supported Java Development Kit (JDK).	/u02/oracle/products/jdk
<i>WEB_DOMAIN_HOME</i>	The Domain home for the standalone Oracle HTTP Server domain, which is created when you install Oracle HTTP Server on the local disk of each web tier host.	/u02/oracle/config/domains/ <i>domain_name</i> In this example, replace <i>domain_name</i> with the name of the WebLogic Server domain.

Table 7-3 (Cont.) Sample Values for Key Directory Variables on the Web Tier

Directory Variable	Description	Sample Value on the Web Tier
<i>WEB_CONFIG_DIR</i>	This is the location where you edit the Oracle HTTP Server configuration files (for example, <code>httpd.conf</code> and <code>moduleconf/*.conf</code>) on each web host. Note this directory is also referred to as the OHS Staging Directory. Changes made here are later propagated to the OHS Runtime Directory. See <i>Staging and Run-time Configuration Directories in the Oracle Fusion Middleware Administering Oracle HTTP Server</i>.	<pre>/u02/oracle/config/ domains /domain_name/ config/fmwconfig /components/OHS/ instance/ /instance_name</pre>
<i>WEB_KEYSTORE_HOME</i>	If you use Oracle Traffic Director as your web server, this is the location for custom certificates and keystores.	<pre>/u02/oracle/config/ keystores</pre>

About Creating and Mounting the Directories for an Enterprise Deployment

Oracle recommends that you implement certain best practices when you create or mount the top-level directories in an enterprise deployment.

- For the application tier, install the Oracle home, which contains the software binaries, on a second shared storage volume or second partition that is mounted to WCCHOST2. Be sure the directory path to the binaries on WCCHOST2 is identical to the directory path on WCCHOST1.

For example:

```
/u01/oracle/products/fmw/
```

See [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#).

- This enterprise deployment guide assumes that the Oracle Web tier software is installed on a local disk.

The Web tier installation is typically performed on local storage to the WEBHOST nodes. When you use shared storage, you can install the Oracle Web tier binaries (and create the Oracle HTTP Server instances) on a shared disk. However, if you do so, then the shared disk *must* be separate from the shared disk used for the application tier, and you must consider the appropriate security restrictions for access to the storage device across tiers.

As with the application tier servers (WCCHOST1 and WCCHOST2), use the same directory path on both computers.

For example:

```
/u02/oracle/products/fmw/
```

Summary of the Shared Storage Volumes in an Enterprise Deployment

It is important to understand the shared volumes and their purpose in a typical Oracle Fusion Middleware enterprise deployment.

You can use shared storage to host the Web tier binaries and config to make backups easier so that files are stored on a more fault-tolerant hardware, but each node needs to use a private directory that is not shared with the other nodes.

The following table summarizes the shared volumes and their purpose in a typical Oracle Fusion Middleware enterprise deployment.

See [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#).

Table 7-4 Shared Storage Volumes in an Enterprise Deployment

Volume in Shared Storage	Mounted to Host	Mount Directories	Description and Purpose
NFS Volume 1	WCCHOST1	/u01/oracle/products/	Storage for the product binaries to be used by WCCHOST1; this is where the Oracle home directory and product directories are installed. Used initially by WCCHOST1, but can be shared with other hosts when scaling-out the topology.
NFS Volume 2	WCCHOST2	/u01/oracle/products/	Storage for the product binaries to be used by WCCHOST2; this is where the Oracle home directory and product directories are installed. Used initially by WCCHOST2, but can be shared with other hosts when scaling-out the topology.
NFS Volume 3	WCCHOST1 WCCHOST2	/u01/oracle/config/	Administration Server domain configuration, mounted to all hosts; used initially by WCCHOST1, but can be failed over to any host.

Table 7-4 (Cont.) Shared Storage Volumes in an Enterprise Deployment

Volume in Shared Storage	Mounted to Host	Mount Directories	Description and Purpose
NFS Volume 4	WCCHOST1 WCCHOST2	/u01/oracle/runtime/	The runtime artifacts directory, mounted to all hosts, contains runtime artifacts such as JMS logs, blogs, and any cluster-dependent shared files needed.
NFS Volume 5	WCCHOST1	/u02/oracle/config/	Local storage for the Managed Server domain directory to be used by WCCHOST1, if the private Managed Server domain directory resides on shared storage.
NFS Volume 6	WCCHOST2	/u02/oracle/config/	Local storage for the Managed Server domain directory to be used by WCCHOST2, if the private Managed Server domain directory resides on shared storage.
NFS Volume 7	WEBHOST1	/u02/oracle/	Local storage for the Oracle HTTP Server or the Oracle Traffic Director software binaries (Oracle home) and domain configuration files that are used by WEBHOST1, if the web tier private binary and config directories reside on shared storage.
NFS Volume 8	WEBHOST2	/u02/oracle/	Local storage for the Oracle HTTP Server or the Oracle Traffic Director software binaries (Oracle home) and domain configuration files that are used by WEBHOST2, if the Web Tier private binary and config directories reside on shared storage.

8

Preparing the Host Computers for an Enterprise Deployment

It is important to perform a set of tasks on each computer or server before you configure the enterprise deployment topology. This involves verifying the minimum hardware and operating system requirements for each host, configuring operating system users and groups, enabling Unicode support, mounting the required shared storage systems to the host and enabling the required virtual IP addresses on each host.

This chapter describes the tasks that you must perform from each computer or server that is hosting the enterprise deployment.

- [Verifying the Minimum Hardware Requirements for Each Host](#)
After you procure the required hardware for the enterprise deployment, it is important to ensure that each host computer meets the minimum system requirements.
- [Verifying Linux Operating System Requirements](#)
You can review the typical Linux operating system settings for an enterprise deployment in this section.
- [Setting the DNS Settings](#)
- [Configuring Operating System Users and Groups](#)
The users and groups to be defined on each of the computers that host the enterprise deployment are listed in this section.
- [Enabling Unicode Support](#)
It is recommended to enable Unicode support in your operating system so as to allow processing of characters in Unicode.
- [Mounting the Required Shared File Systems on Each Host](#)
It is important to understand how to mount the shared storage to all the servers that require access.
- [Enabling the Required Virtual IP Addresses on Each Host](#)
You must enable the required virtual IP addresses on each host in order to prepare the host for the enterprise deployment.

Verifying the Minimum Hardware Requirements for Each Host

After you procure the required hardware for the enterprise deployment, it is important to ensure that each host computer meets the minimum system requirements.

After you have procured the required hardware for the enterprise deployment, log in to each host computer and verify the system requirements listed in [Hardware and Software Requirements for the Enterprise Deployment Topology](#).

If you deploy to a virtual server environment, such as Oracle Exalogic, ensure that each of the virtual servers meets the minimum requirements.

Ensure that you have sufficient local disk storage and shared storage configured as described in [Preparing the File System for an Enterprise Deployment](#).

Allow sufficient swap and temporary space; specifically:

- **Swap Space**—The system must have at least 500 MB.
- **Temporary Space**—There must be a minimum of 500 MB of free space in the /tmp directory.

Verifying Linux Operating System Requirements

You can review the typical Linux operating system settings for an enterprise deployment in this section.

To ensure the host computers meet the minimum operating system requirements, ensure that you have installed a certified operating system and that you have applied all the necessary patches for the operating system.

In addition, review the following sections for typical Linux operating system settings for an enterprise deployment.

- [Setting Linux Kernel Parameters](#)
- [Setting the Open File Limit and Number of Processes Settings on UNIX Systems](#)
- [Verifying IP Addresses and Host Names in DNS or hosts File](#)

Setting Linux Kernel Parameters

The kernel-parameter and shell-limit values shown in [Table 8-1](#) are recommended values only. Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.

Kernel parameters must be set to a minimum of those in [Table 8-1](#) on all nodes in the topology.

The values in the following table are the current Linux recommendations. For the latest recommendations for Linux and other operating systems, see *Oracle Fusion Middleware System Requirements and Specifications*.

If you deploy a database onto the host, you might need to modify additional kernel parameters. Refer to 12c (12.2.1.3.0) Configuring Kernel Parameters in *Oracle Grid Infrastructure Installation Guide for Linux*.

Table 8-1 UNIX Kernel Parameters

Parameter	Value
kernel.sem	256 32000 100 142
kernel.shmmax	4294967295

To set these parameters:

1. Sign in as root and add or amend the entries in the `/etc/sysctl.conf` file.
2. Save the file.
3. Activate the changes by entering the following command:

```
/sbin/sysctl -p
```

Setting the Open File Limit and Number of Processes Settings on UNIX Systems

On UNIX operating systems, the Open File Limit is an important system setting, which can affect the overall performance of the software running on the host computer.

For guidance on setting the Open File Limit for an Oracle Fusion Middleware enterprise deployment, see [Host Computer Hardware Requirements](#).

Note:

The following examples are for Linux operating systems. Consult your operating system documentation to determine the commands to be used on your system.

For more information, see the following sections.

- [Viewing the Number of Currently Open Files](#)
- [Setting the Operating System Open File and Processes Limits](#)

Viewing the Number of Currently Open Files

You can see how many files are open with the following command:

```
/usr/sbin/lsof | wc -l
```

To check your open file limits, use the following commands.

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

Setting the Operating System Open File and Processes Limits

To change the Open File Limit values:

1. Sign in as root user and edit the following file:

```
/etc/security/limits.conf
```
2. Add the following lines to the `limits.conf` file. (The values shown here are for example only):

```
* soft  nofile  4096
* hard  nofile  65536
* soft  nproc   2047
* hard  nproc   16384
```

The `nofiles` values represent the open file limit; the `nproc` values represent the number of processes limit.

3. Save the changes, and close the `limits.conf` file.

 Note:

If you are running Oracle Enterprise Linux 6 or Red Hat Linux 6, locate the following operating system configuration file: `/etc/security/limits.d/90-nproc.conf`

Ensure that the same values are added to the `90-nproc.conf` file. Otherwise, the values in the `90-nproc.conf` file overrides the values in the `limits.conf` file.

4. Re-login into the host computer.

Verifying IP Addresses and Host Names in DNS or hosts File

Before you begin the installation of the Oracle software, ensure that the IP address, fully qualified host name, and the short name of the host are all registered with your DNS server. Alternatively, you can use the local `hosts` file and add an entry similar to the following:

```
IP_Address Fully_Qualified_Name Short_Name
```

For example:

```
10.229.188.205 host1.example.com host1
```

Setting the DNS Settings

Configure the host to access your corporate DNS hosts. To do this, update DNS settings by updating the file `/etc/resolv.conf`.

Configuring Operating System Users and Groups

The users and groups to be defined on each of the computers that host the enterprise deployment are listed in this section.

Groups

You must create the following groups on each node.

- `oinstall`
- `dba`

Users

You must create the following user on each node.

- nobody—An unprivileged user.
- oracle—The owner of the Oracle software. You may use a different name. The primary group for this account must be oinstall. The account must also be in the dba group.

 Note:

- The group oinstall must have write privileges to all the file systems on shared and local storage that are used by the Oracle software.
- Each group must have the same Group ID on every node.
- Each user must have the same User ID on every node.

Enabling Unicode Support

It is recommended to enable Unicode support in your operating system so as to allow processing of characters in Unicode.

Your operating system configuration can influence the behavior of characters supported by Oracle Fusion Middleware products.

On UNIX operating systems, Oracle highly recommends that you enable Unicode support by setting the LANG and LC_ALL environment variables to a locale with the UTF-8 character set. This enables the operating system to process any character in Unicode. Oracle WebCenter Content technologies, for example, are based on Unicode.

If the operating system is configured to use a non-UTF-8 encoding, Oracle WebCenter Content components may function in an unexpected way. For example, a non-ASCII file name might make the file inaccessible and cause an error. Oracle does not support problems caused by operating system constraints.

Mounting the Required Shared File Systems on Each Host

It is important to understand how to mount the shared storage to all the servers that require access.

The shared storage configured, as described in [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#), must be available on the hosts that use it.

In an enterprise deployment, it is assumed that you have a hardware storage filer, which is available and connected to each of the host computers that you have procured for the deployment.

You must mount the shared storage to all servers that require access.

Each host must have appropriate privileges set within the Network Attached Storage (NAS) or Storage Area Network (SAN) so that it can write to the shared storage.

Follow the best practices of your organization for mounting shared storage. This section provides an example of how to do this on Linux by using NFS storage.

You must create and mount shared storage locations so that WCCHOST1 and WCCHOST2 can see the same location if it is a binary installation in two separate volumes.

See [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#).

You use the following command to mount shared storage from a NAS storage device to a Linux host. If you are using a different type of storage device or operating system, refer to your manufacturer documentation for information about how to do this.

**Note:**

The user account used to create a shared storage file system owns and has read, write, and execute privileges for those files. Other users in the operating system group can read and execute the files, but they do not have write privileges.

See *Selecting an Installation User in the Oracle Fusion Middleware Installation Planning Guide*.

In the following example, `nasfiler` represents the shared storage filer. Also note that these are examples only. Typically, the mounting of these shared storage locations should be done by using the `/etc/fstabs` file on UNIX systems, so that the mounting of these devices survives a reboot. Refer to your operating system documentation for more information.

To mount the shared storage on Linux:

1. Create the mount directories on WCCHOST1, as described in [Summary of the Shared Storage Volumes in an Enterprise Deployment](#), and then mount the shared storage. For example:

```
mount -t nfs nasfiler:VOL1/oracle/products/ /u01/oracle/products/
```

2. Repeat the procedure on WCCHOST2 using VOL2.

Validating the Shared Storage Configuration

Ensure that you can read and write files to the newly mounted directories by creating a test file in the shared storage location that you just configured.

For example:

```
$ cd newly mounted directory
$ touch testfile
```

Verify that the owner and permissions are correct:

```
$ ls -l testfile
```

Then remove the file:

```
$ rm testfile
```

 Note:

The shared storage can be a NAS or SAN device. The following example illustrates creating storage for a NAS device from WCCHOST1. The options may differ depending on the specific storage device.

```
mount -t nfs -o  
rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsz=32768,wsz=32768  
nasfiler:VOL1/Oracle/u01/oracle
```

Contact your storage vendor and machine administrator to learn about the appropriate options for your environment.

Enabling the Required Virtual IP Addresses on Each Host

You must enable the required virtual IP addresses on each host in order to prepare the host for the enterprise deployment.

To prepare each host for the enterprise deployment, you must enable the virtual IP (VIP) addresses that are described in [Reserving the Required IP Addresses for an Enterprise Deployment](#).

It is assumed that you have already reserved the VIP addresses and host names and that they have been enabled by your network administrator. You can then enable the VIPs on the appropriate host.

Note that the virtual IP addresses used for the enterprise topology are not persisted because they are managed by Whole Server Migration (for selected Managed Servers and clusters) or by manual failover (for the Administration Server).

Starting with Oracle Enterprise Linux 6, the "ifconfig" command is deprecated and is replaced with the "ip" command.

To enable the VIP addresses on each host, run the following commands as root:

1. Determine the CIDR notation of the netmask. Each Netmask has a CIDR notation. For example, 255.255.240.0 has a CIDR of 20.

If the netmask you are adding is the same as the interface, the fastest way to determine this is to examine the existing IP address that are assigned to the network card. You can do this by using the following command:

```
ip addr show dev eth0
```

Sample output:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc  
pfifo_fast qlen 1000  
link/ether 00:21:f6:03:85:9f brd ff:ff:ff:ff:ff:ff  
inet 192.168.20.1/20 brd 10.248.11.255 scope global eth0
```

In this example, the CIDR value is the value after the forward slash (/), which is, 20. If you are unsure of the CIDR value, contact your network administrator.

2. Configure the additional IP address on the appropriate network interface card with an appropriately suffixed label using the following command:

```
ip addr add VIP/CIDR dev nic# label nic#:n
```

 Note:

For each VIP/VHN that you need to add, increment the :n suffix starting with :1

Example: For VIP IP of 192.168.20.3, netmask: 255.255.240.0 (CIDR: 20), and the eth0 NIC:

```
ip addr add 192.168.20.3/20 dev eth0 label eth0:1
```

3. For each of the virtual IP addresses that you define, update the ARP caches by using the following command:

```
arping -b -A -c 3 -I eth0 192.168.20.3
```

9

Preparing the Database for an Enterprise Deployment

Preparing the database for an enterprise deployment involves ensuring that the database meets specific requirements, creating database services, using SecureFiles for large objects in the database, and creating database backup strategies.

This chapter provides information about the database requirements, creating database services, and about the database backup strategies.

- [Overview of Preparing the Database for an Enterprise Deployment](#)
It is important to understand how to configure a supported database as part of an Oracle Fusion Middleware enterprise deployment.
- [About Database Requirements](#)
Before you configure the enterprise deployment topology, you have to verify that the database meets the requirements described in the following sections.
- [Creating Database Services](#)
When multiple Oracle Fusion Middleware products are sharing the same database, each product should be configured to connect to a separate, dedicated database service. This service should be different from the default database service. Having a different service name from the default, allows you to create role based database services for Disaster Recovery and Multi-Datacenter topologies.
- [Using SecureFiles for Large Objects \(LOBs\) in an Oracle Database](#)
SecureFiles is a new LOB storage architecture introduced in Oracle Database 11g Release 1. It is recommended to use SecureFiles for the Oracle Fusion Middleware schemas, in particular for the Oracle SOA Suite schemas.
- [About Database Backup Strategies](#)
Performing a database backup at key points in the installation and configuration of an enterprise deployment enables you to recover quickly from any issue that might occur in the later configuration steps.

Overview of Preparing the Database for an Enterprise Deployment

It is important to understand how to configure a supported database as part of an Oracle Fusion Middleware enterprise deployment.

Most Oracle Fusion Middleware products require a specific set of schemas that must be installed in a supported database. The schemas are installed by using the Oracle Fusion Middleware Repository Creation Utility (RCU).

In an enterprise deployment, Oracle recommends a highly available Real Application Clusters (Oracle RAC) database for the Oracle Fusion Middleware product schemas.

About Database Requirements

Before you configure the enterprise deployment topology, you have to verify that the database meets the requirements described in the following sections.

- [Supported Database Versions](#)
- [Additional Database Software Requirements](#)
- [Installing and Validating Oracle Text](#)

Supported Database Versions

Use the following information to verify what databases are supported by each Oracle Fusion Middleware release and which version of the Oracle database you are currently running:

- For a list of all certified databases, refer to *Oracle Fusion Middleware Supported System Configurations*.
- To check the release of your database, query the `PRODUCT_COMPONENT_VERSION` view:

```
SQL> SELECT VERSION FROM SYS.PRODUCT_COMPONENT_VERSION WHERE  
        PRODUCT LIKE 'Oracle%';
```

Oracle Fusion Middleware requires that the database supports the AL32UTF8 character set. Check the database documentation for information on choosing a character set for the database.

For enterprise deployments, Oracle recommends that you use GridLink data sources to connect to Oracle RAC databases.



Note:

For more information about using GridLink data sources and SCAN, see Using Active GridLink Data Sources in *Oracle Fusion Middleware Administering JDBC Data Sources for Oracle WebLogic Server*.

Use of Active GridLink has specific licensing requirements, including a valid WebLogic Suite license. See [Oracle Oracle WebLogic Server data sheet](#).

Additional Database Software Requirements

In the enterprise topology, there are two database host computers in the data tier that host the two instances of the RAC database. These hosts are referred to as `DBHOST1` and `DBHOST2`.

Before you install or configure the enterprise topology, you must ensure that the following software is installed and available on `DBHOST1` and `DBHOST2`:

- **Oracle Clusterware**

See Installing Oracle Grid Infrastructure for a Cluster in *Oracle Grid Infrastructure Installation Guide for Linux*.

- **Oracle Real Application Clusters**

See Installing Oracle RAC and Oracle RAC One Node in *Oracle Real Application Clusters Installation Guide for Linux and UNIX*.

- **Time synchronization between Oracle RAC database instances**

The clocks of the database instances must be in sync if they are used by servers in a Fusion Middleware cluster configured with server migration.

- **Automatic Storage Management (optional)**

See Introducing Oracle Automatic Storage Management in *Oracle Automatic Storage Management Administrator's Guide*.

Installing and Validating Oracle Text

Before you install or configure the WebCenter Content enterprise topology, you must be sure that Oracle Text is installed and available on DBHOST1 and DBHOST2.

For more information on installing Oracle Text, see the *Oracle Database Installation Guide for Linux*.

To make sure that the database used for WebCenter Content installation has Oracle Text enabled, run the following command:

```
SQL> select comp_name, status, substr(version,1,10) as version from dba_registry
where comp_id = 'CONTEXT';
```

```
COMP_NAME STATUS VERSION
-----
Oracle Text VALID 12.1.0.1.0
```

Creating Database Services

When multiple Oracle Fusion Middleware products are sharing the same database, each product should be configured to connect to a separate, dedicated database service. This service should be different from the default database service. Having a different service name from the default, allows you to create role based database services for Disaster Recovery and Multi-Datacenter topologies.

 Note:

The instructions in this section are for the Oracle Database 12c (12.1) release. If you are using another supported database, refer to the appropriate documentation library for more up-to-date and release-specific information.

For more information about connecting to Oracle databases using services, see Overview of Using Dynamic Database Services to Connect to Oracle Databases in *Real Application Clusters Administration and Deployment Guide*.

In addition, the database service should be different from the default database service. For complete instructions on creating and managing database services for an Oracle Database 12c database, see Overview of Automatic Workload Management

with Dynamic Database Services in *Real Application Clusters Administration and Deployment Guide*.

Runtime connection load balancing requires configuring Oracle RAC Load Balancing Advisory with service-level goals for each service for which load balancing is enabled.

You can configure the Oracle RAC Load Balancing Advisory for `SERVICE_TIME` or `THROUGHPUT`. Set the connection load-balancing goal to **SHORT**.

You create and modify Oracle Database services by using the `srvctl` utility.

To create and modify a database service:

1. Add the service to the database and assign it to the instances by using `srvctl`:

```
srvctl add service -db wccdb -service wccedg.example.com -preferred  
wccdb1,wccdb2
```

 Note:

For the Service Name of the Oracle RAC database, use lowercase letters, followed by the domain name. For example: `wccedg.example.com`

2. Start the service:

```
srvctl start service -db wccdb -service wccedg.example.com
```

 Note:

For complete instructions on creating and managing database services with SRVCTL, see *Creating Services with SRVCTL* in the *Real Application Clusters Administration and Deployment Guide*.

3. Modify the service so that it uses the Load Balancing Advisory and the appropriate service-level goals for runtime connection load balancing.

Use the following resources in the Oracle Database 12c *Real Application Clusters Administration and Deployment Guide* to set the `SERVICE_TIME` and `THROUGHPUT` service-level goals:

- Overview of the Load Balancing Advisory
- Configuring Your Environment to Use the Load Balancing Advisory

For example:

Check the default configuration of the service by using this command:

```
srvctl config service -db wccdb -service wccedg.example.com
```

Several parameters are shown. Check the following parameters:

- Connection Load Balancing Goal: Long
- Runtime Load Balancing Goal: NONE

You can modify these parameters by using the following command:

```
srvctl modify service -db wccdb -service wccedg.example.com -
rlbgoal SERVICE_TIME -clbgoal SHORT
```

4. Restart the service:

```
srvctl stop service -db wccdb -service wccedg.example.com
srvctl start service -db wccdb -service wccedg.example.com
```

5. Verify the change in the configuration:

```
srvctl config service -db wccdb -service wccedg.example.com
Runtime Load Balancing Goal: SERVICE_TIME
Service name: wccedg.example.com
Service is enabled
Server pool: wccdb_wccedg.example.com
...
Connection Load Balancing Goal: SHORT
Runtime Load Balancing Goal: SERVICE_TIME
...
```

Using SecureFiles for Large Objects (LOBs) in an Oracle Database

SecureFiles is a new LOB storage architecture introduced in Oracle Database 11g Release 1. It is recommended to use SecureFiles for the Oracle Fusion Middleware schemas, in particular for the Oracle SOA Suite schemas.

Beginning with Oracle Database 11g Release 1, Oracle introduced SecureFiles, a new LOB storage architecture. Oracle recommends that you use SecureFiles for the Oracle Fusion Middleware schemas, in particular for the Oracle SOA Suite schemas. See Using Oracle SecureFiles LOBs in the *Oracle Database SecureFiles and Large Objects Developer's Guide*.

In Oracle 12c Databases, the default setting for using SecureFiles is `PREFERRED`. This means that the database attempts to create a SecureFiles LOB unless a BasicFiles LOB is explicitly specified for the LOB or the parent LOB (if the LOB is in a partition or sub-partition). The Oracle Fusion Middleware schemas do not explicitly specify BasicFiles, which means that Oracle Fusion Middleware LOBs defaults to SecureFiles when installed in an Oracle 12c database.

For Oracle 11g databases, the `db_securefile` system parameter controls the SecureFiles usage policy. This parameter can be modified dynamically. The following options can be used for using SecureFiles:

- `PERMITTED`: Allows SecureFiles to be created (This is the default setting for `db_securefile`. The default storage method uses BasicFiles).
- `FORCE`: Creates all (new) LOBs as SecureFiles.
- `ALWAYS`: Tries to create LOBs as SecureFiles, but falls back to BasicFiles if not possible (if ASSM is disabled).

Other values for the `db_securefile` parameter are:

- IGNORE: Ignore attempts to create SecureFiles.
- NEVER: Disallow new SecureFiles creations.

For Oracle 11g Databases, Oracle recommends that you set the `db_securefile` parameter to `FORCE` before you create the Oracle Fusion Middleware schemas with the Repository Creation Utility (RCU).

Note that the SecureFiles segments require tablespaces managed with automatic segment space management (ASSM). This means that LOB creation on SecureFiles will fail if ASSM is not enabled. However, the Oracle Fusion Middleware tablespaces are created by default with ASSM enabled. As a result, with the default configuration, nothing needs to be changed to enable SecureFiles for the Oracle Fusion Middleware schemas.

About Database Backup Strategies

Performing a database backup at key points in the installation and configuration of an enterprise deployment enables you to recover quickly from any issue that might occur in the later configuration steps.

At key points in the installation and configuration of an enterprise deployment, this guide recommends that you back up your current environment. For example, after you install the product software and create the schemas for a particular Oracle Fusion Middleware product, you should perform a database backup. Performing a backup allows you to perform a quick recovery from any issue that might occur in the later configuration steps.

You can choose to use your own backup strategy for the database, or you can simply make a backup by using operating system tools or RMAN for this purpose.

Oracle recommends that you use Oracle Recovery Manager for the database, particularly if the database was created using Oracle Automatic Storage Management. If possible, you can also perform a cold backup by using operating system tools such as `tar`.

Part III

Configuring the Enterprise Deployment

The tasks that need to be performed to configure the enterprise deployment topology are detailed in this section.

Part III contains the following chapters:

- [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#)
- [Configuring the Web Tier for an Enterprise Deployment](#)
- [Extending the Domain to Include Oracle WebCenter Content](#)
You need to perform certain tasks in order to extend the enterprise deployment domain with the Oracle WebCenter Content software. This includes installing the WebCenter Content, extending the domain for WebCenter Content and completing post-configuration and verification tasks.
- [Extending the Domain with Oracle SOA Suite](#)
- [Extending the Domain to Include Inbound Refinery](#)
- [Extending the Domain to Include Capture](#)
You need to perform certain tasks in order to extend the enterprise deployment domain with Oracle WebCenter Enterprise Capture software.
- [Extending the Domain to Include Imaging](#)
You need to perform certain tasks in order to extend the enterprise deployment domain with Oracle WebCenter Enterprise Imaging software.
- [Extending the Domain to Include WebCenter Content User Interface](#)
You need to perform certain tasks in order to extend the enterprise deployment domain to include Oracle WebCenter Content User Interface software.

Creating the Initial Infrastructure Domain for an Enterprise Deployment

It is important to understand how to install and configure an initial domain, which can be used as the starting point for an enterprise deployment. You can extend this initial domain with the various products and components that constitute the enterprise topology you are deploying.

This chapter provides information on variables used when creating the infrastructure domain, creating the database schemas and configuring the infrastructure domain.

- [Variables Used When Creating the Infrastructure Domain](#)
While creating the infrastructure domain, you will be referencing the directory variables listed in this section.
- [Understanding the Initial Infrastructure Domain](#)
Before creating the initial Oracle Fusion Middleware Infrastructure domain, ensure that you review the following key concepts.
- [Installing the Oracle Fusion Middleware Infrastructure on WCCHOST1](#)
Use the following sections to install the Oracle Fusion Middleware Infrastructure software in preparation for configuring a new domain for an enterprise deployment.
- [Creating the Database Schemas](#)
Oracle Fusion Middleware components require the existence of schemas in a database before you configure a Fusion Middleware Infrastructure domain. Install the schemas listed in this topic in a certified database for use with this release of Oracle Fusion Middleware.
- [Configuring the Infrastructure Domain](#)
You can create and configure a WebLogic domain for the enterprise deployment topology using the configuration wizard.
- [Starting the Administration Server](#)
After the domain is created, you can then perform the following tasks on WCCHOST1.
- [Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group](#)
When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Server authentication provider (DefaultAuthenticator). However, for an enterprise deployment, Oracle recommends that you use a dedicated, centralized LDAP-compliant authentication provider.

Variables Used When Creating the Infrastructure Domain

While creating the infrastructure domain, you will be referencing the directory variables listed in this section.

The directory variables are defined in [File System and Directory Variables Used in This Guide](#).

- `ORACLE_HOME`
- `APPLICATION_HOME`
- `JAVA_HOME`

In addition, you'll be referencing the following virtual IP (VIP) addresses and host names defined in [Reserving the Required IP Addresses for an Enterprise Deployment](#):

- `ADMINVHN`
- `WCCHOST1`
- `WCCHOST2`
- `DBHOST1`
- `DBHOST2`
- SCAN Address for the Oracle RAC Database (`DB-SCAN.example.com`)

Understanding the Initial Infrastructure Domain

Before creating the initial Oracle Fusion Middleware Infrastructure domain, ensure that you review the following key concepts.

- [About the Infrastructure Distribution](#)
- [Characteristics of the Initial Infrastructure Domain](#)

About the Infrastructure Distribution

You create the initial Infrastructure domain for an enterprise deployment by using the Oracle Fusion Middleware Infrastructure distribution. This distribution contains both the Oracle WebLogic Server software and the Oracle JRF software.

The Oracle JRF software consists of Oracle Web Services Manager, Oracle Application Development Framework (Oracle ADF), Oracle Enterprise Manager Fusion Middleware Control, the Repository Creation Utility (RCU), and other libraries and technologies that are required to support the Oracle Fusion Middleware products.

Later in this guide, you can then extend the domain to support the Oracle Fusion Middleware products that are required for your enterprise deployment.

See Understanding Oracle Fusion Middleware Infrastructure in *Understanding Oracle Fusion Middleware*.

Characteristics of the Initial Infrastructure Domain

The following table lists some of the key characteristics of the initial Infrastructure domain. By reviewing and understanding these characteristics, you can better understand the purpose and context of the procedures used to configure the domain.

Many of these characteristics are described in more detail in [Understanding a Typical Enterprise Deployment](#).

Characteristic of the Domain	More Information
Contains only an Administration Server. Managed Servers are added to the domain later, when you extend the initial domain to include Oracle Fusion Middleware products.	About a Typical Enterprise Deployment
Uses a separate virtual IP (VIP) address for the Administration Server.	Configuration of the Administration Server and Managed Servers Domain Directories
Uses a per domain Node Manager configuration.	About the Node Manager Configuration in a Typical Enterprise Deployment
Requires a separately installed LDAP-based authentication provider.	Understanding OPSS and Requests to the Authentication and Authorization Stores

Installing the Oracle Fusion Middleware Infrastructure on WCCHOST1

Use the following sections to install the Oracle Fusion Middleware Infrastructure software in preparation for configuring a new domain for an enterprise deployment.

- [Installing a Supported JDK](#)
- [Starting the Infrastructure Installer on WCCHOST1](#)
- [Navigating the Infrastructure Installation Screens](#)
- [Installing Oracle Fusion Middleware Infrastructure on the Other Host Computers](#)
- [Checking the Directory Structure](#)
After you install the Oracle Fusion Middleware Infrastructure and create the Oracle home, you should see the directory and sub-directories listed in this topic. The contents of your installation vary based on the options that you selected during the installation.
- [Disabling the Derby Database](#)

Installing a Supported JDK

Oracle Fusion Middleware requires that a certified Java Development Kit (JDK) is installed on your system.

- [Locating and Downloading the JDK Software](#)
- [Installing the JDK Software](#)

Locating and Downloading the JDK Software

To find a certified JDK, see the certification document for your release on the Oracle Fusion Middleware Supported System Configurations page.

After you identify the Oracle JDK for the current Oracle Fusion Middleware release, you can download an Oracle JDK from the following location on Oracle Technology Network:

<http://www.oracle.com/technetwork/java/index.html>

Be sure to navigate to the download for the Java SE JDK.

Installing the JDK Software

Install the JDK onto the V0L1 and V0L2 shared storage volumes mounted to /u01/oracle/products on the application tier hosts. Name the folder for the JDK without version numbers to avoid re-configuration challenges during JDK upgrades. Example: /u01/oracle/products/jdk.



Note:

Multiple installations may be needed as recommended mount points use multiple product shared volumes.

For more information about the recommended location for the JDK software, see the [Understanding the Recommended Directory Structure for an Enterprise Deployment](#).

The following example describes how to install a recent version of JDK 1.8.0_131.

1. Change directory to the location where you downloaded the JDK archive file.

```
cd download_dir
```

2. Unpack the archive into the JDK home directory, and then run the following commands:

```
tar -xzf jdk-8u131-linux-x64.tar.gz
```

Note that the JDK version listed here was accurate at the time this document was published. For the latest supported JDK, see the *Oracle Fusion Middleware System Requirements and Specifications* for the current Oracle Fusion Middleware release.

3. Move the JDK directory to the recommended location in the directory structure.

For example:

```
mv ./jdk1.8.0_131 /u01/oracle/products/jdk
```

See [File System and Directory Variables Used in This Guide](#).

4. Define the `JAVA_HOME` and `PATH` environment variables for running Java on the host computer.

For example:

```
export JAVA_HOME=/u01/oracle/products/jdk
export PATH=$JAVA_HOME/bin:$PATH
```

5. Run the following command to verify that the appropriate java executable is in the path and your environment variables are set correctly:

```
java -version
```

The Java version in the output should be displayed as 1.8.0_131.

6. Repeat steps 1 through 5 for each unique *products* shared volume on an appropriate host. For example: WCCHOST1 and WCCHOST2.

Starting the Infrastructure Installer on WCCHOST1

To start the installation program, perform the following steps.

1. Log in to WCCHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the following example:

```
$JAVA_HOME/bin/java -d64 -jar distribution_file_name.jar
```

In this example:

- Replace `JAVA_HOME` with the environment variable or actual JDK location on your system.
- Replace `distribution_file_name` with the actual name of the distribution JAR file.

If you download the distribution from the Oracle Technology Network (OTN), then the JAR file is typically packaged inside a downloadable compressed file.

To install the software required for the initial Infrastructure domain, the distribution you want to install is **fmw_12.2.1.3.0_infrastructure.jar**.

For more information about the actual file names of each distribution, see [Identifying and Obtaining Software Downloads for an Enterprise Deployment](#).

When the installation program appears, you are ready to begin the installation. See [Navigating the Installation Screens](#) for a description of each installation program screen.

Navigating the Infrastructure Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name or click the **Help** button on the screen.

Table 10-1 Navigating the Infrastructure Installation Screens

Screen	Description
Installation Inventory Setup	On UNIX operating systems, this screen appears if you are installing any Oracle product on this host for the first time. Specify the location where you want to create your central inventory. Ensure that the operating system group name selected on this screen has write permissions to the central inventory location. See Understanding the Oracle Central Inventory in <i>Oracle Fusion Middleware Installing Software with the Oracle Universal Installer</i>.  Note: Oracle recommends that you configure the central inventory directory on the products shared volume. Example: <code>/u01/oracle/products/oraInventory</code> You may also need to execute the <code>createCentralInventory.sh</code> script as root from the <code>oraInventory</code> folder after the installer completes.
Welcome	This screen introduces you to the product installer.
Auto Updates	Use this screen to search My Oracle Support automatically for available patches or automatically search a local directory for patches that you have already downloaded for your organization.
Installation Location	Use this screen to specify the location of your Oracle home directory. For the purposes of an enterprise deployment, enter the value of the <code>ORACLE_HOME</code> variable listed in Table 7-2 .
Installation Type	Use this screen to select the type of installation and as a consequence, the products and feature sets that you want to install. For this topology, select Fusion Middleware Infrastructure.  Note: The topology in this document does not include server examples. Oracle strongly recommends that you do not install the examples into a production environment.
Prerequisite Checks	This screen verifies that your system meets the minimum requirements. If there are any warning or error messages, refer to the Oracle Fusion Middleware System Requirements and Specifications document on the Oracle Technology Network (OTN).
Security Updates	If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates. If you do not have one and are sure that you want to skip this step, clear the check box and verify your selection in the follow-up dialog box.

Table 10-1 (Cont.) Navigating the Infrastructure Installation Screens

Screen	Description
Installation Summary	Use this screen to verify the installation options that you have selected. If you want to save these options to a response file, click Save Response File and provide the location and name of the response file. Response files can be used later in a silent installation situation. For more information about silent or command-line installation, see Using the Oracle Universal Installer in Silent Mode in <i>Oracle Fusion Middleware Installing Software with the Oracle Universal Installer</i> .
Installation Progress	This screen allows you to see the progress of the installation.
Installation Complete	This screen appears when the installation is complete. Review the information on this screen, then click Finish to dismiss the installer.

Installing Oracle Fusion Middleware Infrastructure on the Other Host Computers

If you have configured a separate shared storage volume or partition for secondary hosts, then you must install the Infrastructure on one of those hosts.

See [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#).

To install the software on the other host computers in the topology, log in to each host, and use the instructions in [Starting the Infrastructure Installer on WCCHOST1](#) and [Navigating the Infrastructure Installation Screens](#) to create the Oracle home on the appropriate storage device.

Note:

In previous releases, the recommended enterprise topology included a colocated set of Oracle HTTP Server instances. In those releases, there was a requirement to install the Infrastructure on the web tier hosts (WEBHOST1 and WEBHOST2). However, for this release, the Enterprise Deployment topology assumes that the web servers are installed and configured in standalone mode, so they are not considered part of the application tier domain. See [Configuring the Web Tier for an Enterprise Deployment](#)

Checking the Directory Structure

After you install the Oracle Fusion Middleware Infrastructure and create the Oracle home, you should see the directory and sub-directories listed in this topic. The contents of your installation vary based on the options that you selected during the installation.

To check the directory structure:

1. Change to the `ORACLE_HOME` directory where you installed the Infrastructure.

2. Enter the following command:

```
ls --format=single-column
```

The directory structure on your system must match the structure shown in the following example:

```
cfgtoollogs  
coherence  
em  
inventory  
OPatch  
oracle_common  
oraInst.loc  
oui  
wlserver
```

See [What are the Key Oracle Fusion Middleware Directories?](#) in *Understanding Oracle Fusion Middleware*.

Disabling the Derby Database

Disable the embedded Derby database, which is a file-based database, packaged with Oracle WebLogic Server. The Derby database is used primarily for development environments. As a result, you must disable it when you are configuring a production-ready enterprise deployment environment; otherwise, the Derby database process starts automatically when you start the Managed Servers.

To disable the Derby database:

1. Navigate to the following directory in the Oracle home:

```
cd WL_HOME/common/derby/lib
```
2. Rename the Derby library jar file:

```
mv derby.jar disable_derby.jar
```
3. If each host uses a separate file system, repeat steps 1 and 2 on each host.

Creating the Database Schemas

Oracle Fusion Middleware components require the existence of schemas in a database before you configure a Fusion Middleware Infrastructure domain. Install the schemas listed in this topic in a certified database for use with this release of Oracle Fusion Middleware.

- Metadata Services (MDS)
- Audit Services (IAU)
- Audit Services Append (IAU_APPEND)
- Audit Services Viewer (IAU_VIEWER)
- Oracle Platform Security Services (OPSS)
- User Messaging Service (UMS)
- WebLogic Services (WLS)

- Common Infrastructure Services (STB)

Use the Repository Creation Utility (RCU) to create the schemas. This utility is installed in the Oracle home for each Oracle Fusion Middleware product. For more information about RCU and how the schemas are created and stored in the database, see *Preparing for Schema Creation in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Complete the following steps to install the required schemas:

- [Installing and Configuring a Certified Database](#)
- [Starting the Repository Creation Utility \(RCU\)](#)
- [Navigating the RCU Screens to Create the Schemas](#)
- [Verifying Schema Access](#)

Installing and Configuring a Certified Database

Make sure that you have installed and configured a certified database, and that the database is up and running.

See the [Preparing the Database for an Enterprise Deployment](#).

Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Set the `JAVA_HOME` environment variable so it references the location where you installed a supported JDK.

See [File System and Directory Variables Used in This Guide](#).

2. Navigate to the following directory on WCCHOST1:

`ORACLE_HOME/oracle_common/bin`

3. Start RCU:

`./rcu`

Note:

If your database has Transparent Data Encryption (TDE) enabled, and you want to encrypt your tablespaces created by the RCU, provide the `-encryptTablespace true` option when you start the RCU.

This will default the appropriate RCU GUI Encrypt Tablespace checkbox selection on the Map Tablespaces screen without further effort during the RCU execution. See *Encrypting Tablespaces in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Navigating the RCU Screens to Create the Schemas

Follow the instructions in this section to create the schemas for the Fusion Middleware Infrastructure domain:

- [Task 1, Introducing RCU](#)
- [Task 2, Selecting a Method of Schema Creation](#)
- [Task 3, Providing Database Connection Details](#)
- [Task 4, Specifying a Custom Prefix and Selecting Schemas](#)
- [Task 5, Specifying Schema Passwords](#)
- [Task 6, Verifying the Tablespaces for the Required Schemas](#)
- [Task 7, Creating Schemas](#)
- [Task 8, Reviewing Completion Summary and Completing RCU Execution](#)

Task 1 Introducing RCU

Review the Welcome screen and verify the version number for RCU. Click **Next** to begin.

Task 2 Selecting a Method of Schema Creation

If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load** on the Create Repository screen. The procedure in this document assumes that you have the necessary privileges. If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option generates a SQL script, which can be provided to your database administrator. See Understanding System Load and Product Load in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*. Click **Next**.



Tip:

For more information about the options on this screen, see Create repository in *Creating Schemas with the Repository Creation Utility*.

Task 3 Providing Database Connection Details

Provide the database connection details for RCU to connect to your database.

1. In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.
2. Enter the **Port** number of the RAC database scan listener, for example 1521.
3. Enter the RAC **Service Name** of the database.
4. Enter the **User Name** of a user that has permissions to create schemas and schema objects, for example SYS.
5. Enter the **Password** of the user name that you provided in step 4.
6. If you have selected the SYS user, ensure that you set the role to SYSDBA.
7. Click **Next** to proceed, and then click **OK** on the dialog window confirming that connection to the database was successful.

 Tip:

For more information about the options on this screen, see Database Connection Details in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Task 4 Specifying a Custom Prefix and Selecting Schemas

1. Specify the custom prefix that you want to use to identify the Oracle Fusion Middleware schemas.

The custom prefix is used to logically group these schemas together for use in this domain. For the purposes of this guide, use the prefix FMW1221_

 Tip:

Make a note of the custom prefix that you choose to enter here; you need this later, during the domain creation process.

For more information about custom prefixes, see Understanding Custom Prefixes in *Creating Schemas with the Repository Creation Utility*.

2. Select **AS Common Schemas**.

When you select **AS Common Schemas**, all the schemas in this section are automatically selected.

If the schemas in this section are not automatically selected, then select the required schemas.

There are two mandatory schemas that are selected by default. You cannot deselect them: **Common Infrastructure Services** (the STB schema) and **WebLogic Services** (the WLS schema). The **Common Infrastructure Services** schema enables you to retrieve information from RCU during domain configuration. See Understanding the Service Table Schema in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

 Tip:

For more information about how to organize your schemas in a multi-domain environment, see Planning Your Schema Creation in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, and then click **OK** on the dialog window confirming that prerequisite checking for schema creation was successful.

Task 5 Specifying Schema Passwords

Specify how you want to set the schema passwords on your database, then specify and confirm your passwords. Ensure that the complexity of the passwords meet the database security requirements before you continue. RCU proceeds at this point even if you do not meet the password policies. Hence, perform this check outside RCU itself.

Click **Next**.

**Tip:**

You must make a note of the passwords you set on this screen; you need them later on during the domain creation process.

Task 6 Verifying the Tablespaces for the Required Schemas

You can accept the default settings on the remaining screens, or you can customize how RCU creates and uses the required tablespaces for the Oracle Fusion Middleware schemas.

**Note:**

You can configure a Fusion Middleware component to use JDBC stores for JMS servers and Transaction Logs, by using the Configuration Wizard. These JDBC stores are placed in the Weblogic Services component tablespace. If your environment expects to have a high level of transactions and JMS activity, you can increase the default size of the `<PREFIX>_WLS` tablespace to better suit the environment load.

Click **Next** to continue, and then click **OK** on the dialog window to confirm the tablespace creation.

For more information about RCU and its features and concepts, see *About the Repository Creation Utility* in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Task 7 Creating Schemas

Review the summary of the schemas to be loaded and click **Create** to complete schema creation.

**Note:**

If failures occurred, review the listed log files to identify the root cause, resolve the defects, and then use RCU to drop and recreate the schemas before you continue.

Task 8 Reviewing Completion Summary and Completing RCU Execution

When you reach the Completion Summary screen, verify that all schema creations have been completed successfully, and then click **Close** to dismiss RCU.

Verifying Schema Access

Verify schema access by connecting to the database as the new schema users are created by the RCU. Use SQL*Plus or another utility to connect, and provide the appropriate schema names and passwords entered in the RCU.

For example:

```
./sqlplus
```

```
SQL*Plus: Release 12.1.0.2.0 Production on Wed Mar 15 03:17:54 2017
```

Copyright (c) 1982, 2014, Oracle. All rights reserved.

```
Enter user-name: FMW1221_WLS
Enter password: WLS_schema_password
Last Successful login time: Tue Feb 28 2017 09:37:25 -07:00
```

```
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Real Application Clusters, Automatic Storage Management, OLAP, Advanced
Analytics and Real Application Testing options
```

```
SQL>
```

Configuring the Infrastructure Domain

You can create and configure a WebLogic domain for the enterprise deployment topology using the configuration wizard.

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

- [Starting the Configuration Wizard](#)
- [Navigating the Configuration Wizard Screens to Configure the Infrastructure Domain](#)

Starting the Configuration Wizard

To begin domain configuration, run the following command in the Oracle Fusion Middleware Oracle home on WCCHOST1.

```
ORACLE_HOME/oracle_common/common/bin/config.sh
```

Navigating the Configuration Wizard Screens to Configure the Infrastructure Domain

Follow the instructions in this section to create and configure the domain for the topology.

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Create a New Domain**.

In the **Domain Location** field, specify the value of the `ASERVER_HOME` variable, as defined in [File System and Directory Variables Used in This Guide](#).

Tip:

For more information about the other options on this screen of the Configuration Wizard, see "Configuration Type" in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Templates

On the Templates screen, make sure **Create Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Enterprise Manager - 12.2.1.2.0 [em]**

Selecting this template automatically selects the following dependencies:

- **Oracle JRF - 12.2.1.2.0 [oracle_common]**
- **WebLogic Coherence Cluster Extension - 12.2.1.2.0 [wlserver]**

Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Selecting the Application Home Location

On the Application Location screen, specify the value of the `APPLICATION_HOME` variable, as defined in [File System and Directory Variables Used in This Guide](#).

Tip:

More information about the options on this screen can be found in Application Location in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 4 Configuring the Administrator Account

On the Administrator Account screen, specify the user name and password for the default WebLogic Administrator account for the domain.

Make a note of the user name and password specified on this screen; you will need these credentials later to boot and connect to the domain's Administration Server.

Task 5 Specifying the Domain Mode and JDK

On the Domain Mode and JDK screen:

- Select **Production** in the **Domain Mode** field.
- Select the **Oracle Hotspot** JDK in the **JDK** field.

Selecting **Production Mode** on this screen gives your environment a higher degree of security, requiring a user name and password to deploy applications and to start the Administration Server.

 Tip:

More information about the options on this screen, including the differences between development mode and production mode, can be found in Domain Mode and JDK in *Creating WebLogic Domains Using the Configuration Wizard*.

In production mode, a boot identity file can be created to bypass the need to provide a user name and password when starting the Administration Server. For more information, see [Creating the boot.properties File](#).

Task 6 Specifying the Database Configuration Type

Select **RCU Data** to activate the fields on this screen.

The **RCU Data** option instructs the Configuration Wizard to connect to the database and Service Table (STB) schema to automatically retrieve schema information for the schemas needed to configure the domain.

 Note:

If you choose to select **Manual Configuration** on this screen, you will have to manually fill in the parameters for your schema on the JDBC Component Schema screen.

After selecting **RCU Data**, fill in the fields as shown in the following table. Refer to [#unique_146/unique_146_Connect_42_BABHHCBF](#) for a partial screen shot of a sample Database Configuration Type screen.

Field	Description
DBMS/Service	Enter the service name for the Oracle RAC database where you will install the product schemas. For example: orcl.example.com Be sure this is the common service name that is used to identify all the instances in the Oracle RAC database; do not use the host-specific service name.
Host Name	Enter the Single Client Access Name (SCAN) Address for the Oracle RAC database, which you entered in the <i>Enterprise Deployment Workbook</i> .
Port	Enter the port number on which the database listens. For example, 1521.
Schema Owner Schema Password	Enter the user name and password for connecting to the database's Service Table schema. This is the schema user name and password that was specified for the Service Table component on the Schema Passwords screen in RCU (see Creating the Database Schemas). The default user name is <i>prefix_STB</i> , where <i>prefix</i> is the custom prefix that you defined in RCU.

Click **Get RCU Configuration** when you are finished specifying the database connection information. The following output in the Connection Result Log indicates that the operation succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.

Click **Next** if the connection to the database is successful.

**Tip:**

More information about the **RCU Data** option can be found in "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*. More information about the other options on this screen can be found in Datasource Defaults in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 7 Specifying JDBC Component Schema Information

Verify that the values on the JDBC Component Schema screen are correct for all schemas.

The schema table should be populated because you selected **Get RCU Data** on the previous screen. As a result, the Configuration Wizard locates the database connection values for all the schemas required for this domain.

At this point, the values are configured to connect to a single-instance database. However, for an enterprise deployment, you should use a highly available Real Application Clusters (RAC) database, as described in [Preparing the Database for an Enterprise Deployment](#).

In addition, Oracle recommends that you use an Active GridLink datasource for each of the component schemas. For more information about the advantages of using GridLink data sources to connect to a RAC database, see "Database Considerations" in the *High Availability Guide*.

To convert the data sources to GridLink:

1. Select all the schemas by selecting the check box at in the first header row of the schema table.
2. Click **Convert to GridLink** and click **Next**.

Task 8 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information required to connect to the RAC database and component schemas, as shown in [Table 10-2](#) and in [#unique_146/unique_146_Connect_42_BABJBCFF](#).

Element	Description and Recommended Value
SCAN, Host Name, and Port	Select the SCAN check box. In the Host Name field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database. In the Port field, enter the SCAN listening port for the database (for example, 1521).

Element	Description and Recommended Value
ONS Host and Port	In the ONS Port field, enter the SCAN address for the Oracle RAC database. In the Port field, enter the ONS Remote port (typically, 6200).
Enable Fan	Select the Enable Fan check box to receive and process FAN events.

For more information about specifying the information on this screen, as well as information about how to identify the correct SCAN address, see "Configuring Active GridLink Data Sources with Oracle RAC" in the *High Availability Guide*. You can also click **Help** to display a brief description of each field on the screen.

Task 9 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

Tip:

More information about the other options on this screen can be found in Test Component Schema in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 10 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Administration Server**
This is required to properly configure the listen address of the Administration Server.
- **Node Manager**
This is required to configure Node Manager.
- **Topology**
This is required to configure the Managed Servers and cluster, and also for configuring the machine and targeting the Managed Servers to the machine.



Note:

When using the Advanced Configuration screen in the Configuration Wizard:

- If any of the above options are not available on the screen, then return to the Templates screen, and be sure you selected the required templates for this topology.
- Do not select the **Domain Frontend Host Capture** advanced configuration option. You will later configure the frontend host property for specific clusters, rather than for the domain.

Task 11 Configuring the Administration Server Listen Address

On the Administration Server screen:

1. In the **Server Name** field, retain the default value - AdminServer.
2. In the **Listen Address** field, enter the virtual host name that corresponds to the VIP of the ADMINVHN that you procured in [Procuring Resources for an Enterprise Deployment](#) and enabled in [Preparing the Host Computers for an Enterprise Deployment](#).

For more information on the reasons for using the ADMINVHN virtual host, see [Reserving the Required IP Addresses for an Enterprise Deployment](#).

3. Leave the other fields at their default values.

In particular, be sure that no server groups are assigned to the Administration Server.

Task 12 Configuring Node Manager

Select **Per Domain Default Location** as the Node Manager type, then specify the Node Manager credentials you will use to connect to the Node Manager.



Tip:

For more information about the options on this screen, see Node Manager in *Creating WebLogic Domains Using the Configuration Wizard*.

For more information about per domain and per host Node Manager implementations, see [About the Node Manager Configuration in a Typical Enterprise Deployment](#).

For additional information, see Configuring Node Manager on Multiple Machines in *Administering Node Manager for Oracle WebLogic Server*.

Task 13 Configuring Managed Servers

There are no Managed Servers in the initial Infrastructure domain. Click **Next** to proceed to the next screen.

Task 14 Configuring a Cluster

There are no clusters in the initial Infrastructure domain. Click **Next** to proceed to the next screen.

Task 15 Configure Server Templates

There are no server templates in the initial Infrastructure domain. Click **Next** to proceed to the next screen.

Task 16 Configure Coherence Clusters

There are no clusters in the initial Infrastructure domain. Click **Next** to proceed to the next screen.

Task 17 Creating Machines

Use the Machines screen to create a new machine in the domain. A machine is required in order for the Node Manager to be able to start and stop the servers.

1. Select the **Unix Machine** tab.
2. Click the **Add** button to create a new Unix machine.
Use the values in [Table 10-3](#) to define the Name and Node Manager Listen Address of the new machine.
3. Verify the port in the **Node Manager Listen Port** field.
The port number 5556, shown in this example, may be referenced by other examples in the documentation. Replace this port number with your own port number as needed.

Name	Node Manager Listen Address	Node Manager Listen Port
ADMINHOST	Enter the value of the ADMINVHN variable.	5556

 Tip:

More information about the options on this screen can be found in Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 18 Assigning Server To Machine

Complete the following steps:

1. Select admin server from the Server pane.
2. Select ADMINHOST from the Machines pane.
3. Click **Next** to proceed to the next screen.

Task 19 Reviewing Virtual Targets

Click **Next** to proceed to the next screen.

Task 20 Reviewing Partitions

Click **Next** to proceed to the next screen.

Task 21 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Create**.



Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 22 Monitoring Configuration Progress

After all the processes are complete, click **Next** to proceed to the next screen.

Task 23 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

Starting the Administration Server

After the domain is created, you can then perform the following tasks on WCCHOST1.

- [Starting the Node Manager in the Administration Server Domain Home on WCCHOST1](#)
Use these steps to start the per-domain Node Manager for the `ASERVER_HOME` domain directory.
- [Creating the boot.properties File](#)
You must create a `boot.properties` if you want to start the Administrator Server without being prompted for the Administrator Server credentials. This step is required in an enterprise deployment. When you start the Administration Server, the credentials that you enter in this file are encrypted.
- [Starting the Administration Server Using the Node Manager](#)
After you have configured the domain and configured the Node Manager, you can start the Administration Server by using the Node Manager. In an enterprise deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.
- [Validating the Administration Server](#)
Before you proceed with the configuration steps, validate that the Administration Server has started successfully by making sure that you have access to the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control; both of these are installed and configured on the Administration Servers.

Starting the Node Manager in the Administration Server Domain Home on WCCHOST1

Use these steps to start the per-domain Node Manager for the *ASERVER_HOME* domain directory.

1. Verify that the listen address in the `nodemanager.properties` file is set correctly.
 - a. Open the `nodemanager.properties` file for editing:

```
ASERVER_HOME/nodemanager/nodemanager.properties
```

- b. Make sure the `ListenAddress` property is set to the value of the ADMINVHN virtual IP address.
 - c. Make sure that `QuitEnabled` is set to 'true'. If this line is not present in the `nodemanager.properties` file, add the following line:

```
QuitEnabled=true
```

2. Change to the following directory:

```
ASERVER_HOME/bin
```

3. Start the Node Manager by entering the following command:

```
nohup ./startNodeManager.sh > ASERVER_HOME/nodemanager/nodemanager.out 2>&1 &
```

For more information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

Creating the boot.properties File

You must create a `boot.properties` if you want to start the Administrator Server without being prompted for the Administrator Server credentials. This step is required in an enterprise deployment. When you start the Administration Server, the credentials that you enter in this file are encrypted.

To create a `boot.properties` file for the Administration Server:

1. Create the following directory structure:

```
mkdir -p ASERVER_HOME/servers/AdminServer/security
```

2. In a text editor, create a file called `boot.properties` in the security directory that you created in the previous step, and enter the Administration Server credentials that you defined when you ran the Configuration Wizard to create the domain:

```
username=adminuser  
password=password
```

 Note:

When you start the Administration Server, the username and password entries in the file are encrypted.

For security reasons, minimize the amount of time the entries in the file are left unencrypted; after you edit the file, you should start the server as soon as possible so that the entries are encrypted.

3. Save the file and close the editor.

Starting the Administration Server Using the Node Manager

After you have configured the domain and configured the Node Manager, you can start the Administration Server by using the Node Manager. In an enterprise deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

To start the Administration Server by using the Node Manager:

1. Start the WebLogic Scripting Tool (WLST):

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

2. Connect to Node Manager by using the Node Manager credentials:

```
wls:/
offline>nmConnect('nodemanager_username','nodemanager_password',
                  'ADMINVHN','5556','domain_name',
                  'ASERVER_HOME')
```

 Note:

This user name and password are used only to authenticate connections between Node Manager and clients. They are independent of the server administrator ID and password and are stored in the `nm_password.properties` file located in the following directory:

`ASERVER_HOME/config/nodemanager`

3. Start the Administration Server:

```
nmStart('AdminServer')
```

**Note:**

When you start the Administration Server, it attempts to connect to Oracle Web Services Manager for WebServices policies. It is expected that the WSM-PM Managed Servers are not yet started, and so, the following message appears in the Administration Server log:

```
<Warning><oracle.wsm.resources.policymanager>  
<WSM-02141><Unable to connect to the policy access service  
due to Oracle WSM policy manager host server being down.>
```

4. Exit WLST:

```
exit()
```

Validating the Administration Server

Before you proceed with the configuration steps, validate that the Administration Server has started successfully by making sure that you have access to the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control; both of these are installed and configured on the Administration Servers.

To navigate to Fusion Middleware Control, enter the following URL, and log in with the Oracle WebLogic Server administrator credentials:

```
ADMINVHN:7001/em
```

To navigate to the Oracle WebLogic Server Administration Console, enter the following URL, and log in with the same administration credentials:

```
ADMINVHN:7001/console
```

Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group

When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Server authentication provider (DefaultAuthenticator). However, for an enterprise deployment, Oracle recommends that you use a dedicated, centralized LDAP-compliant authentication provider.

The following topics describe how to use the Oracle WebLogic Server Administration Console to create a new authentication provider for the enterprise deployment domain. This procedure assumes that you have already installed and configured a supported LDAP directory, such as Oracle Unified Directory or Oracle Internet Directory.

- [About the Supported Authentication Providers](#)
- [About the Enterprise Deployment Users and Groups](#)
- [Prerequisites for Creating a New Authentication Provider and Provisioning Users and Groups](#)
- [Provisioning a Domain Connector User in the LDAP Directory](#)

- [Creating the New Authentication Provider](#)
- [Provisioning an Enterprise Deployment Administration User and Group](#)
- [Adding the Administration Role to the New Administration Group](#)
- [Updating the boot.properties File and Restarting the System](#)

About the Supported Authentication Providers

Oracle Fusion Middleware supports a variety of LDAP authentication providers. See Identity Store Types and WebLogic Authenticators in *Securing Applications with Oracle Platform Security Services*.

The instructions in this guide assume that you are using one of the following providers:

- Oracle Unified Directory
- Oracle Internet Directory
- Microsoft Active Directory



Note:

By default, the instructions here describe how to configure the identity service instance to support querying against a single LDAP identity store with an unencrypted connection.

If the connection to your identity provider has to be secured through SSL, then additional keystone configuration is required for role management in the Enterprise Manager Fusion Middleware Control to function correctly. For additional configuration information, see Doc ID 1670789.1 at support.oracle.com.

Also, you can configure the service to support a virtualized identity store, which queries multiple LDAP identity stores, by using LibOVD.

For more information about configuring a Multi-LDAP lookup, refer to Configuring the Identity Store Service in *Securing Applications with Oracle Platform Security Services*.

About the Enterprise Deployment Users and Groups

The following topics provide important information on the purpose and characteristics of the enterprise deployment administration users and groups.

- [About Using Unique Administration Users for Each Domain](#)
- [About the Domain Connector User](#)
- [About Adding Users to the Central LDAP Directory](#)
- [About Product-Specific Roles and Groups for Oracle WebCenter Content](#)
- [Example Users and Groups Used in This Guide](#)

About Using Unique Administration Users for Each Domain

When you use a central LDAP user store, you can provision users and groups for use with multiple Oracle WebLogic Server domains. As a result, there is a possibility that one WebLogic administration user can have access to all the domains within an enterprise.

It is a best practice to create and assign a unique distinguished name (DN) within the directory tree for the users and groups that you provision for the administration of your Oracle Fusion Middleware domains.

For example, if you plan to install and configure an Oracle WebCenter Content enterprise deployment domain, then create a user called **weblogic_wcc** and an administration group called **WCCAdministrators**.

About the Domain Connector User

Oracle recommends that you create a separate domain connector user (for example, **wccLDAP**) in your LDAP directory. This user allows the domain to connect to the LDAP directory for the purposes of user authentication. It is recommended that this user be a non-administrative user.

In a typical Oracle Identity and Access Management deployment, you create this user in the **systemids** container. This container is used for system users that are not normally visible to users. Placing the user into the **systemids** container ensures that customers who have Oracle Identity Governance do not reconcile this user.

A few products, such as IPM require the domain connector user to have the permission to modify data of the LDAP directory. If such products are included, then the domain connector user should be the administrative user.

About Adding Users to the Central LDAP Directory

After you configure a central LDAP directory to be the authenticator for the enterprise domain, then you should add all new users to the new authenticator and not to the default WebLogic Server authenticator.

To add new users to the central LDAP directory, you cannot use the WebLogic Administration Console. Instead, you must use the appropriate LDAP modification tools, such as **ldapbrowser** or **JXplorer**.

When you are using multiple authenticators (a requirement for an enterprise deployment), login and authentication will work, but role retrieval will not. The role is retrieved from the first authenticator only. If you want to retrieve roles using any other authenticator, then you must enable virtualization for the domain.

To enable virtualization:

1. Browse to the Fusion Middleware Control, and log in with the administrative credentials.

`http://adminvhn:7001/em`
2. Navigate to **WebLogic Domain > Security > Security Provider Configuration**.
3. Expand **Security Store Provider**.
4. Expand **Identity Store Provider**.

5. Click **Configure**.
6. Add a custom property.
7. Select property `virtualize` with value `true` and click **OK**.
8. Select property `user.create.bases`, example value used in this guide is `cn=users,dc=example,dc=com`.
9. Select property `group.create.bases`, example value used in this guide is `cn=groups,dc=example,dc=com`.
10. Click **OK** again to persist the change.
11. Restart the Administration Server and all managed servers.

For more information about the `virtualize` property, see *OPSS System and Configuration Properties in Oracle Fusion Middleware Securing Applications with Oracle Platform Security Services*.

About Product-Specific Roles and Groups for Oracle WebCenter Content

Each Oracle Fusion Middleware product implements its own predefined roles and groups for administration and monitoring.

As a result, as you extend the domain to add additional products, you can add these product-specific roles to the `WCCAdministrators` group. After they are added to the `WCCAdministrators` group, each product administrator user can administer the domain with the same set of privileges for performing administration tasks.

For instructions on adding additional roles to the `WCCAdministrators` group, see [Common Configuration and Management Tasks for an Enterprise Deployment](#).

Example Users and Groups Used in This Guide

In this guide, the examples assume that you provision the following administration user and group with the following DNS:

- Admin User DN:
`cn=weblogic_wcc,cn=users,dc=example,dc=com`
- Admin Group DN:
`cn=WCCAdministrators,cn=groups,dc=example,dc=com`
- Product-specific LDAP Connector User:
`cn=WCCLDAP,cn=systemids,dc=example,dc=com`

This is the user that you use to connect WebLogic Managed Servers to the LDAP authentication provider. This user must have permissions to read and write to the Directory Trees:

```
cn=users,dc=example,dc=com
cn=groups,dc=example,dc=com
```

 Note:

This user needs to be granted membership in the following groups to provide read and write access:

```
cn=orclFAUserReadPrivilegeGroup,cn=groups,dc=example,dc=com  
cn=orclFAUserWritePrivilegeGroup,cn=groups,dc=example,dc=com  
cn=orclFAGroupReadPrivilegeGroup,cn=groups,dc=example,dc=com  
cn=orclFAGroupWritePrivilegeGroup,cn=groups,dc=example,dc=com
```

Prerequisites for Creating a New Authentication Provider and Provisioning Users and Groups

Before you create a new LDAP authentication provider, back up the relevant configuration files:

```
ASERVER_HOME/config/config.xml  
ASERVER_HOME/config/fmwconfig/jps-config.xml  
ASERVER_HOME/config/fmwconfig/system-jazn-data.xml
```

In addition, back up the `boot.properties` file for the Administration Server in the following directory:

```
ASERVER_HOME/servers/AdminServer/security
```

- [Backing up the Configuration](#)
- [Enabling Authentication Provider Virtualization](#)

Backing up the Configuration

Before you create a new LDAP authentication provider, back up the relevant configuration files:

```
ASERVER_HOME/config/config.xml  
ASERVER_HOME/config/fmwconfig/jps-config.xml  
ASERVER_HOME/config/fmwconfig/system-jazn-data.xml
```

In addition, back up the `boot.properties` file for the Administration Server in the following directory:

```
ASERVER_HOME/servers/AdminServer/security
```

Enabling Authentication Provider Virtualization

When you are using multiple authenticators (a requirement for an enterprise deployment), login and authentication will work, but role retrieval will not. The role is retrieved from the first authenticator only. If you want to retrieve roles using any other authenticator, then you must enable virtualization for the domain.

To enable virtualization:

1. Sign-in to the Fusion Middleware Control by using the administrator's account. For example: weblogic.
`http://adminvhn:7001/em`
2. Click **WebLogic Domain > Security > Security Provider Configuration**.
3. Expand **Security Store Provider**.
4. Expand **Identity Store Provider**.
5. Click **Configure**.
6. Add a custom property.
7. Select property **virtualize** with value **true** and click **OK**.
8. Click **OK** again to persist the change.
9. Restart the Administration Server and all managed servers.

For more information about the virtualize property, see OPSS System and Configuration Properties in *Oracle Fusion Middleware Securing Applications with Oracle Platform Security Services*.

Provisioning a Domain Connector User in the LDAP Directory

This example shows how to create a user called wccLDAP in the central LDAP directory.

To provision the user in the LDAP provider:

1. Create an LDIF file named `domain_user.ldif` with the following contents and then save the file:

```
dn: cn=wccLDAP,cn=systemids,dc=example,dc=com
changetype: add
orclsamaccountname: wccLDAP
userpassword: password
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
mail: wccLDAP@example.com
givenname: wccLDAP
sn: wccLDAP
cn: wccLDAP
uid: wccLDAP
```

 Note:

If you use Oracle Unified Directory, then add the following four group memberships to the end of the LDIF file to grant the appropriate read/write privileges:

```
dn:
cn=orclFAUserReadPrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wccLDAP,cn=systemids,dc=example,dc=com

dn:
cn=orclFAGroupReadPrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wccLDAP,cn=systemids,dc=example,dc=com

dn:
cn=orclFAUserWritePrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wccLDAP,cn=systemids,dc=example,dc=com

dn:
cn=orclFAGroupWritePrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wccLDAP,cn=systemids,dc=example,dc=com
```

2. Provision the user in the LDAP directory.

For example, for an Oracle Unified Directory LDAP provider:

```
OID_INSTANCE_HOME/bin/ldapmodify -a \
    -h idstore.example.com
    -D "cn=oudadmin" \
    -w password \
    -p 1389 \
    -f domain_user.ldif
```

For Oracle Internet Directory:

```
OID_ORACLE_HOME/bin/ldapadd -h idstore.example.com \
    -p 3060 \
    -D cn="orcladmin" \
    -w password \
    -c \
    -v \
    -f domain_user.ldif
```

Creating the New Authentication Provider

To configure a new LDAP-based authentication provider:

1. Log in to the WebLogic Server Administration Console.
2. Click **Security Realms** in the left navigational bar.
3. Click the **myrealm** default realm entry.
4. Click the **Providers** tab.

Note that there is a DefaultAuthenticator provider configured for the realm. This is the default WebLogic Server authentication provider.

Authentication Providers

New Delete Reorder Showing 1 to 3 of 3 Previous | Next

☐	Name	Description	Version
☐	Trust Service Identity Asserter	Trust Service Identity Assertion Provider	1.0
☐	DefaultAuthenticator	WebLogic Authentication Provider	1.0
☐	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

New Delete Reorder Showing 1 to 3 of 3 Previous | Next

5. Click **Lock & Edit** in the Change Center.
6. Click the **New** button below the **Authentication Providers** table.
7. Enter a name for the provider.

Use one of the following names, based on the LDAP directory service that you plan to use as your credential store:

- OUDAuthenticator for Oracle Unified Directory
- OIDAuthenticator for Oracle Internet Directory
- OVDAuthenticator for Oracle Virtual Directory

8. Select the authenticator type from the **Type** drop-down list.

Select one of the following types, based on the LDAP directory service that you plan to use as your credential store:

- OracleUnifiedDirectoryAuthenticator for Oracle Unified Directory
- OracleInternetDirectoryAuthenticator for Oracle Internet Directory
- OracleVirtualDirectoryAuthenticator for Oracle Virtual Directory

9. Click **OK** to return to the Providers screen.
10. On the Providers screen, click the newly created authenticator in the table.
11. Select **SUFFICIENT** from the **Control Flag** drop-down menu.

 Control Flag:

Save

SUFFICIENT
REQUIRED
REQUISITE
SUFFICIENT
OPTIONAL

Setting the control flag to **SUFFICIENT** indicates that if the authenticator can successfully authenticate a user, then the authenticator should accept that authentication and should not continue to invoke any additional authenticators.

If the authentication fails, it falls through to the next authenticator in the chain. Make sure all subsequent authenticators also have their control flags set to **SUFFICIENT**; in particular, check the **DefaultAuthenticator** option and make sure that its control flag is set to **SUFFICIENT**.

12. Click **Save** to save the control flag settings.
13. Click the **Provider Specific** tab and enter the details specific to your LDAP server, as shown in the following table.

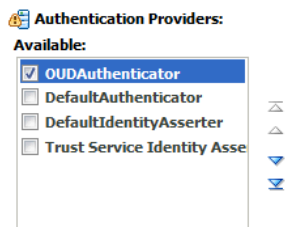
Note that only the required fields are discussed in this procedure. For information about all the fields on this page, consider the following resources:

- To display a description of each field, click **Help** on the **Provider Specific** tab.
- For more information on setting the **User Base DN**, **User From Name Filter**, and **User Attribute** fields, see *Configuring Users and Groups in the Oracle Internet Directory and Oracle Virtual Directory Authentication Providers in Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

Parameter	Sample Value	Value Description
Host	For example: idstore.example.com	The LDAP server's server ID.
Port	For example: 1389	The LDAP server's port number.
Principal	For example: cn=wccLDAP, cn=systemids,dc=example,dc=com	The LDAP user DN used to connect to the LDAP server.
Credential	Enter LDAP password.	The password used to connect to the LDAP server.
SSL Enabled	Unchecked (clear)	Specifies whether SSL protocol is used when connecting to the LDAP server.
User Base DN	For example: cn=users,dc=example,dc=com	Specify the DN under which your users start.
All Users Filter	(&(uid=*)(objectclass=person))	Instead of a default search criteria for All Users Filter, search all users based on the uid value. If the User Name Attribute for the user object class in the LDAP directory structure is a type other than uid, then change that type in the User From Name Filter field. For example, if the User Name Attribute type is cn, then this field should be set to: (&(cn=*)(objectclass=person)))

Parameter	Sample Value	Value Description
User From Name Filter	For example: ((&(uid=%u)(objectclass=person)))	If the User Name Attribute for the user object class in the LDAP directory structure is a type other than uid, then change that type in the settings for the User From Name Filter . For example, if the User Name Attribute type is cn, then this field should be set to: ((&(cn=%u)(objectclass=person))).
User Name Attribute	For example: uid	The attribute of an LDAP user object that specifies the name of the user.
Group Base DN	For example: cn=groups,dc=example,dc=com	Specify the DN that points to your Groups node.
Use Retrieved User Name as Principal	Checked	Must be turned on.
GUID Attribute	entryuuid	This value is prepopulated with entryuuid when OracleUnifiedDirectoryAuthenticator is used for OUD. Check this value if you use Oracle Unified Directory as your authentication provider.

14. Click **Save** to save the changes.
15. Click **Security Realms** in the right navigation pane, and then click the default realm name (**myrealm**), and then **Providers** to return to the Providers page.
16. Click **Reorder**, and then use the resulting page to make the Provider you just created first in the list of authentication providers.



17. Click **OK**.
18. On the Providers Page, click **DefaultAuthenticator**.
19. From the Control Flag drop-down, select **SUFFICIENT**.
20. Click **Save** to update the DefaultAuthenticator settings.
21. In the Change Center, click **Activate Changes**.
22. Restart the Administration Server.

To stop and start the Administration Server using the Node Manager:

- a. Start WLST:

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

- b. Connect to Node Manager using the Node Manager credentials you defined in when you created the domain in the Configuration Wizard:

```
wls:/offline>nmConnect('nodemanager_username','nodemanager_password',
                      'ADMINVHN','5556','domain_name',
                      'ASERVER_HOME')
```

- c. Stop the Administration Server:

```
nmKill('AdminServer')
```

- d. Start the Administration Server:

```
nmStart('AdminServer')
```

- e. Exit WLST:

```
exit()
```

23. After the restart, review the contents of the following log file:

```
ASERVER_HOME/servers/AdminServer/logs/AdminServer.log
```

Verify that no LDAP connection errors occurred. For example, look for errors such as the following:

```
The LDAP authentication provider named "OUDAuthenticator" failed to make
connection to ldap server at ...
```

If you see such errors in the log file, then check the authorization provider connection details to verify that they are correct and try saving and restarting the Administration Server again.

24. After you restart and verify that no LDAP connection errors are in the log file, try browsing the users and groups that exist in the LDAP provider:

In the Administration Console, navigate to the **Security Realms > myrealm > Users and Groups** page. You should be able to see all users and groups that exist in the LDAP provider structure.

Provisioning an Enterprise Deployment Administration User and Group

This example shows how to create a user called **weblogic_wcc** and a group called **WCCAdministrators**.

To provision the administration user and group in LDAP provider:

1. Create an LDIF file named `admin_user.ldif` with the following contents and then save the file:

```
dn: cn=weblogic_wcc,cn=users,dc=example,dc=com
changetype: add
orclsamaccountname: weblogic_wcc
userpassword: password
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
mail: weblogic_wcc@example.com
givenname: weblogic_wcc
```

```
sn: weblogic_wcc
cn: weblogic_wcc
uid: weblogic_wcc
```

2. Provision the user in the LDAP directory.

For example, for an Oracle Unified Directory LDAP provider:

```
OID_INSTANCE_HOME/bin/ldapmodify -a \
    -h idstore.example.com
    -D "cn=oudadmin" \
    -w password \
    -p 1389 \
    -f admin_user.ldif
```

For Oracle Internet Directory:

```
OID_ORACLE_HOME/bin/ldapadd -h idstore.example.com \
    -p 3060 \
    -D cn="orcladmin" \
    -w password \
    -c \
    -v \
    -f admin_user.ldif
```

3. Create an LDIF file named admin_group.ldif with the following contents and then save the file:

```
dn: cn=WCCAdministrators,cn=Groups,dc=example,dc=com
displayname: WCCAdministrators
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=weblogic_wcc,cn=users,dc=example,dc=com
cn: WCCAdministrators
uniquemember: cn=wccLDAP, cn=systemids, dc=example, dc=com
cn: WCCAdministrators
description: Administrators Group for the Oracle WebCenter Content
Domain
```

4. Provision the group in the LDAP Directory.

For Oracle Unified Directory:

```
OID_INSTANCE_HOME/bin/ldapmodify -a \
    -D "cn=oudadmin" \
    -h oudhost.example.com \
    -w password \
    -p 1380 \
    -f admin_group.ldif
```

For Oracle Internet Directory:

```
OID_ORACLE_HOME/bin/ldapadd -h oidhost.example.com \
    -p 3060 \
    -D cn="orcladmin" \
    -w password \
    -c \
    -v \
    -f admin_group.ldif
```

5. Verify that the changes were made successfully:
 - a. Log in to the Oracle WebLogic Server Administration Console.
 - b. In the left pane of the console, click **Security Realms**.
 - c. Click the default security realm (**myrealm**).
 - d. Click the **Users and Groups** tab.
 - e. Verify that the administrator user and group that you provisioned are listed on the page.

Adding the Administration Role to the New Administration Group

After you add the users and groups to Oracle Internet Directory, the group must be assigned the Administration role within the WebLogic domain security realm. This enables all users that belong to the group to be administrators for the domain.

To assign the Administration role to the new enterprise deployment administration group:

1. Log in to the WebLogic Administration Server Console by using the administration credentials that you provided in the Configuration Wizard.
Do not use the credentials for the administration user that you created and provided for the new authentication provider.
2. In the left pane of the Administration Console, click **Security Realms**.
3. Click the default security realm (**myrealm**).
4. Click the **Roles and Policies** tab.
5. Expand the **Global Roles** entry in the table and click **Roles**.

Figure 10-1 Global Roles Under Security Realms

⊕ Domain
⊖ Global Roles
⊕ Roles
⊕ JCOM

6. Click the **Admin** role.

Figure 10-2 Adding Conditions for the Admin Role

Role Name ↕	Provider Name
Admin	XACMLRoleMapper

7. Click **Add conditions**.
8. Select **Group** from the **Predicate List** drop-down menu, and then click **Next**.
9. Enter WCCAdministrators in the **Group Argument Name** field, and then click **Add**.

WCCAdministrators is added to the list box of arguments.

10. Click **Finish** to return to the Edit Global Role page.

The WCCAdministrators group is now listed.

11. Click **Save** to finish adding the **Admin** Role to the WCCAdministrators group.
12. Validate that the changes were made by logging in to the WebLogic Administration Server Console by using the new `weblogic_wcc` user credentials.

If you can log in to the Oracle WebLogic Server Administration Console and Fusion Middleware Control with the credentials of the new administration user that you just provisioned in the new authentication provider, then you have configured the provider successfully.

Updating the boot.properties File and Restarting the System

After you create the new administration user and group, you must update the Administration Server `boot.properties` file with the administration user credentials that you created in the LDAP directory:

1. On WCCHOST1, go the following directory:
`ASERVER_HOME/servers/AdminServer/security`
2. Rename the existing `boot.properties` file:
`mv boot.properties boot.properties.backup`
3. Use a text editor to create a file called `boot.properties` under the security directory.
4. Enter the following lines in the file:
`username=weblogic_wcc`
`password=password`
5. Save the file.
6. Restart the Administration Server.

Configuring the Web Tier for an Enterprise Deployment

It is important to understand how to install and configure a standalone Oracle HTTP Server domain that contains two Oracle HTTP Server instances: one on WEBHOST1 and one on WEBHOST2.

This chapter provides information on variables used when configuring the web tier and installing and configuring a web tier domain.

- [Variables Used When Configuring the Web Tier](#)
While configuring the web tier, you will be referencing the directory variables listed in this section.
- [About the Web Tier Domains](#)
In an enterprise deployment, each Oracle HTTP Server instance is configured on a separate host and in its own standalone domain. This allows for a simple configuration that requires a minimum amount of configuration and a minimum amount of resources to run and maintain.
- [Installing a Supported JDK](#)
- [Installing Oracle HTTP Server on WEBHOST1](#)
It is important to understand the procedure for installing the Oracle HTTP Server software on the web tier.
- [Creating a Web Tier Domain on WEBHOST1](#)
It is essential to understand how to create a new Oracle HTTP Server standalone domain on the first Web tier host.
- [Installing and Configuring a Web Tier Domain on WEBHOST2](#)
After you install Oracle HTTP Server and configure a Web Tier domain on WEBHOST1, then you must also perform the same tasks on WEBHOST2.
- [Starting the Node Manager and Oracle HTTP Server Instances on WEBHOST1 and WEBHOST2](#)
It is important to understand how to start the Oracle HTTP Server instances on WEBHOST1 and WEBHOST2.
- [Configuring Oracle HTTP Server to Route Requests to the Application Tier](#)
It is important to understand how to update the Oracle HTTP Server configuration files so that the web server instances route requests to the servers in the domain.

Variables Used When Configuring the Web Tier

While configuring the web tier, you will be referencing the directory variables listed in this section.

The values for several directory variables are defined in [File System and Directory Variables Used in This Guide](#).

- `OHS_ORACLE_HOME`
- `OHS_DOMAIN_HOME`

In addition, you'll be referencing the following virtual IP (VIP) address and host names:

- ADMINVHN
- WEBHOST1
- WEBHOST2

About the Web Tier Domains

In an enterprise deployment, each Oracle HTTP Server instance is configured on a separate host and in its own standalone domain. This allows for a simple configuration that requires a minimum amount of configuration and a minimum amount of resources to run and maintain.

For more information about the role and configuration of the Oracle HTTP Server instances in the web tier, see [Understanding the Web Tier](#).

Installing a Supported JDK

Oracle Fusion Middleware requires that a certified Java Development Kit (JDK) is installed on your system.

- [Locating and Downloading the JDK Software](#)
- [Installing the JDK Software](#)

Oracle Fusion Middleware requires you to install a certified Java Development Kit (JDK) on your system.

Locating and Downloading the JDK Software

To find a certified JDK, see the certification document for your release on the Oracle Fusion Middleware Supported System Configurations page.

After you identify the Oracle JDK for the current Oracle Fusion Middleware release, you can download an Oracle JDK from the following location on Oracle Technology Network:

<http://www.oracle.com/technetwork/java/index.html>

Be sure to navigate to the download for the Java SE JDK.

Installing the JDK Software

Oracle Fusion Middleware requires you to install a certified Java Development Kit (JDK) on your system.

You must install the JDK in the following locations:

On the local storage device for each of the Web tier host computers. The Web tier host computers, which reside in the DMZ, do not necessarily have access to the shared storage on the application tier.

See the [Understanding the Recommended Directory Structure for an Enterprise Deployment](#).

To install JDK 1.8.0_131:

1. Change directory to the location where you downloaded the JDK archive file.

```
cd download_dir
```

2. Unpack the archive into the JDK home directory, and then run the following commands:

```
tar -xzf jdk-8u131-linux-x64.tar.gz
```

Note that the JDK version listed here was accurate at the time this document was published. For the latest supported JDK, see the *Oracle Fusion Middleware System Requirements and Specifications* for the current Oracle Fusion Middleware release.

3. Move the JDK directory to the recommended location in the directory structure.

For example:

```
mv ./jdk1.8.0_131 /u02/oracle/products/jdk
```

See [File System and Directory Variables Used in This Guide](#).

4. Define the `JAVA_HOME` and `PATH` environment variables for running Java on the host computer.

For example:

```
export JAVA_HOME=/u02/oracle/products/jdk
export PATH=$JAVA_HOME/bin:$PATH
```

5. Run the following command to verify that the appropriate java executable is in the path and your environment variables are set correctly:

```
java -version
```

The Java version in the output should be displayed as 1.8.0_131.

Installing Oracle HTTP Server on WEBHOST1

It is important to understand the procedure for installing the Oracle HTTP Server software on the web tier.

- [Starting the Installer on WEBHOST1](#)
- [Navigating the Oracle HTTP Server Installation Screens](#)
- [Verifying the Oracle HTTP Server Installation](#)

Starting the Installer on WEBHOST1

To start the installation program, perform the following steps.

1. Log in to WEBHOST1.
2. Go to the directory in which you downloaded the installation program.
3. Enter the following command to launch the installation program:

```
./fmw_12.2.1.3.0_ohs_linux64.bin
```

When the installation program appears, you are ready to begin the installation.

Navigating the Oracle HTTP Server Installation Screens

The following table lists the screens in the order that the installation program displays them.

If you need additional help with any of the installation screens, click the screen name.

Table 11-1 Oracle HTTP Server Installation Screens

Screen	Description
Installation Inventory Setup	On UNIX operating systems, this screen appears if you install any Oracle product on this host for the first time. Specify the location where you want to create your central inventory. Ensure that the operating system group name selected on this screen has write permissions to the central inventory location. See <i>Understanding the Oracle Central Inventory in Oracle Fusion Middleware Installing Software with the Oracle Universal Installer</i>.
	 Note: Oracle recommends that you configure the central inventory directory within the products directory. Example: /u02/oracle/products/oraInventory You may also need to execute the <code>createCentralInventory.sh</code> script as root from the <code>oraInventory</code> folder after the installer completes.
Welcome	This screen introduces you to the product installer.
Auto Updates	Use this screen to automatically search My Oracle Support for available patches or automatically search the local directory for patches that you have already downloaded for your organization.
Installation Location	Use this screen to specify the location of your Oracle home directory. For the purposes of an enterprise deployment, enter the value of the <code>WEB_ORACLE_HOME</code> variable listed in Table 7-3.

Table 11-1 (Cont.) Oracle HTTP Server Installation Screens

Screen	Description
Installation Type	Select Standalone HTTP Server (Managed independently of WebLogic server) . This installation type allows you to configure the Oracle HTTP Server instances independently from any other existing Oracle WebLogic Server domains.
JDK Selection	For the value of JDK Home, enter the value of <i>JAVA_HOME</i> that you set when installing the JDK software.
Prerequisite Checks	This screen verifies that your system meets the minimum necessary requirements. If there are any warning or error messages, verify that your host computers and the required software meet the system requirements and certification information described in Host Computer Hardware Requirements and Operating System Requirements for the Enterprise Deployment Topology .
Installation Summary	Use this screen to verify the installation options that you selected. If you want to save these options to a response file, click Save Response File and provide the location and name of the response file. Response files can be used later in a silent installation situation. See Using the Oracle Universal Installer in Silent Mode in <i>Oracle Fusion Middleware Installing Software with the Oracle Universal Installer</i> .
Installation Progress	This screen allows you to see the progress of the installation.
Installation Complete	This screen appears when the installation is complete. Review the information on this screen, then click Finish to close the installer.

Verifying the Oracle HTTP Server Installation

Verify that the Oracle HTTP Server installation completed successfully by validating the `WEB_ORACLE_HOME` folder contents.

Run the following command to compare the installed folder structure with the following list:

```
ls --format=single-column WEB_ORACLE_HOME
```

The following files and directories are listed in the Oracle HTTP Server Oracle Home:

```
bin
cdata
cfgtoollogs
crs
css
cv
has
```

```
install
inventory
jlib
ldap
lib
network
nls
ohs
OPatch
oracle_common
oracore
oraInst.loc
oui
perl
plsql
plugins
precomp
QOPatch
racg
rdbms
slax
sqlplus
srvm
webgate
wlserver
xdk
```

Creating a Web Tier Domain on WEBHOST1

It is essential to understand how to create a new Oracle HTTP Server standalone domain on the first Web tier host.

- [Starting the Configuration Wizard on WEBHOST1](#)
- [Navigating the Configuration Wizard Screens for an Oracle HTTP Server Domain](#)

Starting the Configuration Wizard on WEBHOST1

To start the Configuration Wizard, navigate to the following directory and start the WebLogic Server Configuration Wizard, as follows:

```
cd WEB_ORACLE_HOME/oracle_common/common/bin
./config.sh
```

Navigating the Configuration Wizard Screens for an Oracle HTTP Server Domain

Oracle recommends that you create a standalone domain for the Oracle HTTP Server instances on each web tier host.

The following topics describe how to create a new standalone Oracle HTTP Server domain:

- Task 1, Selecting the Domain Type and Domain Home Location
- Task 2, Selecting the Configuration Templates
- Task 3, Selecting the JDK for the Web Tier Domain.
- Task 4, Configuring System Components
- Task 5, Configuring OHS Server
- Task 7, Reviewing Your Configuration Specifications and Configuring the Domain
- Task 8, Writing Down Your Domain Home

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Create a new domain**.

In the **Domain Location** field, enter the value assigned to the `WEB_DOMAIN_HOME` variable.

Note the following:

- The Configuration Wizard creates the new directory that you specify here.
- Create the directory on local storage, so the web servers do not have any dependencies on storage devices outside the DMZ.

Task 2 Selecting the Configuration Templates

On the Templates screen, select **Oracle HTTP Server (Standalone) - 12.2.1.3.0 [ohs]**.

Tip:

More information about the options on this screen can be found in Templates in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Selecting the JDK for the Web Tier Domain.

Select the Oracle HotSpot JDK installed in the `/u02/oracle/products/jdk` directory prior to the Oracle HTTP Server installation.

Task 4 Configuring System Components

On the System Components screen, configure one Oracle HTTP Server instance. The screen should, by default, have a single instance defined. This is the only instance that you need to create.

1. The default instance name in the **System Component** field is `ohs1`. Use this default name when you configure `WEBHOST1`.
2. Make sure that OHS is selected in the **Component Type** field.
3. If an application is not responding, use the **Restart Interval Seconds** field to specify the number of seconds to wait before you attempt a restart if an application is not responding.
4. Use the **Restart Delay Seconds** field to specify the number of seconds to wait between restart attempts.

Task 5 Configuring OHS Server

Use the OHS Server screen to configure the OHS servers in your domain:

1. Select **ohs1** from the **System Component** drop-down menu.
2. In the **Listen Address** field, enter *WEBHOST1*.
All the remaining fields are prepopulated, but you can change the values as required for your organization. See OHS Server in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.
3. In the **Server Name** field, verify the value of the listen address and listen port.
It should appear as follows:

`http://WEBHOST1:7777`

Task 6 Configuring Node Manager

Select **Per Domain Default Location** as the Node Manager type, and specify the user name and password for the Node Manager.

Note:

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

For information about Node Manager configuration, see Configuring Node Manager on Multiple Machines in *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

Task 7 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains detailed configuration information for the domain that you are about to create. Review the details of each item on the screen and verify that the information is correct.

If you need to make any changes, you can go back to any previous screen either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation does not begin until you click **Create**.

In the Configuration Progress screen, click **Next** when it finishes.

Tip:

More information about the options on this screen can be found in Configuration Summary in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 8 Writing Down Your Domain Home

The Configuration Success screen shows the domain home location.

Make a note of the information provided here, as you need it to start the servers and access the Administration Server.

Click **Finish** to close the Configuration Wizard.

Installing and Configuring a Web Tier Domain on WEBHOST2

After you install Oracle HTTP Server and configure a Web Tier domain on WEBHOST1, then you must also perform the same tasks on WEBHOST2.

1. Log in to WEBHOST2 and install Oracle HTTP Server, using the instructions in [Installing Oracle HTTP Server on WEBHOST1](#).
2. Configure a new standalone domain on WEBHOST2, using the instructions in [Creating a Web Tier Domain on WEBHOST1](#).

Use the name ohs2 for the instance on WEBHOST2, and be sure to replace all occurrences of WEBHOST1 with WEBHOST2 and all occurrences of ohs1 with ohs2 in each of the examples.

Starting the Node Manager and Oracle HTTP Server Instances on WEBHOST1 and WEBHOST2

It is important to understand how to start the Oracle HTTP Server instances on WEBHOST1 and WEBHOST2.

- [Starting the Node Manager on WEBHOST1 and WEBHOST2](#)
- [Starting the Oracle HTTP Server Instances](#)

Starting the Node Manager on WEBHOST1 and WEBHOST2

Before you can start the Oracle HTTP Server instances, you must start the Node Manager on WEBHOST1 and WEBHOST2:

1. Log in to WEBHOST1 and navigate to the following directory:
`WEB_DOMAIN_HOME/bin`
2. Start the Node Manager as shown in the following sections by using `nohup` and `nodemanager.out` as an example output file:
`nohup WEB_DOMAIN_HOME/bin/startNodeManager.sh > WEB_DOMAIN_HOME/nodemanager/nodemanager.out 2>&1 &`
3. Log in to WEBHOST2 and perform steps 1 and 2.

See Advanced Node Manager Configuration in *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

Starting the Oracle HTTP Server Instances

To start the Oracle HTTP Server instances:

1. Navigate to the following directory on WEBHOST1:
`WEB_DOMAIN_HOME/bin`

For more information about the location of the WEB_DOMAIN_HOME directory, see [File System and Directory Variables Used in This Guide](#).

2. Enter the following command:

```
./startComponent.sh ohs1
```

 Note:

Every time you start the Oracle HTTP server, you will be asked for the Node Manager password. If you do not wish this behaviour, then use the following command the first time you start the Oracle HTTP server:

```
./startComponent.sh ohs1 storeUserConfig
```

This time when you enter the Node Manager password, it will be encrypted and stored. Future start and stop of the Oracle HTTP server will not require you to enter the Node Manager password.

3. When prompted, enter the Node Manager password.
4. Repeat steps 1 through 3 to start the ohs2 instance on WEBHOST2. See Starting Oracle HTTP Server Instances in *Administering Oracle HTTP Server*.

Configuring Oracle HTTP Server to Route Requests to the Application Tier

It is important to understand how to update the Oracle HTTP Server configuration files so that the web server instances route requests to the servers in the domain.

- [About the Oracle HTTP Server Configuration for an Enterprise Deployment](#)
- [Modifying the httpd.conf File to Include Virtual Host Configuration Files](#)
- [Creating the Virtual Host Configuration Files](#)
- [Validating the Virtual Server Configuration on the Load Balancer](#)
- [Configuring Routing to the Administration Server](#)
- [Turning On the WebLogic Server Plug-In Enabled Flag](#)
- [Setting the Front-End URL for the Administration Console and Setting Redirection Preferences](#)
- [Validating Access to the Management Consoles and Administration Server](#)

About the Oracle HTTP Server Configuration for an Enterprise Deployment

The following topics provide overview information about the changes that are required to the Oracle HTTP Server configuration files in an enterprise deployment.

- [Purpose of the Oracle HTTP Server Virtual Hosts](#)
- [Recommended Structure of the Oracle HTTP Server Configuration Files](#)

Purpose of the Oracle HTTP Server Virtual Hosts

The reference topologies in this guide require that you define a set of virtual servers on the hardware load balancer. You can then configure Oracle HTTP Server to recognize requests to specific virtual hosts (that map to the load balancer virtual servers) by adding `<VirtualHost>` directives to the Oracle HTTP Server instance configuration files.

For each Oracle HTTP Server virtual host, you define a set of specific URLs (or context strings) that route requests from the load balancer through the Oracle HTTP Server instances to the appropriate Administration Server or Managed Server in the Oracle WebLogic Server domain.

Recommended Structure of the Oracle HTTP Server Configuration Files

Rather than adding multiple virtual host definitions to the `httpd.conf` file, Oracle recommends that you create separate, smaller, and more specific configuration files for each of the virtual servers required for the products that you are deploying. This avoids populating an already large `httpd.conf` file with additional content, and it can make troubleshooting configuration problems easier.

For example, in a typical Oracle Fusion Middleware Infrastructure domain, you can add a specific configuration file called `admin_vh.conf` that contains the virtual host definition for the Administration Server virtual host (ADMINVHN).

Modifying the `httpd.conf` File to Include Virtual Host Configuration Files

Perform the following tasks to prepare the `httpd.conf` file for the additional virtual hosts required for an enterprise topology:

1. Log in to WEBHOST1.
2. Locate the `httpd.conf` file for the first Oracle HTTP Server instance (ohs1) in the domain directory:

```
cd WEB_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/
```

3. Verify if the `httpd.conf` file has the appropriate configuration as follows:
 - a. Run the following command to verify the `ServerName` parameter, be sure that it is set correctly, substituting the correct value for the current WEBHOST n :

```
grep "ServerName http" httpd.conf
ServerName http://WEBHOST1:7777
```

- b. Run the following command to verify there is an include statement that includes all `*.conf` files from the `moduleconf` subdirectory:

```
grep moduleconf httpd.conf
IncludeOptional "moduleconf/*.conf"
```

- c. If either validation fails to return results, or returns results that are commented out, open the `httpd.conf` file in a text editor and make the required changes in the appropriate locations.

```
#
# ServerName gives the name and port that the server uses to
# identify itself.
# This can often be determined automatically, but we recommend
# you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP
# address here.
#
ServerName http://WEBHOST1:7777
# and at the end of the file:
# Include the admin virtual host (Proxy Virtual Host) related
# configuration
include "admin.conf"
IncludeOptional "moduleconf/*.conf"
```

- d. Save the `httpd.conf` file.
4. Log in to `WEBHOST2` and perform steps 2 and 3 for the `httpd.conf` file, replacing any occurrences of `WEBHOST1` or `ohs1` with `WEBHOST2` or `ohs2` in the instructions as necessary.

Creating the Virtual Host Configuration Files

To create the virtual host configuration files:



Note:

Before you create the virtual host configuration files, be sure that you have configured the virtual servers on the load balancer, as described in [Purpose of the Oracle HTTP Server Virtual Hosts](#).

1. Log in to `WEBHOST1` and change directory to the configuration directory for the first Oracle HTTP Server instance (`ohs1`):

```
cd WEB_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf
```

2. Create the `admin_vh.conf` file and add the following directive:

```
<VirtualHost WEBHOST1:7777>
  ServerName admin.example.com:80
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>
```

3. Create the `wccinternal_vh.conf` file and add the following directive:

```
<VirtualHost WEBHOST1:7777>
  ServerName wccinternal.example.com:80
  ServerAdmin you@your.address
```

```

RewriteEngine On
RewriteOptions inherit
</VirtualHost>

```

4. Restart the ohs1 instance:
 - a. Change directory to the following location:


```
cd WEB_DOMAIN_HOME/bin
```
 - b. Enter the following commands to stop and start the instance; provide the node manager password when prompted:


```
./stopComponent.sh ohs1
./startComponent.sh ohs1
```
5. Copy the admin_vh.conf file and the wccinternal_vh.conf file to the configuration directory for the second Oracle HTTP Server instance (ohs2) on WEBHOST2:


```
WEB_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf
```
6. Edit the admin_vh.conf and wccinternal_vh.conf files and change any references from WEBHOST1 to WEBHOST2 in the <VirtualHost> directives.
7. Restart the ohs2 instance:
 - a. Change directory to the following location:


```
cd WEB_DOMAIN_HOME/bin
```
 - b. Enter the following commands to stop and start the instance:


```
./stopComponent.sh ohs2
./startComponent.sh ohs2
```

Validating the Virtual Server Configuration on the Load Balancer

From the load balancer, access the following URLs to ensure that your load balancer and Oracle HTTP Server are configured properly. These URLs should show the initial Oracle HTTP Server 12c web page.

- <http://admin.example.com/index.html>
- <http://wccinternal.example.com/index.html>

Configuring Routing to the Administration Server

To enable Oracle HTTP Server to route to the Administration Server, you must add a set of <Location> directives to the Oracle HTTP Server admin_vh.conf configuration file:

1. Log in to WEBHOST1, and change directory to the following location:


```
cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
```
2. Add the following directives to the admin_vh.conf file within the <VirtualHost> tags:


```
# Admin Server and EM
<Location /console>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
</Location>
```

```
<Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>
```

```
<Location /em>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>
```

The `admin_vh.conf` file should appear as it does in [Example 11-1](#).

3. Restart the `ohs1` instance:
 - a. Change directory to the following location:


```
cd OHS_DOMAIN_HOME/bin
```
 - b. Enter the following commands to stop and start the instance:


```
./stopComponent.sh ohs1
./startComponent.sh ohs1
```
4. Copy the `admin_vh.conf` file to the configuration directory for the second Oracle HTTP Server instance (`ohs2`) on `WEBHOST2`:


```
OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf/
```
5. Edit the `admin_vh.conf` file and change any references of `WEBHOST1` to `WEBHOST2` in the `<VirtualHost>` directives.
6. Restart the `ohs2` instance:
 - a. Change directory to the following location:


```
cd OHS_DOMAIN_HOME/bin
```
 - b. Enter the following commands to stop and start the instance:


```
./stopComponent.sh ohs2
./startComponent.sh ohs2
```

Example 11-1 Sample Contents of the `admin_vh.conf` File

```
<VirtualHost WEBHOST1:7777>
    ServerName admin.example.com:7777
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

# Admin Server and EM
<Location /console>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

<Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>
```

```
<Location /em>
  SetHandler weblogic-handler
  WebLogicHost ADMINVHN
  WebLogicPort 7001
</Location>
</VirtualHost>
```

Turning On the WebLogic Server Plug-In Enabled Flag

For security purposes, and since the load balancer terminates SSL requests (Oracle HTTP Server routes the requests as non-SSL to WebLogic Server), once you configure SSL for the load balancer, turn on the WebLogic Server plug-in enabled flag for the domain. To turn on the WebLogic Server plug-in enabled flag:

1. Log in to the Administration Console.
2. Click the domain name in the navigation tree on the left.
3. Open the **Web Applications** tab.
4. Click **Lock & Edit**.
5. Select the **WebLogic Plugin Enabled** checkbox.
6. Click **Save** and then click **Activate Changes**.
7. Restart the Administration Server (even if the Administration Console does not specifically prompt for that):
 - a. Start the Oracle WebLogic Scripting Tool (WLST):

```
cd ORACLE_COMMON_HOME/common/bin

./wlst.sh
```

- b. In the WLST shell, connect to Node Manager with the `nmConnect` command and the Node Manager credentials (make sure Node Manager is up and running), and start the Node Manager using `nmStart`:

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"ADMINVHN", "domain_name", "ASERVER_HOME")

wls:/nm/domain_name>nmStart("AdminServer")
```

The values of `node_admin_user` and `node_admin_password` are the Node Manager credentials.

- c. Stop the Administration Server, using either the Administration Console or, as follows, the WLST `nmKill` command:
- d. Start the Administration Server using `nmStart`:

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"WCCHOST1", "5556", "domain_name", "ASERVER_HOME")
```



```
wls:/nm/domain_name/nmStart("AdminServer")
```

Setting the Front-End URL for the Administration Console and Setting Redirection Preferences

When you access the WebLogic Server Administration Console using a load balancer, you must change the Administration Server's front-end URL so that the user's web browser is redirected to the appropriate load-balancer address.

The WebLogic Server Administration Console application tracks changes made to ports, channels and security using the console. When changes made through the console are activated, the console validates its current listen address, port and protocol. If the listen address, port and protocol are still valid, the console redirects the HTTP request, replacing the host and port information with the Administration Server's listen address and port.

To change the Administration Server's front-end URL:

1. Log in to the WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the **Domain Structure** tree on the left.
4. Click **Servers**.
5. On the Summary of Servers page, click **Admin Server** in the **Names** column of the table.
6. On the settings page for Administration Server, click the **Protocols** tab.
7. Click the **HTTP** tab.
8. Set the **Frontend Host** field to `admin.example.com` and the **Frontend HTTP Port** field to 80 (modify accordingly if HTTPS is used for the admin URL).
9. Save and activate the changes.
10. Restart the Administration Server for changes to the front-end host directive to take effect.

Validating Access to the Management Consoles and Administration Server

To verify the changes that you have made in this chapter:

1. Use the following URL to the hardware load balancer to display the Oracle WebLogic Server Administration Console, and log in by using the Oracle WebLogic Server administrator credentials:

```
http://admin.example.com/console
```

This validates that the `admin.example.com` virtual host on the load balancer is able to route requests to the Oracle HTTP Server instances on the web tier, which in turn can route requests for the Oracle WebLogic Server Administration Console to the Administration Server in the application tier.

2. Similarly, you should be able to access the Fusion Middleware Control by using a similar URL:

`http://admin.example.com/em`

Extending the Domain to Include Oracle WebCenter Content

You need to perform certain tasks in order to extend the enterprise deployment domain with the Oracle WebCenter Content software. This includes installing the WebCenter Content, extending the domain for WebCenter Content and completing post-configuration and verification tasks.

This chapter provides information on installing the WebCenter Content, extending the domain for WebCenter Content and completing post-configuration and verification tasks.

- [Installing WebCenter Content for an Enterprise Deployment](#)
The procedure for installing WebCenter Content in an enterprise deployment domain is explained in this section.
- [Creating the Oracle WebCenter Content Database Schemas](#)
Before you can configure an Oracle WebCenter Content domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.
- [Extending the Domain for WebCenter Content](#)
You need to perform the following tasks in order to extend the existing enterprise deployment domain with the Oracle WebCenter Content software.
- [Completing Postconfiguration and Verification Tasks for WebCenter Content](#)
Several configuration and validation steps must be performed to bring the content servers online. Complete the following sections in the order listed.
- [Configuring Content Server for the WebCenter Content User Interface](#)
If you are planning to use the WebCenter Content user interface (in addition to the native user interface for Content Server), you need to enable the Content Server parameters.
- [Configuring Oracle HTTP Server for the WebCenter Content Cluster](#)
The instructions for configuring Oracle HTTP Server for the WebCenter Content Cluster are available in this section.
- [Enabling JDBC Persistent Stores](#)
Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an oracle database and makes resources available for all the servers in the cluster.
- [Enabling Automatic Service Migration](#)
To ensure high availability for the product installed in this chapter, you must configure service migration appropriately.

Installing WebCenter Content for an Enterprise Deployment

The procedure for installing WebCenter Content in an enterprise deployment domain is explained in this section.

This section contains the following procedures.

- [Starting the Installation Program](#)
- [Navigating the Installation Screens](#)
- [Installing Oracle WebCenter Content on the Other Host Computers](#)
- [Verifying the Installation](#)

Starting the Installation Program

To start the installation program:

1. Log in to WCCHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the example below.

```
JAVA_HOME/bin/java -d64 -jar fmw_12.2.1.3.0_wccontent.jar
```

Be sure to replace the JDK location in these examples with the actual JDK location on your system.

When the installation program appears, you are ready to begin the installation.

Navigating the Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

Screen	Description
Installation Inventory Screen	If you did not create a central inventory when you installed the Oracle Fusion Middleware Infrastructure software, then this dialog box appears. Edit the Inventory Directory field so it points to the location of your local inventory, and then click OK .
Welcome	This screen introduces you to the product installer.
Auto Updates	Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization.
Installation Location	Use this screen to specify the location of your Oracle home directory. For more information about Oracle Fusion Middleware directory structure, see "Selecting Directories for Installation and Configuration" in <i>Planning an Installation of Oracle Fusion Middleware</i> .

Screen	Description
Prerequisite Checks	This screen verifies that your system meets the minimum necessary requirements. If there are any warning or error messages, you can refer to one of the documents in the Roadmap for Verifying Your System Environment section in <i>Planning Your Oracle Fusion Middleware Infrastructure Installation</i> .
Installation Summary	Use this screen to verify the installation options you selected. Click Install to begin the installation.
Installation Progress	This screen allows you to see the progress of the installation. Click Next when the progress bar reaches 100% complete.
Installation Complete	Review the information on this screen, then click Finish to dismiss the installer.

Installing Oracle WebCenter Content on the Other Host Computers

If you have followed the EDG shared storage recommendations, there is a separate shared storage volume for product installations on WCCHOST2, and you must also install the software on WCCHOST2. See [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#).

Verifying the Installation

After you complete the installation, you can verify it by successfully completing the following tasks.

- [Reviewing the Installation Log Files](#)
- [Checking the Directory Structure](#)
- [Viewing the Contents of Your Oracle Home](#)

Reviewing the Installation Log Files

Review the contents of the installation log files to make sure that no problems were encountered. For a description of the log files and where to find them, see Understanding Installation Log Files in *Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

Checking the Directory Structure

The contents of your installation vary based on the options you selected during the installation.

The addition of Oracle WebCenter Content will add the following directory and sub-directories:

```
/u01/oracle/products/fmw/wccontent
axf
common
ipm
plugins
ucm
```

```
wccadf
wccadfrui

/u01/oracle/products/fmw/wccapture
capture
common
plugins
```

For more information about the directory structure you should see after installation, see "What are the Key Oracle Fusion Middleware Directories?" in *Understanding Oracle Fusion Middleware*.

Viewing the Contents of Your Oracle Home

You can also view the contents of your Oracle home by using the `viewInventory` script. See Viewing the contents of an Oracle home in *Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

Creating the Oracle WebCenter Content Database Schemas

Before you can configure an Oracle WebCenter Content domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.

Follow the instructions in this section to install the schemas.

- [Starting the Repository Creation Utility \(RCU\)](#)
- [Navigating the RCU Screens to Create the Schemas](#)

Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Navigate to the `ORACLE_HOME/oracle_common/bin` directory on your system.
2. Make sure that the `JAVA_HOME` environment variable is set to the location of a certified JDK on your system. The location should be up to but not including the `bin` directory. For example, if your JDK is located in `/u01/oracle/products/jdk`:

On UNIX operating systems:

```
export JAVA_HOME=/u01/oracle/products/jdk
```

3. Start RCU:

On UNIX operating systems:

```
./rcu
```

**Note:**

If your database has Transparent Data Encryption (TDE) enabled, and you want to encrypt your tablespaces that are created by the RCU, provide the `-encryptTablespace true` option when you start RCU.

This defaults the appropriate RCU GUI Encrypt Tablespace checkbox selection on the Map Tablespaces screen without further effort during the RCU execution. See *Encrypting Tablespaces in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Navigating the RCU Screens to Create the Schemas

After you start the RCU, you can then use the wizard screens to select and install the required schemas for your Oracle Fusion Middleware product. Schema creation involves the following tasks.

Task 1 Introducing RCU

Click **Next**.

Task 2 Selecting a Method of Schema Creation

If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have the necessary privileges.

If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option will generate a SQL script, which can be provided to your database administrator. See "Understanding System Load and Product Load" in *Creating Schemas with the Repository Creation Utility*.

Task 3 Providing Database Connection Details

Provide the database connection details for RCU to connect to your database.

1. In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.
2. Select **Connection Parameters**.
3. Enter the **DBMS/Service** details.
4. Enter the **Schema Owner** and **Schema Password** details.
5. Click **Next** to proceed, then click **OK** on the dialog window confirming that connection to the database was successful.

Task 4 Specifying a Custom Prefix and Selecting Schemas

Select **existing prefix**, and select the prefix you created while configuring the initial domain.

From the list of schemas, select the **WebCenter Content** schema. This will automatically select the following schemas as dependencies:

- **Oracle WebCenter Content Imaging**
- **Oracle WebCenter Content Server - Complete**
- **Oracle WebCenter Enterprise Capture**

- **Oracle WebCenter Content Server - Search Only**

The custom prefix is used to logically group these schemas together for use in this domain only; you must create a unique set of schemas for each domain as schema sharing across domains is not supported.



Tip:

For more information about custom prefixes, see "Understanding Custom Prefixes" in *Creating Schemas with the Repository Creation Utility*.
For more information about how to organize your schemas in a multi-domain environment, see "Planning Your Schema Creation" in *Creating Schemas with the Repository Creation Utility*.



Tip:

You must make a note of the custom prefix you choose to enter here; you will need this later on during the domain creation process.

Click **Next** to proceed, then click **OK** in the dialog window confirming that prerequisite checking for schema creation was successful.

Task 5 Specifying Schema Passwords

Specify how you want to set the schema passwords on your database, then specify and confirm your passwords.



Tip:

You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

Task 6 Verifying the Tablespaces for the Required Schemas

On the Map Tablespaces screen, review the information, and then click **Next** to accept the default values.

Click **OK** in the confirmation dialog box.

Task 7 Completing Schema Creation

Navigate through the remainder of the RCU screens to complete schema creation. When you reach the Completion Summary screen, click **Close** to dismiss RCU.

Task 8 Verifying the Schema Creation

To verify that the schemas were created successfully, and to verify the database connection details, use SQL*Plus or another utility to connect to the database, using the OCS schema name and the password you provided.

For example:

```
./sqlplus
```

```
SQL*Plus: Release 12.1.0.1.0 Production on Tue Mar 7 00:28:06 2017
```


Copyright (c) 1982, 2013, Oracle. All rights reserved.

Enter user-name: FMW12213

Enter password:

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production
With the Partitioning, Real Application Clusters, Automatic Storage Management,
OLAP,
Advanced Analytics and Real Application Testing options

SQL> exit

Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 -
64bit Production
With the Partitioning, Real Application Clusters, Automatic Storage Management,
OLAP,
Advanced Analytics and Real Application Testing options

Extending the Domain for WebCenter Content

You need to perform the following tasks in order to extend the existing enterprise deployment domain with the Oracle WebCenter Content software.

Extending the domain involves the following tasks.

- [Starting the Configuration Wizard](#)
Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.
- [Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Content](#)

Starting the Configuration Wizard

Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.

Note:

If you added any customizations directly to the start scripts in the domain, those are overwritten by the configuration wizard. To customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it, for example, add custom libraries to the WebLogic Server classpath, specify Additional JAVA command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the **pack** and **unpack** commands.

To start the Configuration Wizard:

1. From the WebLogic Server Console, stop any managed servers that are modified by this domain extension. Managed Servers that are not effected can remain on-line.

2. For any managed servers to be modified, verify that the managed server shutdown has completed.
3. Stop the Administration Server once all managed servers are in a steady state.
4. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Content

Follow the instructions in the following sections to extend the domain for the topology with static or dynamic clusters.

- [Extending the Domain with Static Clusters](#)
- [Extending the Domain with Dynamic Clusters](#)

Extending the Domain with Static Clusters

Follow the instructions in this section to extend the domain for the topology with static clusters.



Note:

You can use the procedure described in this section to extend an existing domain with static clusters. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain extension and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Configuring High Availability Options](#)
- [Task 4, Specifying the Database Configuration Type](#)
- [Task 5, Specifying JDBC Component Schema Information](#)
- [Task 6, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 7, Testing the JDBC Connections](#)
- [Task 8, Selecting Advanced Configuration](#)
- [Task 9, Configuring Managed Servers](#)
- [Task 10, Configuring a Cluster](#)
- [Task 11, Assigning Server Templates](#)
- [Task 12, Configuring Dynamic Servers](#)
- [Task 13, Assigning Managed Servers to the Cluster](#)

- [Task 14, Configuring Coherence Clusters](#)
- [Task 15, Creating Machines for WebCenter Content Servers](#)
- [Task 16, Assigning Servers to Machines](#)
- [Task 17, Configuring Virtual Targets](#)
- [Task 18, Configuring Partitions](#)
- [Task 19, Configuring the File Store](#)
- [Task 20, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 21, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 22, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration domain home you created as part of the initial domain.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).

Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wcccontent]**

In addition, the following additional templates should already be selected, because they were used to create the initial Infrastructure domain:

- **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
- **Oracle JRF - 12.2.1.3.0 [oracle_common]**
- **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**

Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Configuring High Availability Options

This screen appears for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. After you select HA Options for a cluster, all subsequent clusters that are added to the domain by using the Configuration Wizard,

automatically apply HA options (that is, the Configuration Wizard creates the JDBC stores and configures ASM for them).

On the High Availability Options screen:

- Select **Enable Automatic Service Migration** with **Database Basis**.
- Set **JTA Transaction Log Persistence** to **JDBC TLog Store**.
- Set **JMS Server Persistence** to **JMS JDBC Store**.



Note:

Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an Oracle database and makes resources available for all the servers in the cluster. So, the Configuration Wizard steps assume that the JDBC persistent stores are used along with Automatic Service Migration.

When you choose JDBC persistent stores, additional unused File Stores are automatically created but are not targeted to your clusters. Ignore these File Stores.

If, for any reason, you want to use File Stores, you can retain the default values for TLOGs and JMS persistent store options in this screen and configure them in a shared location later. See [Task 8, Selecting Advanced Configuration](#). Shared location is required to resume JMS and HA in a failover scenario.

You can also configure TLOGs and JMS persistent stores manually in a post step. For information about the differences between JDBC and File Stores, and for specific instructions to configure them manually, see [Using Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#).

Click **Next**.

Task 4 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring the Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.

 Tip:

For more information about the **RCU Data** option, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.

For more information about the other options on this screen, see "Datasource Defaults" in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 5 Specifying JDBC Component Schema Information

On the JDBC Component Schema screen, select all the UCM schemas (for WebCenter Content) in the table.

When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.

Click **Convert to GridLink** and click **Next**.

Task 6 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information that is required to connect to the RAC database and component schemas, as shown in the following table.

Element	Description and Recommended Value
SCAN, Host Name, and Port	Select the SCAN check box. In the Host Name field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database. In the Port field, enter the SCAN listening port for the database (for example, 1521)
ONS Host and Port	In the ONS Host field, enter the SCAN address for the Oracle RAC database. In the Port field, enter the ONS Remote port (typically, 6200).
Enable Fan	Verify that the Enable Fan check box is selected, so the database can receive and process FAN events.

Task 7 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

 Tip:

For more information about the other options on this screen, see "Test Component Schema" in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 8 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File Store**

Task 9 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server for Oracle WebCenter Content appears in the list of servers.

Perform the following tasks to modify the default Oracle WebCenter Content Managed Server and create a second Managed Server:

1. Rename the default Managed Server to WLS_WCC1.
2. Click **Add** to create a new Managed Server and name it WLS_WCC2.

 Tip:

The server names recommended here will be used throughout this document; if you choose different names, be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Oracle WebCenter Content Managed Server.

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WLS_WCC1	WCCHOST1	16200	Unchecked	Disabled	UCM-MGD-SVR
WLS_WCC2	WCCHOST2	16200	Unchecked	Disabled	UCM-MGD-SVR

 Tip:

More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 10 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle WebCenter Content software.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify WCC_Cluster in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select Unspecified.

 Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to Considerations for Choosing Unicast or Multicast in *Administering Clusters for Oracle WebLogic Server*.

 Tip:

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 11 Assigning Server Templates

Click **Next** to proceed to the next screen.

Task 12 Configuring Dynamic Servers

Verify that all dynamic server options are disabled for clusters that are to remain as static clusters.

1. Confirm that the **Dynamic Cluster**, **Calculated Listen Port**, and **Calculated Machine Names** checkboxes on this screen are unchecked.
2. Confirm the **Server Template** selection is **Unspecified**.
3. Click **Next**.

Task 13 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign WLS_WCC1 and WLS_WCC2 to the new cluster, WCC_Cluster:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, WCC_Cluster.
2. In the Servers pane, assign WLS_WCC1 to WCC_Cluster by doing one of the following:
 - Click once on the WLS_WCC1 Managed Server to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
 - Double-click on WLS_WCC1 to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign WLS_WCC2 to WCC_Cluster.
4. Click **Next** to proceed to the next screen.

 Tip:

More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 14 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Update the port number value to **9991**.

**Note:**

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 15 Creating Machines for WebCenter Content Servers

If required, use the Machines screen to add two new Unix Machines:

1. On the Unix Machines tab, click the **Add** button.
2. Enter WCCHOST1 in the **Name** field.
3. Enter the host name of WCCHOST1 for the Node Manage Listener address. Leave the Node Manager port to the default value of 5556.
4. Repeat the above steps for WCCHOST2.

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain, as shown in the following table. Click **Next** to proceed.

Name	Node Manager Listen Address	Node Manager Listen Port
WCCHOST1	The value of the WCCHOST1 host name variable. For example, WCCHOST1.example.com.	5556
WCCHOST2	The value of the WCCHOST2 host name variable. For example, WCCHOST2.example.com.	5556
ADMINHOST	Enter the value of the ADMINVHN variable.	5556

Task 16 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Oracle WebCenter Content Managed Servers you just created to the corresponding machines in the domain. Use a similar process as when assigning managed servers to the cluster. See [Task 13, Assigning Managed Servers to the Cluster](#).

Assign ADMINVHN to ADMINHOST.

Assign WLS_WCC1 to WCCHOST1, and assign WLS_WCC2 to WCCHOST2.

**Tip:**

More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 17 Configuring Virtual Targets

Click **Next** to proceed to the next screen.

Task 18 Configuring Partitions

Click **Next** to proceed to the next screen.

Task 19 Configuring the File Store

In the File Stores screen, assign the following directory for each of the WebCenter Content Persistence stores including Content Server JMS file stores:

`ORACLE_RUNTIME/domain_name/WCC_Cluster/jms`

 Note:

Create the `jms` folder before starting the managed servers.

In this example, replace `ORACLE_RUNTIME` with the value of the variable for your environment. Replace `WCC_Cluster` with the name you assigned to the WebCenter Content cluster.

Select **Direct-Write** from the drop-down list for **Synchronous Write Policy** (for both the stores).

Task 20 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Click **Update** to execute the domain extension.

 Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 21 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

Task 22 Start the Administration Server

Start the Administration Server, login, and then verify the clusters and servers views to ensure that the changes made to the domain have been applied.

After you have completed extending the domain with static clusters, go to [Completing Postconfiguration and Verification Tasks for WebCenter Content](#).

Extending the Domain with Dynamic Clusters

Follow the instructions in this section to extend the domain for the topology with dynamic clusters.



Note:

This procedure assumes that you are extending an existing domain. If your needs do not match the instructions given in the procedure, ensure that you make your selections accordingly, or refer to the supporting documentation for additional details.

Domain extension and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Configuring High Availability Options](#)
- [Task 4, Specifying the Database Configuration Type](#)
- [Task 5, Specifying JDBC Component Schema Information](#)
- [Task 6, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 7, Testing the JDBC Connections](#)
- [Task 8, Selecting Advanced Configuration](#)
- [Task 9, Configuring Managed Servers](#)
- [Task 10, Configuring a Cluster](#)
- [Task 11, Assigning Server Templates](#)
- [Task 12, Configuring Dynamic Servers](#)
- [Task 13, Configuring Coherence Clusters](#)
- [Task 14, Creating Machines for WebCenter Content Servers](#)
- [Task 15, Assigning Servers to Machines](#)
- [Task 16, Configuring Virtual Targets](#)
- [Task 17, Configuring Partitions](#)
- [Task 18, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 19, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 20, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the ASERVER_HOME variable, which represents the complete path to the Administration domain home you created as part of the initial domain.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).

 Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]**

In addition, the following additional templates should already be selected, because they were used to create the initial Infrastructure domain:

- **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
- **Oracle JRF - 12.2.1.3.0 [oracle_common]**
- **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**

 Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Configuring High Availability Options

This screen appears for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. After you select HA Options for a cluster, all subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply these HA options.

On the High Availability Options screen, complete the following steps:

1. Verify that **Enable Automatic Service Migration** is not selected.
2. Verify that Default Persistent Store is selected as the **JTA Transaction Log Persistence** option.
3. Select JDBC Store as the **JMS Service Persistence** option.

You can configure only JMS Server persistence for Dynamic Clusters by using the Configuration Wizard. You cannot configure Service Migration and JTA Transaction Logs Persistence for Dynamic Clusters by using the Configuration Wizard; you have to configure them manually. Instructions are covered in later chapters of this guide.

 Note:

Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an Oracle database and makes resources available for all the servers in the cluster. So, the Configuration Wizard steps assume that the JDBC persistent stores are used along with Automatic Service Migration. When you choose JDBC persistent stores, additional unused File Stores are automatically created but are not targeted to your clusters. Ignore these File Stores.

If, for any reason, you want to use File Stores, you can retain the default values for TLOGs and JMS persistent store options in this screen and configure them in a shared location later. See [Task 8, Selecting Advanced Configuration](#). Shared location is required to resume JMS and HA in a failover scenario.

You can also configure TLOGs and JMS persistent stores manually in a post step. For information about the differences between JDBC and File Stores, and for specific instructions to configure them manually, see [Using Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#).

Click **Next**.

Task 4 Specifying the Database Configuration Type

1. On the Database Configuration Type screen, select **RCU Data**.
All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.
2. Verify and ensure that credentials in all the fields are the same that you have provided while configuring the Oracle Fusion Middleware Infrastructure.
3. Select **Connection Parameter**.
4. Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done

 Tip:

For more information about the **RCU Data** option, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.
For more information about the other options on this screen, see "Datasource Defaults" in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 5 Specifying JDBC Component Schema Information

On the JDBC Component Schema screen, select all the UCM schemas (for WebCenter Content) in the table.

When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.

Click **Convert to GridLink** and click **Next**.

Task 6 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information that is required to connect to the RAC database and component schemas, as shown in the following table.

Element	Description and Recommended Value
SCAN, Host Name, and Port	Select the SCAN check box. In the Host Name field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database. In the Port field, enter the SCAN listening port for the database (for example, 1521)
ONS Host and Port	In the ONS Host field, enter the SCAN address for the Oracle RAC database. In the Port field, enter the ONS Remote port (typically, 6200).
Enable Fan	Verify that the Enable Fan check box is selected, so the database can receive and process FAN events.

Task 7 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

 Tip:

For more information about the other options on this screen, see "Test Component Schema" in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 8 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**



Note:

JMS JDBC stores are recommended and selected in [Task 3, Configuring High Availability Options](#) so there is no need to configure File Stores. If you choose JMS File Stores in [Task 3, Configuring High Availability Options](#), you have to select the File Stores option to configure them in a shared location in `ORACLE_RUNTIME/domain_name/SOA_Cluster/jms`. Shared location is required to resume JMS and HA in a failover scenario.

Task 9 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server for Oracle WebCenter Content appears in the list of servers.

Static Managed Server definitions are not needed for dynamic cluster configurations. To remove the default Managed Server, complete the following steps:

1. Delete the default Managed Server.
2. Click **Next** to proceed to the next screen.

Task 10 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle WebCenter Content software.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `WCC_Cluster` in the **Cluster Name** field.
3. Leave the **Cluster Address** field blank.
4. From the **Dynamic Server Groups** drop-down list, select `UCM-DYN-CLUSTER`.



Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.



Tip:

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 11 Assigning Server Templates

On the Server Templates screen, verify and update the following UCM server template configuration, add a template if necessary.

For the UCM server template, complete the following steps:

1. Verify UCM-server-template is listed in the **Name** field.
2. Specify 16200 in the **Listen Port** field.
3. Leave the **Enable SSL** option unchecked.
4. Click **Next** to proceed to the next screen.

Task 12 Configuring Dynamic Servers

Use the Dynamic Clusters screen to configure the required clusters:

1. Locate the row with the Cluster Name value of WCC_Cluster.
2. Verify WLS_WCC is listed in the **Server Name Prefix** field.
3. From the **Server Template** drop-down list, select UCM-server-template.
4. Specify 2 in the **Maximum Dynamic Server Count** field.
5. Specify WCCHOST* in the **Machine Name Match Expression** field and select **Calculated Machine Names**.

Note:

The dynamic cluster Calculated Machine Names and Machine Name Match Expression attributes control how server instances in a dynamic cluster are assigned to a machine.

- If the Calculated Machine Names attribute is set to False, the dynamic servers will not be assigned to a machine.
- If the Calculated Machine Names attribute is set to True, the Machine Name Match Expression attribute is used to select the set of machines that is used for the dynamic servers.
- If the Machine Name Match Expression attribute is not set, all of the machines in the domain get selected. Assignments are made by using a round robin algorithm.

To make things easier regardless of your actual physical hostname, Oracle recommends that you use WCCHOST n as your WebLogic machine names, where n is a sequential number. This is explained in [Task 14, Creating Machines for WebCenter Content Servers](#) of configuring the infrastructure domain. This convention makes it easy for dynamic clusters to determine where to start each cluster member. If you want to follow this convention, in the Machine Match Expression field, enter WCCHOST*.

If you do not adopt this convention, the cluster members will be started on each machine that you define in [Task 14, Creating Machines for WebCenter Content Servers](#), including that of ADMINHOST. This situation is undesirable as you would end up with two cluster members that run on the same physical server but are attached to two different domain homes.

6. Select **Calculated Listen Ports** and **Dynamic Cluster** fields.
7. Click **Next** to proceed to the next screen.

Task 13 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Update the port number value to **9991**.

**Note:**

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 14 Creating Machines for WebCenter Content Servers

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain, as shown in the following table.

Name	Node Manager Listen Address	Node Manager Listen Port
ADMINHOST	Enter the value of the ADMINVHN variable.	5556
WCCHOST1	The value of the WCCHOST1 host name variable. For example, WCCHOST1.example.com.	5556
WCCHOST2	The value of the WCCHOST2 host name variable. For example, WCCHOST2.example.com.	5556

If required, use the Machines screen to add two new Unix Machines:

1. On the Unix Machines tab, click the **Add** button.
2. Enter WCCHOST1 in the **Name** field.
3. Enter the host name of WCCHOST1 for the Node Manager Listener address. Leave the Node Manager port to the default value of 5556.
4. Repeat the above steps for WCCHOST2.
5. Click **Next** to proceed.

Task 15 Assigning Servers to Machines

Click **Next** to proceed to the next screen.

Task 16 Configuring Virtual Targets

Click **Next** to proceed to the next screen.

Task 17 Configuring Partitions

Click **Next** to proceed to the next screen.

Task 18 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Click **Update** to execute the domain extension.

**Tip:**

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 19 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server. Click **Finish** to dismiss the configuration wizard.

Task 20 Start the Administration Server

Start the Administration Server, login, and then verify the clusters and servers views to ensure that the changes made to the domain have been applied.

Completing Postconfiguration and Verification Tasks for WebCenter Content

Several configuration and validation steps must be performed to bring the content servers online. Complete the following sections in the order listed.

- [Propagating the Extended Domain to the Domain Directories and Machines](#)
- [Starting the Node Manager in the Managed Server Domain Directory on WCCHOST1](#)
- [Starting the WLS_WCC1 Managed Server](#)
- [Configuring the Content Server on WLS_WCC1 Managed Server](#)
- [Updating the cwallet File in the Administration Server](#)
- [Starting the Node Manager in the Managed Server Domain Directory WCCHOST2](#)
- [Starting the WLS_WCC2 Managed Server](#)
- [Configuring the Content Server on WLS_WCC2 Managed Server](#)
- [Validating GridLink Data Sources](#)
- [Configuring Additional Parameters](#)
- [Configuring Service Retries for Oracle WebCenter Content](#)
- [Granting user administrative access to Oracle WebCenter Content](#)
- [Granting the WebCenter Content Administrative Roles through Credential Map](#)

Propagating the Extended Domain to the Domain Directories and Machines

After you have extended the domain with the Oracle Content, and you have started the Administration Server on WCCHOST1, you can then propagate the domain changes to the domain directories and machines.

- [Packing Up the Extended Domain on WCCHOST1](#)
- [Unpacking the Domain in Managed Server Domain Home on WCCHOST1](#)
- [Unpacking the Domain on WCCHOST2](#)

Packing Up the Extended Domain on WCCHOST1

Use the following steps to create a template JAR file that contains the domain configuration information, which now includes configuration information about Oracle WebCenter Content:

1. Log in to WCCHOST1 and run the pack command to create a template JAR file as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true
          -domain=ASERVER_HOME
          -template=/full_path/edgdomaintemplateExtWCC.jar
          -template_name=edgdomaintemplateExtWCC
```

In this example:

- Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.
 - Replace *full_path* with the complete path to the directory where you want the template jar file saved.
 - *edgdomaintemplateExtWCC.jar* is a sample name for the JAR file you are creating, which will contain the domain configuration files, including the configuration files for Oracle WebCenter Content.
 - *edgdomaintemplateExtWCC* is the name assigned to the domain template file.
2. Make a note of the location of the *edgdomaintemplateExtWCC.jar* file you just created with the pack command.

By default, the pack template file is created in the current directory where you ran the pack command. In this example, it would be created in the *ORACLE_COMMON_HOME/common/bin* directory, but you can specify a full path for the template JAR file as part of the *-template* argument to the pack command.

Tip:

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

Unpacking the Domain in Managed Server Domain Home on WCCHOST1

To copy the updated domain configuration information from the Administration Server domain directory to the Managed Servers domain directory:

1. Log in to WCCHOST1 if you haven't already.
2. If you haven't already, create the recommended directory structure for the Managed Server domain on WCCHOST1.
Use the examples in [File System and Directory Variables Used in This Guide](#) as a guide.
3. Run the unpack command to unpack the template in the domain directory on the local storage, as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME \
  -template=template=/full_path/edgdomaintemplateExtWCC.jar \
  -overwrite_domain=true \
  -app_dir=APPLICATION_HOME \
```

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- Replace *full_path* with the complete path to the directory where you want the template jar file saved.
- *edgdomaintemplateExtWCC.jar* is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
- The *-overwrite_domain=true* argument is necessary when you are unpacking a Managed Server template into an existing domain and existing applications.

For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and EAR files in the Managed Server domain directory, they must be restored after this unpack operation.

- Replace *APPLICATION_HOME* with the complete path to the applications directory for the domain on shared storage.



Tip:

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Change directory to the newly created *MSERVER_HOME* directory and verify that the domain configuration files were copied to the correct location on the Unpacking

the Domain in on Managed Server Domain Home on WCCHOST1 shared storage device.

Unpacking the Domain on WCCHOST2

After you create a domain template jar, you can propagate the domain configuration to other hosts using the unpack command. To unpack the domain template jar file:

1. Log in to WCCHOST2.
2. If you haven't already, create the recommended directory structure for the Managed Server domain on WCCHOST2.
Use the examples in [File System and Directory Variables Used in This Guide](#) as a guide.

3. Make sure the domain template jar file is accessible to WCCHOST2.
For example, if you are using a separate shared storage volume or partition for WCCHOST2, then copy the template to the volume or partition mounted to WCCHOST2.
4. Run the unpack command to unpack the template in the domain directory on the local storage, as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME \
  -template=edgdomaintemplateExtWCC.jar \
  -app_dir=APPLICATION_HOME \
  -overwrite_domain=true
```

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- *edgdomaintemplateExtWCC.jar* is the directory path and name of the template you created when you ran the pack command to pack up the domain.

Note that if you are using a separate shared storage volume or partition for WCCHOST2 (and redundant Oracle homes), then you must first copy the template to the volume or partition mounted to WCCHOST2.

- Replace *APPLICATION_HOME* with the complete path to the applications directory for the domain on shared storage.

Tip:

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

5. Change directory to the newly created *MSERVER_HOME* directory and verify that the domain configuration files were copied to the correct location on WCCHOST2.

Starting the Node Manager in the Managed Server Domain Directory on WCCHOST1

After you create the Managed Server domain directory, there are two domain home directories and two corresponding Node Manager instances on WCCHOST1. You use one Node Manager to control the Administration Server, running from Administration Server domain home, and you use the other Node Manager to control the Managed Servers, running from the Managed Server domain home.

You must start the two Node Managers independently.

Note:

The Node Manager for the Managed Server's *MSERVER_HOME* will be reset every time the domain configuration is unpacked. The *ListenAddress* will be changed to the *ADMINVHN* instead of the correct hostname. This needs to be changed to the correct value before starting the Node Manager service after an unpack is performed.

Follow these steps to update and start the Node Manager from the Managed Server home:

1. Verify that the listen address in the *nodemanager.properties* file is set correctly, by completing the following steps:
 - a. Change to the following directory:

```
MSERVER_HOME/nodemanager/
```

- b. Open the *nodemanager.properties* file for editing.
 - c. Update the *ListenAddress* property to the correct hostname as follows:

```
WCCHOST1: ListenAddress=WCCHOST1
```
 - d. Update the *ListenPort* property with the correct Listen Port details.
 - e. Make sure that *QuitEnabled* is set to 'true'. If this line is not present in the *nodemanager.properties* file, add the following line:

```
QuitEnabled=true
```

2. Change to the following directory:

```
MSERVER_HOME/bin
```

3. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > MSERVER_HOME/nodemanager/nodemanager.out 2>&1 &
```

For information about additional Node Manager configuration options, see *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

Starting the WLS_WCC1 Managed Server

To start the WLS_WCC1 Managed Server:

1. Log in to the Oracle WebLogic Server Administration Console at `http://admin.example.com/console`.
2. Start the WLS_WCC1 Managed Server using the WebLogic Server Administration Console, as follows:
 - a. Expand the **Environment** node in the **Domain Structure** tree on the left.
 - b. Click **Servers**.
 - c. On the Summary of Servers page, open the **Control** tab.
 - d. Select **WLS_WCC1**, and then click **Start**.
3. Verify that the server status is reported as Running in the Administration Console. If the server is shown as Starting or Resuming, wait for the server status to change to Started. If another status is reported (such as Admin or Failed), check the server output log files for errors.

Configuring the Content Server on WLS_WCC1 Managed Server

To configure Content Server:

1. Create the runtime cluster subdirectories required for the Oracle WebCenter Content cluster configuration.

The Oracle WebCenter Content configuration files are on a shared disk so that all members of the cluster can access them. The shared disk location of the Oracle WebCenter Content enterprise deployment is located at `ORACLE_RUNTIME/WCDomain/WCC_Cluster`.

Run the following commands to create the required subdirectories:

```
mkdir -p ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/vault
mkdir -p ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/weblayout
mkdir -p ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/data/users/
profiles
```

2. Log in to WLS_WCC1 at `http://WCCHOST1:16200/cs` using the weblogic user name and password to display a configuration page.

The Oracle WebCenter Content configuration files are on a shared disk so that all members of the cluster can access them. The shared disk location of the Oracle WebCenter Content enterprise deployment is at `ORACLE_RUNTIME/wcpedg_domain/WCC_Cluster`.

3. Change the following values on the server configuration page:

Make sure that the **Is new Content Server Instance?** check box is selected.

- **Content Server Instance Folder:** Set this to `ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/`
For example: `/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/`
- **Native File Repository Location:** Set this to `ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/vault/`

For example: `/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/vault/`

- **WebLayout Folder:** Set this to `ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/weblayout/`
For example: `/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/weblayout/`
- **User Profile Folder:** Set this to `ORACLE_RUNTIME/domain_name/WCC_Cluster/cs/data/users/profiles/`
For example: `/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/data/users/profiles/`
- **Server Socket Port:** 4444
- **Incoming Socket Connection Address Security Filter:** A pipe-delimited list of the local host and the server IP addresses:

```
127.0.0.1|0:0:0:0:0:0:0:1|WCCHOST1-IP|WCCHOST2-IP|WCPHOST1-IP|WCPHOST2-IP|WEBHOST1-IP|WEBHOST2-IP|wcp.example.com-IP|wcpinternal.example.com-IP|load-balancer-host-IP
```

Note:

Must use IP addresses for all entries, including the load-balancer IP addresses for the internal virtual server and the primary interface depending on network address translation configuration settings at the load-balancer.

- **WebServer HTTP/HTTPS Address:** `wcc.example.com:443`
 - **Web Address is HTTPS:** Select this checkbox.
 - **Server Instance Name:** `WCC_Cluster`
 - **Server Instance Label:** `WCC_Cluster`
 - **Server Instance Description:** `WebCenter Content cluster`
 - **Auto_Number Prefix:** `WCC_Cluster-`
4. Click **Submit** when finished.
 5. Restart the Managed Server by using the WebLogic Server Administration Console.

Updating the cwallet File in the Administration Server

Content Server updates the `cwallet.sso` file located in the `MSERVER_HOME/config/fmwconfig` directory when it starts. This change needs to be propagated back to the Administration Server.

To do this, on `WCCHOST1`, copy the `cwallet.sso` file to `ASERVER_HOME/config/fmwconfig/` using the following command (note the back-slash for multi-line format):

```
cp MSERVER_HOME/config/fmwconfig/cwallet.sso \
ASERVER_HOME/config/fmwconfig/cwallet.sso
```



Note:

If any operation is performed in a *WLS_WCCn* server that modifies the *cwallet.sso* file in the *MSERVER_HOME/config/fmwconfig/* directory, the file will have to be immediately copied to the Administration Server domain configuration directory on *WCCHOST1* at *ASERVER_HOME/config/fmwconfig*.

Starting the Node Manager in the Managed Server Domain Directory WCCHOST2

After you have propagated the domain configuration to *WCCHOST2*, you can update and start the Node Manager for the *MSERVER_HOME* domain directory.

You must start the two Node Managers independently.



Note:

The Node Manager for the Managed Server's *MSERVER_HOME* will be reset every time the domain configuration is unpacked. The *ListenAddress* will be changed to the *ADMINVHN* instead of the correct hostname. This needs to be changed to the correct value before starting the Node Manager service after an unpack is performed.

Follow these steps to update and start the Node Manager from the Managed Server home:

1. Verify that the listen address in the *nodemanager.properties* file is set correctly, by completing the following steps:

- a. Change directory to the *MSERVER_HOME/nodemanager* directory:

```
cd MSERVER_HOME/nodemanager
```

- b. Open the *nodemanager.properties* file for editing.
- c. Validate the *ListenAddress* property to the correct hostname as follows:

```
WCCHOST2: ListenAddress=WCCHOST2
```

- d. Update the *ListenPort* property with the correct Listen Port details.
- e. Make sure that *QuitEnabled* is set to 'true'. If this line is not present in the *nodemanager.properties* file, add the following line:

```
QuitEnabled=true
```

2. Change directory to the *MSERVER_HOME* binary directory:

```
cd MSERVER_HOME/bin
```

3. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > $MSERVER_HOME/nodemanager/nodemanager.out 2>&1  
&
```


For information about additional Node Manager configuration options, see *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

Starting the WLS_WCC2 Managed Server

To start the WLS_WCC2 Managed Server:

1. Start the WLS_WCC2 Managed Server using the WebLogic Server Administration Console, as follows:
 - a. Expand the **Environment** node in the **Domain Structure** tree on the left.
 - b. Click **Servers**.
 - c. On the Summary of Servers page, open the **Control** tab.
 - d. Select **WLS_WCC2**, and then click **Start**.
2. Verify that the server status is reported as Running in the Administration Console. If the server is shown as Starting or Resuming, wait for the server status to change to Started. If another status is reported (such as Admin or Failed), check the server output log files for errors.

Configuring the Content Server on WLS_WCC2 Managed Server

To configure Content Server:

1. Log in to WLS_WCC2 at `http://WCCHOST2:16200/cs` using the weblogic administration user name and password to display a configuration page.

The Oracle WebCenter Content configuration files are on a shared disk so that all members of the cluster can access them. The shared disk location of the Oracle WebCenter Content enterprise deployment is at `ORACLE_RUNTIME/WCDomain/WCC_Cluster`.
2. Change the following values on the server configuration page:
 - **Content Server Instance Folder:** Set this to `ORACLE_RUNTIME/WCDomain/WCC_Cluster/cs`.
 - **Native File Repository Location:** Set this to `ORACLE_RUNTIME/WCDomain/WCC_Cluster/cs/vault`.
 - **WebLayout Folder:** Set this to `ORACLE_RUNTIME/WCDomain/WCC_Cluster/cs/weblayout`.
 - **User Profile Folder:** Set this to `ORACLE_RUNTIME/WCDomain/WCC_Cluster/cs/data/users/profiles`.
 - **Content Server URL Prefix:** `/cs/` (default value)

Make sure that the **Is new Content Server Instance?** check box is not selected.

3. Click **Submit** when finished.
4. Restart the Managed Server by using the WebLogic Server Administration Console.

Validating GridLink Data Sources

After the servers are started, verify that the GridLink data sources are correctly configured and that the ONS setup is correct. Perform these procedures for every GridLink data source created.

- [Verifying the Configuration of a GridLink Data Source for WebCenter Content](#)
- [Verifying the Configuration of ONS for a GridLink Data Source](#)

Verifying the Configuration of a GridLink Data Source for WebCenter Content

To verify the configuration of a GridLink data source for WebCenter Content:

1. Log in to the WebLogic Server Administration Console.
2. In the **Domain Structure** tree, expand **Services**, then click **Data Sources**.
3. Click the name of a GridLink data source that was created.
4. Click the **Monitoring** tab.
5. Click the **Testing** tab, select one of the servers, and click **Test Data Source**.
The test should be successful if the configuration is correct.
6. Repeat the test for every WebLogic Server instance that uses the GridLink data source.

Verifying the Configuration of ONS for a GridLink Data Source

To verify the configuration of ONS for a GridLink data source for WebCenter Content:

1. In the **Domain Structure** tree on the Administration Console, expand **Services**, then click **Data Sources**.
2. Click the name of a GridLink data source.
3. Click the **Monitoring** tab.
4. Click the name of the server (WLS_WCC1).
5. Click the **ONS** tab.
6. In the **ONS** tab, select the **Testing** tab.
7. Select a server, and click **Test ONS**.

The test should be successful if the configuration is correct. If the ONS test fails, verify that the ONS service is running in the Oracle RAC database nodes:

```
[orcl@WCCDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node WCCDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node WCCDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node WCCDBHOST2
```

```
[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
```

ONS exists: Local port 6100, remote port 6200, EM port 2016

```
[orcl@WCCDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: WCCDBHOST1
ONS daemon is running on node: WCCDBHOST2
```

8. Repeat the ONS test for every WebLogic Server instance that uses the GridLink data source.

Configuring Additional Parameters

Using a text editor, add the following options to each cluster node's `MSERVER_HOME/ucm/cs/bin/WLS_WCCn_intradoc.cfg` file, where the directories specified are on a direct-bus-attached-controlled local disk and not a remote file system, such as a UNIX/Linux mounted NFS or clustered file system (like OCFS2, GFS2, or GPFS):

```
TraceDirectory=MSERVER_HOME/servers/WLS_WCCN/logs
EventDirectory=MSERVER_HOME/servers/WLS_WCCN/logs/event/
ArchiverDoLocks=true
DisableSharedCacheChecking=true
```

The trailing *N* should match your nodes server names, like `WLS_WCC1` is for `WCCHOST1` and `WLS_WCC2` is for `WCCHOST2`, and so on.

These changes will take effect after a restart of all WebCenter Content Managed Servers, at the end of the procedure described in [Configuring Service Retries for Oracle WebCenter Content](#).

Note:

The directories can reside in any local disk path that you have determined to have enough space to hold the WebCenter Content logs and any trace that you may configure. The preceding paths are a suggestion.

Configuring Service Retries for Oracle WebCenter Content

The following parameter should be set in the Content Server `config.cfg` file to enable login retries during an Oracle RAC failover:

```
ServiceAllowRetry=true
```

If this value is not set, users will need to manually retry any operation that was in progress when the failover began.

To configure service retries for Oracle WebCenter Content:

1. Go to Content Server at `http://WCCHOST1:16200/cs`, and log in using the non-LDAP WebLogic Server administration user name (for example, *weblogic*) and password.

2. From the **Administration** tray or menu, choose **Admin Server**, then **General Configuration**.
3. On the General Configuration page, add the following parameter in the **Additional Configuration Variables** box:

```
ServiceAllowRetry=true
```

4. Click **Save**.

 Note:

The new parameter is included in the `config.cfg` file, which is at the following location:

```
ORACLE_RUNTIME/domain_name/cluster_name/cs/config/config.cfg
```

(You can also edit this file directly in a text editor. Remember to restart all WebCenter Content Managed Servers.

Granting user administrative access to Oracle WebCenter Content

To grant users administrative access to Oracle WebCenter Content, configure the Administrators group in the LDAP directory and then add the `weblogic_wcc` user as a member of the group.

If adding the `weblogic_wcc` user to Administrators group is not allowed by your LDAP directory administrator, see [Granting the WebCenter Content Administrative Roles via Credential Map](#).

Granting the WebCenter Content Administrative Roles through Credential Map

You must configure the Credential map to grant the Content Server administrative roles to the **WCCAdministrators** LDAP group.

The **WCCAdministrators** LDAP group is created in the [Provisioning an Enterprise Deployment Administration User and Group](#) section completed earlier. This configuration of credential map ensures consistent use of the LDAP administrative user for all configuration, administration, and maintenance tasks.

To configure a credential map and provide the necessary role grants to the LDAP-based **WCCAdministrators** group:

1. Log in to content server using the *weblogic* account.
2. Expand the **Administration** menu, select **Credential Maps**.
3. In the Map Identifier Field, enter a name for the new credential map: **LDAPAdmins**.

4. Add the following lines to map the LDAP group to the multiple administrative roles:

```
# Assign full set of administration roles to the LDAP
WCCAdministrators group
    WCCAdministrators, admin
    WCCAdministrators, sysmanager
    WCCAdministrators, refineryadmin
    WCCAdministrators, rmaadmin
    WCCAdministrators, pcadmin
    WCCAdministrators, ermadmin
# Allow existing roles to propagate without mappings
|#all| , %%
#
# Comment the following if you are not implementing Accounts in
Content Server
    WCCAdministrators, @#all(RWDA)
    WCCAdministrators, @#none(RWDA)
```



Note:

If you are not implementing **Accounts**, comment out the last two lines of the previous example.

5. Click **Update**.
6. Navigate to **Administration > Providers**.
7. Click the **info** link for the existing JPS provider.
8. Make sure that the **Credential Map** parameter does not already have a map identifier listed.
9. Click the **Edit** button.
10. Enter the name of the Map Identifier from step 3 above as the Credential Map value.



Note:

Double-check the value entered for any typos, extra characters, and so on. If this is set incorrectly, you will not be able to log-in to your content server instances.

11. Click **Update**.
12. Repeat a modified process for the content server on WCCHOST2.
 - a. Confirm that the LDAPAdmins credential map is already available for selection on the Credential Maps view.
 - b. Repeat the edit of the JpsUserProvider noting that even though the correct LDAPAdmins credential Map value appears in the form automatically, it must still be submitted on each server to take effect.
13. Restart the managed servers in the **WCC_Cluster**.

14. Log in to each content server using the `weblogic_wcc` LDAP user and verify that the administrative menu options appear in the user interface.

 Note:

If the provider configuration was entered incorrectly and you can no longer log-in, the `jpsuserprovider` data file needs to be corrected manually. In this case, shutdown all content server instances and edit the value of the `ProviderCredentialsMap` parameter in `ORACLE_RUNTIME/DOMAIN_NAME/WCC_Cluster/cs/data/providers/jpsuserprovider/provider.hda`, and restart/test one server instance at a time.

Configuring Content Server for the WebCenter Content User Interface

If you are planning to use the WebCenter Content user interface (in addition to the native user interface for Content Server), you need to enable the Content Server parameters.

From the **Administration** tray or menu, select **Admin Server > Component Manager** and then enable the following parameters:

- `AutoSuggestConfig`
- `DynamicConverter`
- `FrameworkFolders`

In addition, you need to set up the Remote Intradoc Client (RIDC) for communication between the WebCenter Content user interface and Content Server.

You can also set the following Content Server parameters for folders and searching, for the WebCenter Content user interface. To set the Content Server parameters for folders and searching for the WebCenter Content user interface:

1. From the **Administration** menu, select **Admin Server**.
2. Select **General Configuration**.
3. On the General Configuration page, add the following parameters in the **Additional Configuration Variables** tab:
 - `FoldersIndexParentFolderValues=true`
 - `FldEnforceFolderFileNameUniqueness=true`
 - `FldEnforceCaseInsensitiveNameUniqueness=true`
 - `SearchIndexerEngineName=OracleTextSearch` or `SearchIndexerEngineName=DATABASE.METADATA`

Select either one of the values - `OracleTextSearch` or `DATABASE.METADATA`.

Configuring Oracle HTTP Server for the WebCenter Content Cluster

The instructions for configuring Oracle HTTP Server for the WebCenter Content Cluster are available in this section.

- [Configuring Oracle HTTP Server for the WLS_WCC Managed Servers](#)
- [Enabling Access for Content Server Admin Applets](#)
- [Validating Access Through the Load Balancer](#)

Configuring Oracle HTTP Server for the WLS_WCC Managed Servers

To configure the Oracle HTTP Server instances in the web tier so they route requests correctly to the Oracle WebCenter Content cluster, use the following procedure to create an additional Oracle HTTP Server configuration file that creates and defines the parameters of the `wcc.example.com` virtual server. To configure Oracle HTTP Server for the WLS_WCC Managed Servers:

1. Log in to `WEBHOST1` and change directory to the configuration directory for the first Oracle HTTP Server instance (`ohs1`).

```
cd WEB_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
```



Note:

There are separate directories for configuration and runtime instance files. The runtime files under the `.../OHS/instances/ohsn/*` folder should not be edited directly. Edit only the `.../OHS/ohsn/*` configuration files.

2. Create the `wcc_vh.conf` file and add the following directive:

```
<VirtualHost WEBHOST1:7777>
  ServerName https://wcc.example.com:443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>
```

3. In the `wcc_vh.conf` file, add the following lines between the `<VirtualHost>` and `</VirtualHost>` tags:

 Note:

- For static clusters: The port numbers for WCCHOST1 and WCCHOST2 are 16200.
- For dynamic clusters: If the **Calculated Listen Ports** option is enabled, then the port number for WCCHOST1 is 16201 and WCCHOST2 is 16202.
- In the following example, it is assumed that you are using dynamic clusters and the **Calculated Listen Ports** option is enabled.

```
#UCM
<Location /cs>
    WebLogicCluster WCCHOST1:16201,WCCHOST2:16202
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /adfAuthentication>
    WebLogicCluster WCCHOST1:16201,WCCHOST2:16202
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /_ocsh>
    WebLogicCluster WCCHOST1:16201,WCCHOST2:16202
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

4. Copy the wcc_vh.conf file to the configuration directory for the second Oracle HTTP Server instance (ohs2):
`WEB_DOMAIN_HOME/config/fmwconfig/components/ohs2/moduleconf/`
5. Edit the wcc_vh.conf and change any references of WEBHOST1 to WEBHOST2 in the <VirtualHost> directives.
6. Restart the Oracle HTTP server instances on WEBHOST1 and WEBHOST2.

Enabling Access for Content Server Admin Applets

Because the SSL termination is configured on Oracle Web Tier for the enterprise deployment reference topology, the WebLogic Plug-In needs to be enabled for each WebCenter Content Managed Server for successful access to the Content Server Admin Applets. To enable access for Content Server Admin Applets:

1. Log in to the WebLogic Server Administration Console at `http://host.domain:port/console`; for example:
`http://ADMINVHN:7001/console`
2. (For Dynamic clusters only) On the **Environment** tab, click **Servers**.
3. Click **WLS_WCC1**.
4. Click the **General** tab on the **Configuration** tab, and go to the Advanced section.
5. Click **Lock & Edit**.
6. Select **Yes** from the **WebLogic Plug-In Enabled** drop-down menu.
7. Click the **Save** button to save the change.
8. Click **Activate Changes**.
9. Restart the WLS_WCC1 Managed Server from the Administration Console.
10. Repeat the above instructions for the WLS_WCC2 Managed Server.

Validating Access Through the Load Balancer

You should verify URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to WCC_Cluster.

- [Verifying the URLs](#)
- [Verifying the Cluster Nodes](#)

Verifying the URLs

To verify the URLs:

1. While WLS_WCC2 is running, stop WLS_WCC1 using the WebLogic Server Administration Console.
2. Access `https://wcc.example.com/cs` to verify that it is functioning properly.
3. Start WLS_WCC1 from the WebLogic Server Administration Console.
4. Stop WLS_WCC2 from the WebLogic Server Administration Console.
5. Access `https://wcc.example.com/cs` to verify that it is functioning properly.

You can verify the cluster node to which you were directed after the traffic balancing provided through your load balancer and then again through the web tier.

Verifying the Cluster Nodes

To verify the cluster node:

1. Log in to the following WebCenter Content page, using your administrator user and password credentials:
`https://wcc.example.com/cs/idcplg?IdcService=CONFIG_INFO`
2. Browse to the Administration/Configuration for WCC_Cluster page.
3. In the Options and Others section of the page, click **Java Properties** on the right.
4. Obtain the value for **weblogic.Name**.

This value denotes the cluster node you are accessing at the moment.

Enabling JDBC Persistent Stores

Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an Oracle database and makes resources available for all the servers in the cluster.

Follow these guidelines to ensure that you use JDBC stores, when you use static or dynamic clusters:

- **For static clusters**

If you have made the following selections in the High Availability Options screen, as recommended in this guide for static clusters, then JDBC persistent stores are already configured for both JMS and TLOGS:

- Set **JTA Transaction Log Persistence** to **JDBC TLog Store**.
- Set **JMS Server Persistence** to **JMS JDBC Store**.

- **For dynamic clusters**

You can configure only JMS Server persistence for dynamic clusters by using the Configuration Wizard. JTA Transaction Logs Persistence must be configured manually, if required. If you have made the following selections in the High Availability Options screen, as recommended in this guide for dynamic clusters, then JDBC persistent stores are already configured for JMS.

- Set **JMS Server Persistence** to **JMS JDBC Store**.
- Verify that **JTA Transaction Log Persistence** is set to **Default Persistent Store**.

Additional steps are needed to configure JTA Transaction Log with JDBC store. See [Roadmap for Configuring a JDBC Persistent Store for TLOGs](#).

In case you did not select JDBC for JMS and TLOGS persistent in the High Availability Options screen, you can still configure JDBC stores manually in a post step. For specific instructions to configure them manually, see [Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#).



Note:

The High Availability Options screen appears during the Configuration Wizard session for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. All subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.

Enabling Automatic Service Migration

To ensure high availability for the product installed in this chapter, you must configure service migration appropriately.

Follow these guidelines to ensure that you provide the required high availability for Weblogic services when you use static or dynamic clusters:

- **For static clusters**

Automatic Service Migration is already configured if you select **Enable Automatic Service Migration** with **Database Basis** in the High Availability Options screen.

The Database Leasing is already configured and the migratable targets are created with the appropriate policies for the cluster. If you have implemented these settings, validate the configuration, as described in [Validating Automatic Service Migration in Static Clusters](#).

In case you do not select this option during the Configuration Wizard session, you can configure automatic migration manually in a post step. For instructions to complete the steps for static clusters, see [Configuring Automatic Service Migration in an Enterprise Deployment](#).

- **For dynamic clusters**

You cannot configure Service Migration for dynamic clusters by using the Configuration Wizard, it needs to be configured manually. The following steps are needed:

- Configure the database leasing for the cluster.
- Set the appropriate migration policies for JTA Service and JMS Persistent Stores.

For instructions to complete the steps for dynamic clusters, see [Configuring Automatic Service Migration in an Enterprise Deployment](#).

 Note:

The High Availability Options screen appears during the Configuration Wizard session for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. All subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.

Extending the Domain with Oracle SOA Suite

You need to perform certain tasks in order to extend the enterprise deployment domain with the Oracle SOA Suite software.

- [Variables Used When Configuring Oracle SOA Suite](#)
While extending the domain with Oracle SOA Suite, you will be referencing the directory variables listed in this section.
- [Support for Dynamic Clusters in Oracle SOA Suite](#)
SOA supports two different topologies: static clusters-based topology and dynamic clusters-based topology. When choosing the dynamic cluster topology, there are some differences with respect to the conventional static clusters configuration.
- [Synchronizing the System Clocks](#)
Before you extend the domain to include Oracle SOA Suite, verify that the system clocks on each host computer are synchronized.
- [Installing the Software for an Enterprise Deployment](#)
The procedure to install the software for an enterprise deployment is explained in this section.
- [Creating the Oracle SOA Suite Database Schemas](#)
Before you can configure an Oracle SOA Suite domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.
- [Extending the Enterprise Deployment Domain with Oracle SOA Suite](#)
Perform the following tasks to extend the existing enterprise deployment domain with the Oracle SOA Suite software.
- [Propagating the Extended Domain to the Domain Directories and Machines](#)
After you have extended the domain with the Oracle WebCenter Content instances, and you have restarted the Administration Server on WCCHOST1, you must then propagate the domain changes to the domain directories and machines.
- [Updating the NodeManager Configuration After Unpacking the Domain](#)
When extending a domain, the `nodemanager.properties` file in `MSERVER_HOME` may be overwritten with some values from the `nodemanager.properties` file for `ASERVER_HOME`. Specifically, the `ListenAddress` and/or `CustomIdentityAlias` values can be reset.
- [Modifying the Upload and Stage Directories to an Absolute Path in an Enterprise Deployment](#)
After you configure the domain and unpack it to the Managed Server domain directories on all the hosts, verify and update the upload and stage directories for Managed Servers in the new clusters. Also, update the upload directory for the AdminServer to have the same absolute path instead of relative, otherwise deployment issues can occur. If you implement dynamic clusters, the configuration of the server template assigned to each newly added cluster should be verified and updated, otherwise, verify and update every statically-defined Managed Server for the newly added clusters.

- [Configuring Listen Addresses When Using Dynamic Clusters](#)
- [Starting and Validating the WLS_SOA1 Managed Server](#)
Now that you have extended the domain, started the Administration Server, and propagated the domain to the other hosts, you can start the newly configured Oracle SOA Suite Managed Servers.
- [Starting and Validating the WLS_SOA2 Managed Server](#)
After you validate the successful configuration and startup of the WLS_SOA1 Managed Server, you can start and validate the WLS_SOA2 Managed Server.
- [Configuring Oracle HTTP Server for the Extended Domain](#)
The following sections describe how to configure the Oracle HTTP Server instances so they route requests for both public and internal URLs to the proper clusters in the enterprise topology.
- [Post-Configuration Steps for Oracle SOA Suite](#)
After you install and configure Oracle SOA Suite, consider the following post-configuration tasks.
- [Enabling JDBC Persistent Stores](#)
Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an oracle database and makes resources available for all the servers in the cluster.
- [Enabling Automatic Service Migration](#)
To ensure high availability for the product installed in this chapter, you must configure service migration appropriately.

Variables Used When Configuring Oracle SOA Suite

While extending the domain with Oracle SOA Suite, you will be referencing the directory variables listed in this section.

The values for several directory variables are defined in [File System and Directory Variables Used in This Guide](#).

- ORACLE_HOME
- ASERVER_HOME
- MSERVER_HOME
- APPLICATION_HOME
- DEPLOY_PLAN_HOME
- OHS_DOMAIN_HOME
- JAVA_HOME
- ORACLE_RUNTIME

In addition, you'll be referencing the following virtual IP (VIP) address defined in [Reserving the Required IP Addresses for an Enterprise Deployment](#):

- ADMINVHN

Actions in this chapter will be performed on the following host computers:

- WCCHOST1
- WCCHOST2

- WEBHOST1
- WEBHOST2

Support for Dynamic Clusters in Oracle SOA Suite

SOA supports two different topologies: static clusters-based topology and dynamic clusters-based topology. When choosing the dynamic cluster topology, there are some differences with respect to the conventional static clusters configuration.

Static clusters, also called configured clusters, are conventional clusters where you manually configure and add each server instance. A dynamic cluster includes a new "server-template" object that is used to define a centralized configuration for all generated (dynamic) server instances. When you create a dynamic cluster, the dynamic servers are preconfigured and automatically generated for you. This feature enables you to scale up the number of server instances in the dynamic cluster when you need additional server capacity. You can simply start the dynamic servers without having to first manually configure and add them to the cluster.

The steps in this section include instructions to configure the domain for both static or dynamic topologies. The differences between the two types of configurations are listed below:

- The Configuration Wizard process may differ for each case. For example, you should define server templates for dynamic clusters instead of servers.
- For dynamic clusters, you should perform the server-specific configurations such as setting the listen address, configuring the upload and staging directories, or configuring the keystores in the server template instead of in the server.
- Service migration is configured in a different way for dynamic clusters. Dynamic clusters do not use migratable targets, instead the JMS resources are targeted to the cluster. Specific procedure for configuring service migration for dynamic clusters is included in this guide.

Mixed clusters (clusters that contains both dynamic and configured server instances) are not supported in the Oracle WebCenter Content enterprise deployment.

Synchronizing the System Clocks

Before you extend the domain to include Oracle SOA Suite, verify that the system clocks on each host computer are synchronized.

To verify the time synchronization, query the NTP service by running the `ntpstat` command on each host.

Sample output:

```
$ ntpstat
synchronised to NTP server (10.132.0.121) at stratum 3
time correct to within 42 ms
polling server every 16 s
```

Installing the Software for an Enterprise Deployment

The procedure to install the software for an enterprise deployment is explained in this section.

- [Starting the Oracle SOA Suite Installer on WCCHOST1](#)
- [Navigating the Installation Screens](#)
- [Installing Oracle SOA Suite on the Other Host Computers](#)
- [Verifying the Installation](#)

Starting the Oracle SOA Suite Installer on WCCHOST1

To start the installation program:

1. Log in to WCCHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the following example:

```
JAVA_HOME/bin/java -d64 -jar Installer File Name
```

Be sure to replace the JDK location in these examples with the actual JDK location on your system.

Replace *Installer File Name* with the name of the actual installer file for your product listed in [Identifying and Obtaining Software Distributions for an Enterprise Deployment](#).

When the installation program appears, you are ready to begin the installation.

Navigating the Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

Screen	Description
Welcome	This screen introduces you to the product installer.
Auto Updates	Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you have already downloaded for your organization.
Installation Location	Use this screen to specify the location of your Oracle home directory. For more information about Oracle Fusion Middleware directory structure, see Selecting Directories for Installation and Configuration in <i>Planning an Installation of Oracle Fusion Middleware</i> .
Installation Type	Use this screen to select the type of installation and consequently, the products and feature sets you want to install. • Select SOA Suite

Screen	Description
Prerequisite Checks	This screen verifies that your system meets the minimum necessary requirements. If there are any warning or error messages, you can refer to one of the documents in the Roadmap for Verifying Your System Environment section in <i>Oracle Fusion Middleware Installing and Configuring the Oracle Fusion Middleware Infrastructure</i> .
Installation Summary	Use this screen to verify the installation options that you selected. Click Install to begin the installation.
Installation Progress	This screen allows you to see the progress of the installation. Click Next when the progress bar reaches 100% complete.
Installation Complete	Review the information on this screen, then click Finish to dismiss the installer.

Installing Oracle SOA Suite on the Other Host Computers

If you have configured a separate shared storage volume or partition for the products mount point and `ORACLE_HOME` on `WCCHOST2`, then you must also perform the product installation on `WCCHOST2`.

See [Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment](#).

To install the software on the other host computers in the topology, log in to each host, and use the instructions in [Starting the Infrastructure Installer on WCCHOST1](#) and [Navigating the Infrastructure Installation Screens](#) to create the Oracle home on the appropriate storage device.

Verifying the Installation

After you complete the installation, you can verify it by successfully completing the following tasks.

- [Reviewing the Installation Log Files](#)
- [Checking the Directory Structure](#)
- [Viewing the Contents of Your Oracle Home](#)

Reviewing the Installation Log Files

Review the contents of the installation log files to make sure that no problems were encountered. For a description of the log files and where to find them, see Understanding Installation Log Files in *Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

Checking the Directory Structure

The contents of your installation vary based on the options that you select during the installation.

The addition of Oracle SOA Suite adds the following directory and sub-directories. Use the `ls --format=single-column` command to verify the directory structure.


```
ls --format=single-column /u01/oracle/products/fmw/soa

bam
bin
bpm
common
integration
jlib
modules
plugins
readme.txt
reports
soa
```

For more information about the directory structure you should see after installation, see *What are the Key Oracle Fusion Middleware Directories?* in *Understanding Oracle Fusion Middleware*.

Viewing the Contents of Your Oracle Home

You can also view the contents of your Oracle home by using the `viewInventory` script. See *Viewing the contents of an Oracle home* in *Installing Software with the Oracle Universal Installer*.

Creating the Oracle SOA Suite Database Schemas

Before you can configure an Oracle SOA Suite domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.

- [Starting the Repository Creation Utility \(RCU\)](#)
- [Navigating the RCU Screens to Create the Schemas](#)
- [Verifying Schema Access](#)
- [Configuring SOA Schemas for Transactional Recovery](#)

Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Navigate to the `ORACLE_HOME/oracle_common/bin` directory on your system.
2. Make sure that the `JAVA_HOME` environment variable is set to the location of a certified JDK on your system. The location should be up to but not including the `bin` directory. For example, if your JDK is located in `/u01/oracle/products/jdk`:

On UNIX operating systems:

```
export JAVA_HOME=/u01/oracle/products/jdk
```

3. Start RCU:

On UNIX operating systems:

```
./rcu
```

**Note:**

If your database has Transparent Data Encryption (TDE) enabled, and you want to encrypt your tablespaces that are created by the RCU, provide the `-encryptTablespace true` option when you start RCU.

This defaults the appropriate RCU GUI Encrypt Tablespace checkbox selection on the Map Tablespaces screen without further effort during the RCU execution. See *Encrypting Tablespaces in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Navigating the RCU Screens to Create the Schemas

Schema creation involves the following tasks:

- [Task 1, Introducing RCU](#)
- [Task 2, Selecting a Method of Schema Creation](#)
- [Task 3, Providing Database Connection Details](#)
- [Task 4, Specifying a Custom Prefix and Selecting Schemas](#)
- [Task 5, Specifying Schema Passwords](#)
- [Task 6, Specifying Custom Variables](#)
- [Task 7, Verifying the Tablespaces for the Required Schemas](#)
- [Task 8, Creating Schemas](#)
- [Task 9, Reviewing Completion Summary and Completing RCU Execution](#)

Task 1 Introducing RCU

Click **Next**.

Task 2 Selecting a Method of Schema Creation

If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have the necessary privileges.

If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option generates a SQL script, which can be provided to your database administrator to create the required schema. See *Understanding System Load and Product Load in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Click **Next**.

Task 3 Providing Database Connection Details

Provide the database connection details for RCU to connect to your database.

1. In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.
2. Enter the **Port** number of the RAC database scan listener, for example 1521.
3. Enter the RAC **Service Name** of the database.
4. Enter the **User Name** of a user that has permissions to create schemas and schema objects, for example SYS.

5. Enter the **Password** of the user name that you provided in step 4.
6. If you have selected the SYS user, ensure that you set the role to SYSDBA.
7. Click **Next** to proceed, then click **OK** on the dialog window confirming that connection to the database was successful.

Task 4 Specifying a Custom Prefix and Selecting Schemas

Choose **Select existing prefix**, and then select the prefix you used when you created the initial domain.

From the list of schemas, select the **SOA Suite** schema. This automatically selects **SOA Infrastructure**. In addition, the following dependent schemas have already been installed with the Infrastructure and are grayed out:

- **Common infrastructure Services**
- **Oracle Platform Security Services**
- **User Messaging Service**
- **Audit Services**
- **Audit Services Append**
- **Audit Services Viewer**
- **Metadata Services**
- **Weblogic Services**
- **Oracle WebCenter Content Server - Complete**

The custom prefix is used to logically group these schemas together for use in this domain only; you must create a unique set of schemas for each domain as schema sharing across domains is not supported.



Tip:

For more information about custom prefixes, see Understanding Custom Prefixes in *Creating Schemas with the Repository Creation Utility*.
For more information about how to organize your schemas in a multi-domain environment, see Planning Your Schema Creation in *Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, then click **OK** on the dialog window to confirm that prerequisite checking for schema creation was successful.

Task 5 Specifying Schema Passwords

Specify how you want to set the schema passwords on your database, then specify and confirm your passwords. Ensure that the complexity of the passwords meet the database security requirements before you continue. RCU proceeds at this point even if you do not meet the password policies. Hence, perform this check outside RCU itself.

 Tip:

You must make a note of the passwords that you set on this screen; you need them later on during the domain creation process.

Click **Next**.

Task 6 Specifying Custom Variables

Specify the custom variables for the SOA Infrastructure schema.

For the enterprise deployment topology, enter MEDIUM for the **Database Profile** custom variable; enter NO for the **Healthcare Integration** variable. See About the Custom Variables Required for the SOA Suite Schemas in *Installing and Configuring Oracle SOA Suite and Business Process Management*.

Click **Next**.

Task 7 Verifying the Tablespaces for the Required Schemas

On the Map Tablespaces screen, review the information, and then click **Next** to accept the default values.

Click **OK** in the confirmation dialog box.

Click **Next**.

Task 8 Creating Schemas

Review the summary of the schemas to be loaded, and click **Create** to complete schema creation.

 Note:

If failures occurred, review the listed log files to identify the root cause, resolve the defects, and then use RCU to drop and recreate the schemas before you continue.

Task 9 Reviewing Completion Summary and Completing RCU Execution

When you reach the Completion Summary screen, verify that all schema creations have been completed successfully, and then click **Close** to dismiss RCU.

Verifying Schema Access

Verify schema access by connecting to the database as the new schema users created by the RCU. Use SQL*Plus or another utility to connect, and provide the appropriate schema names and passwords entered in the RCU.

For example:

```
./sqlplus
```

```
SQL*Plus: Release 12.1.0.2.0 Production on Wed Aug 31 05:41:31 2016
```

```
Copyright (c) 1982, 2014, Oracle. All rights reserved.
```

```
Enter user-name: FMW1221_SOAINFRA
```

```
Enter password: soainfra_password
```

```
Connected to:
```

Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Real Application Clusters, Automatic Storage Management,
OLAP, Advanced Analytics and Real Application Testing options

SQL>

Configuring SOA Schemas for Transactional Recovery

After you have installed the Oracle SOA Suite schemas successfully, use the procedure in this section to configure the schemas for transactional recovery.

This procedure sets the appropriate database privileges so that the Oracle WebLogic Server transaction manager can query the schemas for transaction state information and issue the appropriate commands, such as commit and rollback, during recovery of in-flight transactions after a WebLogic Server is unexpectedly unavailable.

These privileges should be granted to the owner of the SOAINFRA schema, which you defined when you created the schemas with the RCU.

To configure the SOA schemas for transactional recovery privileges:

1. Log on to SQL*Plus as a user with sysdba privileges. For example:

```
sqlplus "/ as sysdba"
```

2. Enter the following commands:

```
SQL> Grant select on sys.dba_pending_transactions to  
soa_schema_prefix_soainfra;
```

```
Grant succeeded.
```

```
SQL> Grant force any transaction to soa_schema_prefix_soainfra;
```

```
Grant succeeded.
```

```
SQL>
```

Extending the Enterprise Deployment Domain with Oracle SOA Suite

Perform the following tasks to extend the existing enterprise deployment domain with the Oracle SOA Suite software.



Note:

For an improved footprint and to optimize startup, only core adapters are targeted to the SOA cluster (MFT Cluster if you are configuring MFT) after the Configuration Wizard session. You must target the second-tier adapters manually, if required. See [Targeting Adapters Manually](#).

Extending the domain involves the following tasks:

- [Starting the Configuration Wizard](#)
Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.
- [Navigating the Configuration Wizard Screens to Extend the Domain with Oracle SOA Suite](#)
Follow the instructions in these sections to extend the domain for Oracle SOA Suite, with static or dynamic clusters.
- [Targeting Adapters Manually](#)
Only core adapters are targeted to the SOA cluster after you run the Configuration Wizard. You must target second-tier adapters manually, on a need basis.

Starting the Configuration Wizard

Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.

Note:

If you added any customizations directly to the start scripts in the domain, those are overwritten by the configuration wizard. To customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it, for example, add custom libraries to the WebLogic Server classpath, specify Additional JAVA command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the **pack** and **unpack** commands.

To start the Configuration Wizard:

1. From the WebLogic Server Console, stop any managed servers that are modified by this domain extension. Managed Servers that are not effected can remain on-line.
2. For any managed servers to be modified, verify that the managed server shutdown has completed.
3. Stop the Administration Server once all managed servers are in a steady state.
4. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

Navigating the Configuration Wizard Screens to Extend the Domain with Oracle SOA Suite

Follow the instructions in these sections to extend the domain for Oracle SOA Suite, with static or dynamic clusters.

- [Extending the Domain with Static Clusters](#)

- [Extending the Domain with Dynamic Clusters](#)

Extending the Domain with Static Clusters

Follow the instructions in this section to extend the domain for Oracle SOA Suite, with static clusters.



Note:

This procedure assumes that you are extending an existing domain. If your needs do not match the instructions given in the procedure, ensure that you make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Configuring High Availability Options](#)
- [Task 4, Specifying the Database Configuration Type](#)
- [Task 5, Specifying JDBC Component Schema Information](#)
- [Task 6, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 7, Testing the JDBC Connections](#)
- [Task 8, Keystore](#)
- [Task 9, Selecting Advanced Configuration](#)
- [Task 10, Configuring Managed Servers](#)
- [Task 11, Configuring a Cluster](#)
- [Task 12, Assigning Server Templates](#)
- [Task 13, Configuring Dynamic Servers](#)
- [Task 14, Assigning Managed Servers to the Cluster](#)
- [Task 15, Configuring Coherence Clusters](#)
- [Task 16, Verifying the Existing Machines](#)
- [Task 17, Assigning Servers to Machines](#)
- [Task 18, Configuring Virtual Targets](#)
- [Task 19, Configuring Partitions](#)
- [Task 20, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 21, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 22, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home that you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#).

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).

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

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle SOA Suite - 12.2.1.3.0 [soa]**

The following additional templates should already be selected, because they were used to create the initial domain:

- Oracle Enterprise Manager - 12.2.1.3.0[em]
- Oracle WSM Policy Manager - 12.2.1.3.0[oracle_common]
- Oracle JRF - 12.2.1.3.0[oracle_common]
- WebLogic Coherence Cluster Extension - 12.2.1.3.0[wlserver]

And the following template should also be selected, because you already configured WebCenter Content:

- Oracle Universal Content Management - Content Server - 12.2.1.3.0[wccontent]

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

Task 3 Configuring High Availability Options

This screen appears for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. After you select HA Options for a cluster, all subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply HA options (that is, the Configuration Wizard creates the JDBC stores and configures ASM for them).

On the High Availability Options screen:

- Select **Enable Automatic Service Migration with Database Basis**.
- Set **JTA Transaction Log Persistence** to **JDBC TLog Store**.
- Set **JMS Server Persistence** to **JMS JDBC Store**.

**Note:**

Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an Oracle database and makes resources available for all the servers in the cluster. So, the Configuration Wizard steps assume that the JDBC persistent stores are used along with Automatic Service Migration.

When you choose JDBC persistent stores, additional unused File Stores are automatically created but are not targeted to your clusters. Ignore these File Stores.

If, for any reason, you want to use File Stores, you can retain the default values for TLOGs and JMS persistent store options in this screen and configure them in a shared location later. See [Task 9, Selecting Advanced Configuration](#). Shared location is required to resume JMS and JTA in a failover scenario.

You can also configure TLOGs and JMS persistent stores manually in a post step. For information about the differences between JDBC and File Stores, and for specific instructions to configure them manually, see [Using Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#).

Click **Next**.

Task 4 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are prepopulated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain. In the RCU Data screen:

- Verify that **Vendor** is Oracle and **Driver** is *Oracle's Driver (Thin) for Service Connections; Versions: Any.
- Verify that **Connection Parameters** is selected.
- Verify and ensure that credentials in all the fields are the same as those provided during the configuration of Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operation is successful.

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.

**Tip:**

For more information about the **RCU Data** option, see Understanding the Service Table Schema in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

For more information about the other options on this screen, see Datasource Defaults in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 5 Specifying JDBC Component Schema Information

On the JDBC Component Schema screen, select all the SOA schemas in the table. When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.

Click **Convert to GridLink**, and then click **Next**.

Task 6 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information that is required to connect to the RAC database and component schemas, as shown in the following table.

Element	Description and Recommended Value
SCAN, Host Name, and Port	Select the SCAN check box. In the Host Name field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database. In the Port field, enter the SCAN listening port for the database (for example, 1521).
ONS Host and Port	In the ONS Host field, enter the SCAN address for the Oracle RAC database. In the Port field, enter the ONS Remote port (typically, 6200). These values are required when connecting to Oracle 11g databases but optional when connecting to Oracle database 12c and higher. If you are using an Oracle 12c database, the ONS list is automatically provided from the database to the driver.
Enable Fan	Verify that the Enable Fan check box is selected, so that the database can receive and process FAN events.

Task 7 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections that you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

For more information about the other options on this screen, see Test Component Schema in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 8 Keystore

Use this screen to specify details about the keystore to be used in the domain.

For a typical enterprise deployment, you can leave the default values. See *Keystore in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 9 Selecting Advanced Configuration

To complete domain configuration for the topology, select **Topology** on the Advanced Configuration screen.



Note:

JDBC stores are recommended and selected in [Task 3, Configuring High Availability Options](#) so there is no need to configure File Stores. If you choose File Stores in [Task 3, Configuring High Availability Options](#), you have to select the File Stores option here to configure them in a shared location in `ORACLE_RUNTIME/domain_name/SOA_Cluster/jms`. Shared location is required to resume JMS and JTA in a failover scenario.

Task 10 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server for Oracle SOA Suite appears in the list of servers. This server was created automatically by the Oracle SOA Suite configuration template that you selected in [Task 2, Selecting the Configuration Template](#).

Perform the following tasks to modify the default Oracle SOA Suite Managed Server and create a second Oracle SOA Suite Managed Server:

1. Rename the default Oracle SOA Suite Managed Server to `WLS_SOA1`.
2. Click **Add** to create a new Oracle SOA Suite Managed Server, and name it `WLS_SOA2`.



Tip:

The server names recommended here are used throughout this document; if you choose different names, be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Oracle SOA Suite Managed Server.

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

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WLS_SOA1	WCCHOST1	8001	No	Disabled	SOA-MGD-SVRS-ONLY, WSM-PM-MAN-SVR, WSM-CACHE-SVR, JRF-MAN-SVR
WLS_SOA2	WCCHOST2	8001	No	Disabled	SOA-MGD-SVRS-ONLY, WSM-PM-MAN-SVR, WSM-CACHE-SVR, JRF-MAN-SVR

Task 11 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle SOA Suite software.

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify S0A_Cluster in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select Unspecified.

Note:

By default, server instances in a cluster communicate with one another by using unicast. If you want to change your cluster communications to use multicast, refer to Considerations for Choosing Unicast or Multicast in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

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

Task 12 Assigning Server Templates

Click **Next** to continue.

Task 13 Configuring Dynamic Servers

Verify that all dynamic server options are disabled for clusters that are to remain as static clusters. To configure dynamic servers:

1. Confirm that the **Dynamic Cluster**, **Calculated Listen Port**, and **Calculated Machine Names** checkboxes on this screen are unchecked.
2. Confirm the **Server Template** selection is **Unspecified**.
3. Click **Next**.

Task 14 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign WLS_S0A1 and WLS_S0A2 to the new cluster S0A_Cluster:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, S0A_Cluster.
2. In the Servers pane, assign WLS_S0A1 to S0A_Cluster by doing one of the following:
 - Click WLS_S0A1 Managed Server once to select it, and then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
 - Double-click WLS_S0A1 to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign WLS_S0A2 to S0A_Cluster.

For more information about the options on this screen, see Assign Servers to Clusters in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 15 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 9991, as it was defined during the initial Infrastructure domain creation.

For Coherence licensing information, see Oracle Coherence Products in *Oracle Fusion Middleware Licensing Information User Manual*.

Task 16 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain.

Click **Next** to proceed.

Task 17 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Oracle SOA Suite Managed Servers you just created to the corresponding machines in the domain.

Assign WLS_S0A1 to WCCHOST1, and assign WLS_S0A2 to WCCHOST2.

For more information about the options on this screen, see Assign Servers to Machines in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 18 Configuring Virtual Targets

Click **Next**.

Task 19 Configuring Partitions

Click **Next**.

Task 20 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains detailed configuration information for the domain that you are about to extend. Review the details of each item on the screen and verify that the information is correct.

If you need to make any changes, you can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Click **Update** to execute the domain extension.

In the Configuration Progress screen, click **Next** when it finishes.

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

Task 21 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen shows the following items about the domain that you just configured, including:

- Domain Location
- Administration Server URL

Make a note of both these items, because you need them later; you need the domain location to access the scripts used to start the Administration Server, and you need the Administration Server URL to access the WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control.

Click **Finish** to dismiss the Configuration Wizard.

If the Admin Server was running during the domain extension process, restart the server before you continue.

Task 22 Start the Administration Server

Start the Administration Server to ensure that the changes that you have made to the domain have been applied.

After you complete extending the domain with static clusters, go to [Targeting Adapters Manually](#).

Extending the Domain with Dynamic Clusters

Follow the instructions in this section to extend the domain for Oracle SOA Suite, with dynamic clusters.

Note:

This procedure assumes that you are extending an existing domain. If your needs do not match the instructions given in the procedure, ensure that you make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks.

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying the Database Configuration Type](#)
- [Task 4, Specifying JDBC Component Schema Information](#)
- [Task 5, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 6, Testing the JDBC Connections](#)
- [Task 7, Keystore](#)
- [Task 8, Selecting Advanced Configuration](#)
- [Task 9, Configuring Managed Servers](#)
- [Task 10, Configuring a Cluster](#)
- [Task 11, Assigning Server Templates](#)
- [Task 12, Configuring Dynamic Servers](#)
- [Task 13, Assign Servers to Clusters](#)
- [Task 14, Configuring Coherence Clusters](#)
- [Task 15, Verifying the Existing Machines](#)
- [Task 16, Assigning Servers to Machines](#)
- [Task 17, Virtual Targets](#)
- [Task 18, Partitions](#)
- [Task 19, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 20, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 21, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created when you created the initial domain.

Do not enter the value of the `MSERVER_HOME` variable, which represents the location of the Managed Servers domain directory.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).

Tip:

More information about the other options on this screen can be found in Configuration Type in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle SOA Suite - 12.2.1.3.0 [soa]**

The following additional templates should already be selected, because they were used to create the initial domain:

- Oracle Enterprise Manager - 12.2.1.3.0 [em]
- Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]
- Oracle JRF - 12.2.1.3.0 [oracle_common]
- WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]

And the following template should also be selected, because you already configured WebCenter Content:

- Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]

Tip:

More information about the options on this screen can be found in Templates in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are prepopulated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain. On the RCU Data screen:

- Verify that **Vendor** is Oracle and **Driver** is *Oracle's Driver (Thin) for Service Connections; Versions: Any.
- Verify that **Connection Parameters** is selected.

- Verify and ensure that credentials in all the fields are the same as those provided during the configuration of Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operation is successful:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

Click **Next**.

 Tip:

For more information about the **RCU Data** option, see Understanding the Service Table Schema in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.
For more information about the other options on this screen, see Datasource Defaults in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 4 Specifying JDBC Component Schema Information

On the JDBC Component Schema screen, select all the SOA schemas in the table. When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.
Click **Convert to GridLink** and click **Next**.

Task 5 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information that is required to connect to the RAC database and component schemas, as shown in the following table.

Element	Description and Recommended Value
SCAN, Host Name, and Port	Select the SCAN check box. In the Host Name field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database. In the Port field, enter the SCAN listening port for the database (for example, 1521).
ONS Host and Port	In the ONS Host field, enter the SCAN address for the Oracle RAC database. In the Port field, enter the ONS Remote port (typically, 6200). These values are required when connecting to Oracle 11g databases but optional when connecting to Oracle database 12c and higher. If you are using an Oracle 12c database, the ONS list is automatically provided from the database to the driver.

Element	Description and Recommended Value
Enable Fan	Verify that the Enable Fan check box is selected, so the database can receive and process FAN events.

Task 6 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.



Tip:

For more information about the other options on this screen, see Test Component Schema in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 7 Keystore

Use this screen to specify details about the keystore to be used in the domain.

For a typical enterprise deployment, you can leave the default values.

See Keystore in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 8 Selecting Advanced Configuration

To complete domain configuration for the topology, select **Topology** and **Deployments and Services** on the Advanced Configuration screen.

Task 9 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server for Oracle SOA Suite appears in the list of servers. This server was created automatically by the Oracle SOA Suite configuration template that you selected in [Task 2, Selecting the Configuration Template](#).

SOA Static Managed Server definitions are not needed for dynamic cluster configuration. To remove the default Managed Server, complete the following steps:

1. Click the soa_server1 managed server and click **Delete**.
2. Click **Next**.

Task 10 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle SOA Suite software.

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify SOA_Cluster in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select SOA-DYN-CLUSTER-ONLY.

 Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to Considerations for Choosing Unicast or Multicast in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

 Tip:

More information about the options on this screen can be found in Clusters in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 11 Assigning Server Templates

To configure a template, complete the following steps:

1. Verify that `soa-server-template` is selected in the **Name** field.
2. Specify `8000` in the **Listen Port** field.
3. Leave the **Enable SSL** option unchecked.
4. Click **Next**.

Task 12 Configuring Dynamic Servers

Use the Dynamic Clusters screen to configure the required clusters:

1. Verify `SOA_Cluster` is listed in the **Cluster Name** field.
2. Specify `WLS_SOA` in the **Server Name Prefix** field.
3. From the **Server Template** drop-down list, select `soa-server-template`.
4. Specify `2` in the **Dynamic Cluster Size** field.
5. Specify `WCCHOST*` in the **Machine Name Match Expression** field and select **Calculated Machine Names**.

 Note:

The dynamic cluster **Calculated Machine Names** and **Machine Name Match Expression** attributes control how server instances in a dynamic cluster are assigned to a machine. If the **Calculated Machine Names** attribute is set to *False*, the dynamic servers are not assigned to a machine. If the **Calculated Machine Names** attribute is set to *True*, the **Machine Name Match Expression** attribute is used to select the set of machines that is used for the dynamic servers. If the **Machine Name Match Expression** attribute is not set, all the machines in the domain are selected. Assignments are made by using a round robin algorithm.

6. Select **Calculated Listen Ports** and **Dynamic Cluster** fields.

 Note:

Dynamic clusters with the Calculated Listen Port option selected have incremental port numbers for each dynamic managed server that is created automatically: dynamic server 1 will use Listen Port+1, dynamic server 2 will use Listen Port+2.

Since the Listen Port configured is 8000 and calculated ports is checked, SOA dynamic servers use the following port numbers:

- WLS_SOA1 server listens in 8001 port
- WLS_SOA2 server listens in 8002 port

7. Click **Next**.

 Note:

The Configuration Wizard does not allow you to specify a specific listen address for dynamic servers. For information about setting a specific listen address for WebLogic servers that are members of a dynamic cluster, see [Configuring Listen Addresses in Dynamic Cluster Server Templates](#).

Task 13 Assign Servers to Clusters

This screen appears during dynamic cluster configurations when static configured clusters and managed servers exist, even if the current extension does not include any new static servers.

For the SOA extension with dynamic clusters, no changes are needed.

Click **Next**.

Task 14 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 9991, as it was defined during the initial Infrastructure domain creation.

 Note:

For Coherence licensing information, see Oracle Coherence Products in *Oracle Fusion Middleware Licensing Information User Manual*.

Task 15 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines that you created when creating the initial Infrastructure domain.

Click **Next**.

Task 16 Assigning Servers to Machines

Click **Next**.

Task 17 Virtual Targets

Click **Next**.

Task 18 Partitions

Click **Next**.

Task 19 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains detailed configuration information for the domain that you are about to extend. Review the details of each item on the screen and verify that the information is correct.

If you need to make any changes, you can go back to any previous screen either by using the **Back** button or by selecting the screen in the navigation pane.

Click **Update** to execute the domain extension.

In the Configuration Progress screen, click **Next** when it finishes.

Tip:

More information about the options on this screen can be found in *Configuration Summary in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Task 20 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen shows the following items about the domain that you just configured, including:

- Domain Location
- Administration Server URL

Make a note of both these items, because you need them later; you need the domain location to access the scripts used to start the Administration Server, and you need the Administration Server URL to access the WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control.

Click **Finish** to dismiss the configuration wizard.

If the Admin Server was running during the domain extension process, restart the server before you continue.

Task 21 Start the Administration Server

Start the Administration Server to ensure that the changes that you have made to the domain have been applied.

Targeting Adapters Manually

Only core adapters are targeted to the SOA cluster after you run the Configuration Wizard. You must target second-tier adapters manually, on a need basis.

The following second-tier adapters have to be targeted manually:

Note:

Some of these adapters may not be available with the default installation. See [Oracle Technology Network for Adapter availability](#).

- MSMQAdapter
- SocketAdapter

- OracleBamAdapter
- CoherenceAdapter
- SAPAdapter
- SiebelAdapter
- ERPAdapter
- Oracle SalesCloudAdapter
- RightNowAdapter
- EloquaAdapter
- NetSuiteAdapter
- LdapAdapter
- JDEWorldAdapter

To target a second-tier adapter manually:

1. Navigate to and log into the Oracle WebLogic Server Administration Console. For example: `http://ADMINVHN:7001/console`.

 Note:

If you have already configured web tier, use `http://admin.example.com/console`.

2. In the left pane of the console, click **Deployments**.
3. Locate and click the name of the adapter in the Summary of the Deployments table.
4. Click **Lock & Edit**.
5. In the **Targets** tab, select **SOA_Cluster**.

 Note:

If you are deploying MFT, select **MFT_Cluster** as the target.

6. Click **Save**.
7. Activate the changes.
8. In the left pane of the console, click **Deployments** and verify that the adapter is in the Active state.

Propagating the Extended Domain to the Domain Directories and Machines

After you have extended the domain with the Oracle WebCenter Content instances, and you have restarted the Administration Server on WCCHOST1, you must then propagate the domain changes to the domain directories and machines.

[Table 13-1](#) summarizes the steps required to propagate the changes to all the domain directories and machines.

Note that there is no need to propagate the updated domain to the WEBHOST1 and WEBHOST2 machines because there are no changes to the Oracle HTTP Server instances on those host computers.

Table 13-1 Summary of Tasks Required to Propagate the Domain Changes to Domain Directories and Machines

Task	Description	More Information
Pack up the Extended Domain on WCCHOST1	Use the pack command to create a new template JAR file that contains the new Oracle SOA Suite Managed Servers configuration. When you pack up the domain, create a template JAR file called wccdomaintemplateExtSOA.jar.	Packing Up the Extended Domain on WCCHOST1
Unpack the Domain in the Managed Servers directory on WCCHOST1	Unpack the template JAR file in the Managed Servers directory on WCCHOST1 local storage.	Unpacking the Domain in the Managed Servers Domain Directory on WCCHOST1
Unpack the Domain on WCCHOST2	Unpack the template JAR file in the Managed Servers directory on the WCCHOST2local storage.	Unpacking the Domain on WCCHOST2

- [Packing Up the Extended Domain on WCCHOST1](#)
- [Unpacking the Domain in the Managed Servers Domain Directory on WCCHOST1](#)
- [Unpacking the Domain on WCCHOST2](#)

Packing Up the Extended Domain on WCCHOST1

Use the following steps to create a template JAR file that contains the domain configuration information:

1. Log in to WCCHOST1 and run the pack command to create a template JAR file as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true \
          -domain=ASERVER_HOME \
          -template=full_path/wccdomaintemplateExtSOA.jar \
          -template_name=wcc_domain_template_extension_soa \
```

```
-log=/tmp/pack_soa.log \
-log_priority=debug
```

In this example:

- Replace *ASERVER_HOME* with the actual path to the domain directory that you created on the shared storage device.
 - Replace *full_path* with the complete path to the directory where you want the template jar file saved.
 - *wccdomaintemplateExtSOA.jar* is a sample name for the JAR file that you are creating, which contains the domain configuration files, including the configuration files for the Oracle HTTP Server instances.
 - *wcc_domain_template_extension_soa* is the name assigned to the domain template file.
2. Make a note of the location of the template JAR file that you just created with the *pack* command.

 Tip:

For more information about the *pack* and *unpack* commands, see *Overview of the Pack and Unpack Commands* in *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

Unpacking the Domain in the Managed Servers Domain Directory on WCCHOST1

To copy the updated domain configuration information from the Administration Server domain directory to the Managed Servers domain directory:

1. Log in to WCCHOST1 if you haven't already.
2. If you haven't already, create the recommended directory structure for the Managed Server domain on the WCCHOST1 local storage device.
Use the examples in [File System and Directory Variables Used in This Guide](#) as a guide.
3. Run the *unpack* command to unpack the template in the domain directory onto the local storage, as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME \
-overwrite_domain=true \
-template=/full_path/wccdomaintemplateExtSOA.jar \
-log_priority=DEBUG \
-log=/tmp/unpack.log \
-app_dir=APPLICATION_HOME
```

 Note:

The `-overwrite_domain` option in the `unpack` command allows you to unpack a managed server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the managed server domain directory, they must be restored after this unpack operation.

Additionally, to customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it to, for example, add custom libraries to the WebLogic Server classpath, specify additional JAVA command-line options for running the servers, or specify additional environment variables. Any customizations that you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when you use the `pack` and `unpack` commands.

In this example:

- Replace `MSERVER_HOME` with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain is unpacked.
- Replace `/full_path/wccdomaintemplateExtSOA.jar` with the complete path and file name of the domain template jar file that you created when you ran the `pack` command to pack up the domain on the shared storage device.
- Replace `APPLICATION_HOME` with the complete path to the applications directory for the domain on shared storage. See [File System and Directory Variables Used in This Guide](#)

 Tip:

For more information about the `pack` and `unpack` commands, see *Overview of the Pack and Unpack Commands* in *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Change directory to the newly created `MSERVER_HOME` directory and verify that the domain configuration files were copied to the correct location on the `WCCHOST1` local storage device.

Unpacking the Domain on WCCHOST2

This procedure assumes you have copied the file that you created earlier in a location that is accessible from both `WCCHOST1` and `WCCHOST2`; such as the `ASERVER_HOME` directory, which is located on the shared storage filer:

1. Log in to `WCCHOST2`
2. If you haven't already, create the recommended directory structure for the Managed Server domain on the `WCCHOST2` storage device.

Use the examples in [File System and Directory Variables Used in This Guide](#) as a guide.

3. Make sure the `wccdomaintemplateExtSOA.jar` accessible to `WCCHOST2`.

For example, if you are using a separate shared storage volume or partition for `WCCHOST2`, then copy the template to the volume or partition mounted to `WCCHOST2`.

4. Run the `unpack` command to unpack the template in the domain directory onto the local storage, as follows:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME \
            -overwrite_domain=true \
            -template=/full_path/wccdomaintemplateExtSOA.jar \
            -log_priority=DEBUG \
            -log=/tmp/unpack.log \
            -app_dir=APPLICATION_HOME
```

Note:

The `-overwrite_domain` option in the `unpack` command allows unpacking a managed server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. If any modifications had been applied to the start scripts and ear files in the managed server domain directory, they must be restored after this unpack operation.

Additionally, to customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it to, for example, add custom libraries to the WebLogic Server classpath, specify additional JAVA command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the `pack` and `unpack` commands.

In this example:

- Replace `MSERVER_HOME` with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- Replace `/full_path/wccdomaintemplateExtSOA.jar` with the complete path and file name of the domain template jar file that you created when you ran the `pack` command to pack up the domain on the shared storage device.
- Replace `APPLICATION_HOME` with the complete path to the Application directory for the domain on shared storage. See [File System and Directory Variables Used in This Guide](#).

**Tip:**

For more information about the pack and unpack commands, see Overview of the Pack and Unpack Commands in *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

5. Change directory to the newly created MSERVER_HOME directory and verify that the domain configuration files were copied to the correct location on the WCCHOST2 local storage device.

Updating the NodeManager Configuration After Unpacking the Domain

When extending a domain, the nodemanager.properties file in MSERVER_HOME may be overwritten with some values from the nodemanager.properties file for ASERVER_HOME. Specifically, the ListenAddress and/or CustomIdentityAlias values can be reset.

**Notes::**

- The ListenAddress may typically get reset on the MSERVER_HOME nodemanager residing on the same host as the ASERVER_HOME nodemanager. In this topology, WCCHOST1.
- For domain extensions prior to [Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer](#), steps 2 through 4 regarding the CustomIdentityAlias may not be applicable.

For the MSERVER_HOME/nodemanager/nodemanager.properties file on each host:

1. Verify the correct ListenAddress parameter value and reset it, if required.

```
grep ListenAddress MSERVER_HOME/nodemanager/nodemanager.properties
```

2. Confirm the list of configured Identity Aliases from the domain configuration file as a reference for the next command.

```
grep server-private-key-alias ASERVER_HOME/config/config.xml | sort  
| uniq
```

 Note:

When using Dynamic Clusters, this listing will present only the ADMINVHN and wildcard certificate identity aliases.

Use the appropriate host-specific certificate identity aliases when updating the `nodemanager.properties` `CustomIdentityAlias` property in the next instruction.

3. Verify the current `nodemanager.properties` `CustomIdentityAlias` parameter value matches the alias for the host.

```
grep CustomIdentityAlias MSERVER_HOME/nodemanager/  
nodemanager.properties
```

4. Reset the `CustomIdentityAlias` parameter value to the correct alias string appropriate for the current host, if required.
5. Restart the `nodemanager` process:

```
kill `ps -eaf | grep weblogic.NodeManager | grep MSERVER_HOME |  
grep -v grep | awk '{print $2}'` \  
nohup MSERVER_HOME/bin/startNodeManager.sh > MSERVER_HOME/  
nodemanager/nodemanager.out 2>&1 &
```

6. Stop and restart the `AdminServer` once all node managers are appropriately configured and online.

 Note:

For more information about the `CustomIdentityAlias` parameter, see [Configuring Node Manager to Use the Custom Keystores](#).

Modifying the Upload and Stage Directories to an Absolute Path in an Enterprise Deployment

After you configure the domain and unpack it to the Managed Server domain directories on all the hosts, verify and update the upload and stage directories for Managed Servers in the new clusters. Also, update the upload directory for the `AdminServer` to have the same absolute path instead of relative, otherwise deployment issues can occur. If you implement dynamic clusters, the configuration of the server template assigned to each newly added cluster should be verified and updated, otherwise, verify and update every statically-defined Managed Server for the newly added clusters.

 Note:

This option is applicable only for static clusters.

This step is necessary to avoid potential issues when you perform remote deployments and for deployments that require the stage mode.

To update the directory paths for the Deployment Stage and Upload locations, complete the following steps:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Navigate to and edit the appropriate objects for your cluster type.
 - a. For Static Clusters, navigate to **Servers** and click the name of the Managed Server you want to edit.
 - b. For Dynamic Clusters, navigate to **Clusters > Server Templates**, and click on the name of the server template to be edited.
5. For each new Managed Server or Server Template to be edited:
 - a. Click the **Configuration** tab, and then click the **Deployment** tab.
 - b. Verify that the **Staging Directory Name** is set to the following:

MSERVER_HOME/servers/server_or_template_name/stage

Replace *MSERVER_HOME* with the full path for the *MSERVER_HOME* directory.

If you use static clusters, update with the correct name of the Managed Server that you are editing.

If you use dynamic clusters, leave the template name intact.

For example: */u02/oracle/config/domains/wccedg_domain/servers/XYZ-server-template/stage*

- c. Update the **Upload Directory Name** to the following value:
- ASERVER_HOME/servers/AdminServer/upload*
- Replace *ASERVER_HOME* with the directory path for the *ASERVER_HOME* directory.
- d. Click **Save**.
 - e. Return to the Summary of Servers or Summary of Server Templates screen as applicable.
 6. Repeat the previous steps for each of the new managed servers or dynamic cluster server templates.
 7. Navigate to and update the Upload Directory Name value for the AdminServer:
 - a. Navigate to **Servers**, and select the AdminServer.
 - b. Click the **Configuration** tab, and then click the **Deployment** Tab.
 - c. Verify that the **Staging Directory Name** is set to the following absolute path:

ASERVER_HOME/servers/AdminServer/stage

- d. Update the **Upload Directory Name** to the following absolute path:

ASERVER_HOME/servers/AdminServer/upload

Replace *ASERVER_HOME* with the directory path for the *ASERVER_HOME* directory.

- e. Click **Save**.
8. When you have modified all the appropriate objects, click **Activate Changes**.
9. Restart all Managed Servers for the changes to take effect.

**Note:**

If you continue directly with further domain configurations, a restart to enable the stage and upload directory changes is not strictly necessary at this time.

Configuring Listen Addresses When Using Dynamic Clusters

The default configuration for dynamic managed servers in dynamic clusters is to listen on all available network interfaces. In most cases, the default configuration may be undesirable. To limit the listen address to a specific address when you use dynamic clusters, see [Configuring Listen Addresses in Dynamic Cluster Server Templates](#). Reverify the test URLs that are provided in the previous sections after you change the listen address and restart the clustered managed servers.

Starting and Validating the WLS_SOA1 Managed Server

Now that you have extended the domain, started the Administration Server, and propagated the domain to the other hosts, you can start the newly configured Oracle SOA Suite Managed Servers.

This process involves three tasks as described in the following sections.

- [Starting the WLS_SOA1 Managed Server](#)
- [Adding the SOAAdmin Role to the Administrators Group](#)
- [Validating the Managed Server by Logging in to the SOA Infrastructure](#)

Starting the WLS_SOA1 Managed Server

To start the WLS_SOA1 Managed Server:

1. Enter the following URL into a browser to display the Fusion Middleware Control login screen:

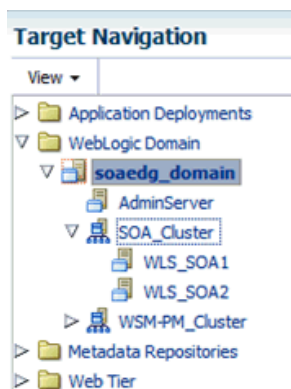
`http://ADMINVHN:7001/em`

**Note:**

If you have already configured web tier, use `http://admin.example.com/console`.

2. Sign in to the Fusion Middleware Control by using the administrator's account. For example: `weblogic_wcc`.

3. In the **Target Navigation** pane, expand the domain to view the Managed Servers in the domain.



4. Select only the **WLS_SOA1** Managed Server and click **Start Up** on the Oracle WebLogic Server toolbar.



Note:

SOA Servers depend on the policy access service to be functional. This implies that the WSM-PM Managed Servers in the domain need to be up and running and reachable before the SOA servers are started.

5. When the startup operation is complete, navigate to the Domain home page and verify that the WLS_SOA1 Managed Server is up and running.

Adding the SOAAdmin Role to the Administrators Group

Before you validate the Oracle SOA Suite configuration on the WLS_SOA1 Managed Server, add the SOAAdmin administration role to the enterprise deployment administration group (WCCAdministrators).

To perform this task, refer to [Configuring Roles for Administration of an Enterprise Deployment](#).

Validating the Managed Server by Logging in to the SOA Infrastructure

After you add the SOAAdmin role to the SOA Administrators group, you can then validate the configuration of the Oracle SOA Suite software on the WLS_SOA1 Managed Server as follows:

1. Use your web browser to navigate to the following URL:
`http://WCCHOST1:8001/soa-infra/`
2. Log in by using the enterprise deployment administrator user credentials (weblogic_wcc).

You should see a web page with the following title:

Welcome to the Oracle SOA Platform on WebLogic

Starting and Validating the WLS_SOA2 Managed Server

After you validate the successful configuration and startup of the WLS_SOA1 Managed Server, you can start and validate the WLS_SOA2 Managed Server.

To start and validate the WLS_SOA2 Managed Server, use the procedure in [Starting and Validating the WLS_SOA1 Managed Server](#) for WLS_SOA2 Managed Server.

For validation of the URL, enter the following URL in your web browser and log in by using the enterprise deployment administrator user (weblogic_soa):

For Static cluster:

`http://WCCHOST2:8001/soa-infra/`

For Dynamic cluster:

`http://WCCHOST2:8002/soa-infra/`

Configuring Oracle HTTP Server for the Extended Domain

The following sections describe how to configure the Oracle HTTP Server instances so they route requests for both public and internal URLs to the proper clusters in the enterprise topology.

- [Configuring Oracle HTTP Server for SOA in an Oracle WebCenter Content Enterprise Deployment](#)
- [Validating the Oracle SOA Suite URLs Through the Load Balancer](#)

Configuring Oracle HTTP Server for SOA in an Oracle WebCenter Content Enterprise Deployment

Configure the virtual host configuration files so that requests are routed properly to the Oracle SOA Suite clusters:

1. Log in to WEBHOST1 and change directory to the configuration directory for the first Oracle HTTP Server instance (ohs1):

```
cd WEB_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
```

2. Edit the `wccinternal_vh.conf` file and add the following directives inside the `<VirtualHost>` tags:

 Note:

- The URL entry for /workflow is optional. It is for workflow tasks associated with Oracle ADF task forms. The /workflow URL itself can be a different value, depending on the form.
- Configure the port numbers appropriately as assigned for your static or dynamic cluster. Dynamic clusters with the Calculate Listen Port option selected will have incremental port numbers for each dynamic managed server created.
- The WebLogicCluster directive needs only a sufficient number of redundant server:port combinations to guarantee initial contact in case of a partial outage. The actual total list of cluster members is retrieved automatically upon first contact with any given node.

```
# soa-infra
<Location /soa-infra>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

# SOA inspection.wsil
<Location /inspection.wsil>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

# Worklist
<Location /integration>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>
```



```
# Workflow
<Location /workflow>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

#Required if attachments are added for workflow tasks
<Location /ADFAttachmentHelper>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

# SOA composer application
<Location /soa/composer>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

<Location /frevvo>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>
</VirtualHost>
```

3. Copy the `wccinternal_vh.conf` to the configuration directory for the second Oracle HTTP Server instance (ohs2):

```
WEB_DOMAIN_HOME/config/fmwconfig/components/ohs2/moduleconf/
```

4. Edit the `wccinternal_vh.conf` to change any references to `WEBHOST1` to `WEBHOST2` in the `<VirtualHost>` directives.
5. Restart both Oracle HTTP servers.

Example 13-1 Sample Content for the `wccinternal_vh.conf` File

```
<VirtualHost WEBHOST1:7777>
  ServerName http://wccinternal.example.com:80
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit

# WSM-PM
<Location /wsm-pm>
  WebLogicCluster WCPHOST1:7010,WCPHOST2:7010
  WLSRequest ON
  WLProxySSL OFF
  WLProxySSLPassThrough OFF
</Location>

#soa-infra
<Location /soa-infra>
  WLSRequest ON
  WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
  WLProxySSL OFF
```

```

        WLProxySSLPassThrough OFF
    </Location>

    # SOA inspection.wsil
    <Location /inspection.wsil>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    # Worklist
    <Location /integration>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    # UMS prefs
    <Location /sdpmessaging/userprefs-ui>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    # Default to-do taskflow
    <Location /DefaultToDoTaskFlow>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    # Workflow
    <Location /workflow>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    #Required if attachments are added for workflow tasks
    <Location /ADFAttachmentHelper>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    # SOA composer application
    <Location /soa/composer>
        WLSRequest ON
        WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
        WLProxySSL OFF
        WLProxySSLPassThrough OFF
    </Location>

    <Location /frevvo>
        WLSRequest ON

```

```
WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
WLProxySSL OFF
WLProxySSLPassThrough OFF
</Location>
</VirtualHost>
```

Validating the Oracle SOA Suite URLs Through the Load Balancer

To validate the configuration of the Oracle HTTP Server virtual hosts and to verify that the hardware load balancer can route requests through the Oracle HTTP Server instances to the application tier:

1. Verify that the server status is reported as **Running** in the Administration Console.
If the server is shown as **Starting** or **Resuming**, wait for the server status to change to **Started**. If another status is reported (such as **Admin** or **Failed**), check the server output log files for errors.
2. Verify that you can access these URLs:
 - <http://wccinternal.example.com/soa-infra>
 - <http://wccinternal.example.com/integration/worklistapp>
 - <http://wccinternal.example.com/sdpMessaging/userprefs-ui>
 - <http://wccinternal.example.com/soa/composer>
 - <http://wccinternal.example.com/wsm-pm>

Post-Configuration Steps for Oracle SOA Suite

After you install and configure Oracle SOA Suite, consider the following post-configuration tasks.

- [Configuring Oracle Adapters for Oracle SOA Suite](#)
- [Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer](#)
- [Considerations for Sync-Async Interactions in a SOA Cluster](#)
- [Updating FusionAppsFrontendHostUrl](#)

Configuring Oracle Adapters for Oracle SOA Suite

If the Oracle SOA Suite applications that you are developing take advantage of any of the Oracle adapters for Oracle SOA Suite, then you should make sure that the adapters are configured to work efficiently and securely in the enterprise topology.

See the following topics for more information.

- [Enabling High Availability for Oracle File and FTP Adapters](#)
- [Enabling High Availability for Oracle JMS Adapters](#)
- [Enabling High Availability for the Oracle Database Adapter](#)

Enabling High Availability for Oracle File and FTP Adapters

If the Oracle SOA Suite applications that you are developing or deploying require the Oracle File and FTP Adapters, you must configure the adapters for high availability in the enterprise deployment topology.

Use the following sections to complete this task.

- [Understanding the Oracle File and FTP Adapter Configuration](#)
- [Configuring the Oracle File Adapter in the Administration Console](#)
- [Editing the JCA File Within the Composite Application](#)
- [Configuring the Oracle FTP Adapter](#)

Understanding the Oracle File and FTP Adapter Configuration

The Oracle File and FTP adapters enable a BPEL process or an Oracle Mediator to read and write files on private file systems and on remote file systems through the File Transfer Protocol (FTP).

When configured properly, these adapters support high availability for an active-active topology with Oracle BPEL Process Manager and Oracle Mediator service engines for both inbound and outbound operations.

For general information about this task, see *Configuring Oracle File and FTP Adapters* in *Oracle Fusion Middleware Understanding Technology Adapters*. The instructions provided here are specific to the Oracle SOA Suite enterprise deployment.

Note:

The File Adapter picks up a file from the inbound directory, processes it, and then outputs a file to the output directory. Because the File Adapter is non-transactional, files can be processed twice. As a result, it is possible to get duplicate files when there is failover in the RAC backend or in the SOA managed servers.

Configuring the Oracle File Adapter in the Administration Console

To make the Oracle File Adapter highly available, first modify the Oracle File Adapter deployment descriptor for the connection-instance that corresponds to eis/HAFi leAdapter.

You can perform this task from the Oracle WebLogic Server console:

1. Navigate to and log into the Oracle WebLogic Server Administration Console.

For example:

`http://ADMINVHN:7001/console`

 Note:

If you have already configured web tier, use `http://admin.example.com/console`.

2. In the left pane of the console, click **Deployments**.
3. Locate the **FileAdapter** resource adapter in the Summary of Deployments table.
4. Click **FileAdapter** to display the Settings for FileAdapter page.
5. Click **Configuration**.
6. Click **Outbound Connection Pools**.
7. Expand **javax.resource.cci.ConnectionFactory** to see the configured connection factories.
8. Click **eis/HAFileAdapter**.
The Outbound Connection Properties for the connection factory appears.
9. Click **Lock & Edit**.
The property value column becomes editable (you can click on any of the rows in the Property Value column and modify the value).
10. Enter the values as shown in [Table 13-2](#).

 Note:

Update `controlDir` and check other values against the default values as mentioned in [Table 13-2](#).

Table 13-2 Values to Provide for the javax.resource.cci.Connectionfactory

Parameter	Description
<code>controlDir</code>	Enter the directory where you want the control files to be stored. You must set it to a shared location if multiple WebLogic Server instances run in a cluster. Structure the directory for shared storage as follows: <i>ORACLE_RUNTIME/domain_name/cluster_name/fadapter</i>
<code>inboundDataSource</code>	Set the value to <code>jdbc/SOADDataSource</code> .
<code>outboundDataSource</code>	Set the value to <code>jdbc/SOADDataSource</code> .
<code>outboundDataSourceLocal</code>	Set the value to <code>jdbc/SOALocalTxDataSource</code> . This is the data source where the schemas that corresponds to high availability are precreated.

Table 13-2 (Cont.) Values to Provide for the `javax.resource.cci.Connectionfactory`

Parameter	Description
<code>outboundLockTypeForWrite</code>	Set the value to <code>oracle</code> if you are using Oracle Database. By default the Oracle File and FTP Adapters use an in-memory mutex to lock outbound write operations. You must choose from the following values for synchronizing write operations: <code>memory</code>: The Oracle File and FTP Adapters use an in-memory mutex to synchronize access to the file system. <code>oracle</code>: The adapter uses Oracle Database sequence. <code>db</code>: The adapter uses a pre-created database table (<code>FILEADAPTER_MUTEX</code>) as the locking mechanism. You must use this option only if you are using a schema other than the Oracle Database schema. <code>user-defined</code>: The adapter uses a user-defined mutex. To configure the user-defined mutex, you must implement the mutex interface: <code>oracle.tip.adapter.file.Mutex</code> and then configure a new binding-property with the name <code>oracle.tip.adapter.file.mutex</code> and value as the fully qualified class name for the mutex for the outbound reference.
<code>workingDirectory</code>	Retain the default value.

11. Click **Save** after you update the properties. The Save Deployment Plan page appears.

12. Create `DEPLOY_PLAN_HOME` directory.

```
mkdir -p DEPLOY_PLAN_HOME/wccedg_domain
```

In this example, replace `DEPLOY_PLAN_HOME` with the actual path to the deployment plan directory that is defined in [File System and Directory Variables Used in This Guide](#).

13. Enter a shared storage location for the deployment plan **path** value. The directory structure is as follows:

```
DEPLOY_PLAN_HOME/wccedg_domain/FileAdapterPlan.xml
```

14. Click **OK** to save the storage location.

15. Click **Save** to save and then click **Activate Changes** to apply your changes to the File Adapter.

16. Update the deployment in the console:

- a. Click **Deployments**.
- b. Click **Lock & Edit**.
- c. Select the checkbox for the **File Adapter deployment**.
- d. Click **Update**.
- e. Select the option: **Update this application in place with new deployment plan changes (A deployment plan must be specified for this option.)**
- f. Click the **Change Path** button and select the `FileAdapterPlan.xml` file from the path to the shared storage location.
- g. Click **Finish**.
- h. Activate the changes.

17. Verify that the FileAdapter deployment is activated and running:

- a. In the Administration Console, click **Deployments** in the left pane.
- b. Locate the FileAdapter deployment in the Deployments table.
- c. If it is not in the active state, click the Control tab under **Summary of Deployments**, and then select **FileAdapter** under **Deployments**. Select **Start**, and then **Servicing All Requests**.
- d. Click **Yes**.

Editing the JCA File Within the Composite Application

After you have configured the FileAdapter deployment in the Administration Console, you can edit the .jca file that is included in the composite applications to be deployed so that they can use the connection factory that was configured in the previous steps, as shown in [Example 13-2](#).



Note:

The location attribute is set to eis/HADFileAdapter for the connection factory.

Example 13-2 Example of the File Adapter .JCA File Modifications for an Enterprise Deployment

```
<adapter-config name="FlatStructureOut"
  adapter="File Adapter"
  xmlns="http://platform.integration.oracle/blocks/adapter/fw/metadata">
  <connection-factory location="eis/HADFileAdapter" adapterRef=""/>
  <endpoint-interaction portType="Write_ptt"
    operation="Write">
    <interaction-spec className="oracle.tip.adapter.file.outbound.FileInteractionSpec">
      <property../>
      <property../>
    </interaction-spec>
  </endpoint-interaction>
</adapter-config>
```

Configuring the Oracle FTP Adapter

If your application requires an FTP Adapter, then repeat the procedures [Configuring the Oracle File Adapter in the Administration Console](#) and [Editing the JCA File Within the Composite Application](#), with the following differences:

- Locate the **FtpAdapter** deployment in the list of deployments in the Administration Console.
- Click **FtpAdapter** to display the Settings for the FtpAdapter page.
- Click **Configuration**.
- Click **Outbound Connection Pools**.
- Expand **javax.resource.cci.ConnectionFactory** to see the configured connection factories.
- Click **eis/Ftp/HADFtpAdapter**.

The Outbound Connection Properties for the connection factory appears.

- Click **Lock & Edit**.
- Modify the adapter properties for high availability. See [Table 13-2](#).
- Update the ControlDir property so it points to the following location:
`ORACLE_RUNTIME/domain_name/cluster_name/ftpadapter`
- Enter a shared storage location for the deployment plan. The directory structure is as follows:
`DEPLOY_PLAN_HOME/wccedg_domain/FtpAdapterPlan.xml`

Enabling High Availability for Oracle JMS Adapters

When the Oracle JMS adapter communicates with multiple servers in a cluster, the adapter's connection factory property `FactoryProperties` must list available servers. If it does not list servers, the connection establishes to only one random server. If that particular server goes down, no further messages are processed.

To verify the adapter's JCA connection factory:

1. Log into your Oracle WebLogic Server Administration Console using the following URL:

`http://ADMINVHN:7001/console`



Note:

If you have already configured Web tier, use `http://admin.example.com/console`.

2. Click **Deployments** in the left pane for Domain Structure.
3. Click **JmsAdapter** under **Summary of Deployments** on the right pane.
4. Click the **Configuration** tab.
5. Click the **Outbound Connection Pools** tab and expand `oracle.tip.adapter.jms.IJmsConnectionFactory` to see the configured connection factories.
6. Click **Lock & Edit**.
7. Click the specific instance you are using (for example, `eis/wls/Queue`). The Outbound Connection Properties for the connection factory opens.
8. In the **FactoryProperties** field (click on the corresponding cell under Property value), enter the following, all on one line, separated by semicolons:

`java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory;
java.naming.provider.url=cluster:t3://SOA_Cluster;
java.naming.security.principal=weblogic;
java.naming.security.credentials=mypassword`
9. Click **Save** after you update the properties. The Save Deployment Plan page appears.
10. (First time only) Enter a shared storage location for the deployment plan. The directory structure is as follows:

`DEPLOY_PLAN_HOME/soaedg_domain/JMSAdapterPlan.xml`

11. Click **OK** to commit the updated storage path.
12. Click **Save**.
13. Repeat steps 7 through 9 for all required connection factories.
14. Click **Activate Changes**.
15. Update the deployment in the console:
 - a. Click **Deployments**.
 - b. Click **Lock & Edit**.
 - c. Select the checkbox for the **JMS Adapter**.
 - d. Click **Update**.
 - e. Select **Update this application in place with new deployment plan changes (A deployment plan must be specified for this option.)** and select the deployment plan saved in a shared storage location; all servers in the cluster must be able to access the plan.
 - f. Click **Finish**.
 - g. Activate the changes.

Enabling High Availability for the Oracle Database Adapter

To ensure High Availability while leveraging the Oracle Database Adapter, the Logical Delete Polling Strategy is used normally as it performs better than a physical delete. However, when you have a clustered environment where multiple nodes are polling for the same data, a single record might get processed more than once. To avoid this problem, Oracle Database Adapter uses a distributed polling technique that uses an Oracle Database feature called skip locking.

If you were using the Logical Delete Polling Strategy approach previously, you can remove (in `db.jca`) or clear (Logical Delete Page of wizard) the `MarkReservedValue`, and you automatically get skip locking.

The benefits of using skip locking over a reserved value include:

- Skip locking scales better in a cluster and under load.
- All work is in one transaction (as opposed to update/reserve, then commit, then select in a new transaction), so the risk of facing a non-recoverable situation in a high availability environment is minimized.
- No unique `MarkReservedValue` must be specified. Previously, for this to work you would have to configure a complex variable, such as `R${weblogic.Name-2}-${IP-2}-${instance}`.

If you are using Logical Delete polling, and you set `MarkReservedValue`, skip locking is not used.

For more information, see "Scalability" and "Polling Strategies" in the Oracle Fusion Middleware User's Guide for Technology Adapters.

Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer

After you extend the domain with Oracle SOA Suite, you should also ensure that the Administration Server and Managed Servers can access the front-end SSL URL of the hardware load balancer.

This allows SOA Composite applications and web services to invoke callbacks and other communications with the front-end secure URL. See [Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer](#).

Considerations for Sync-Async Interactions in a SOA Cluster

In a SOA cluster, the following scenarios are not supported:

- Synchronous BPEL process with mid-process receive.
- Synchronous BPEL process calling asynchronous services.
- Callback from synchronous processes.

Updating FusionAppsFrontendHostUrl

You must configure Oracle Workflow with the appropriate URL so that the default-to-do tasks and custom tasks' details use the front-end load balancer to create task-display URLs.

To configure the appropriate URLs:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control with the username and password that you specified in the `boot.properties` file. See [Creating the boot.properties File](#).
2. In the left navigation tree, expand **WebLogic Domain**, and then click **System MBean Browser**.
3. Navigate to **Application Defined Mbean > oracle.as.soainfra.config**.
 - a. If you are configuring a static cluster, navigate to **Server: WLS_SOA1 > WorkflowConfig**.
 - b. If you are configuring a dynamic cluster, navigate to **Domain: wccedg_domain > WorkflowConfig**.
4. Click **human-workflow**.



Note:

In a clustered environment, there are multiple human-workflow Mbeans, one for every server in the cluster. Modify any one of them to update the property centrally in MDS for the entire cluster.

5. On the right panel, look for the **FusionAppsFrontendHostUrl** attribute.
6. For the **FusionAppsFrontendHostUrl** attribute, specify the value `*=https://wcc.example.com:443`.

7. Click **Apply**.

Enabling JDBC Persistent Stores

Oracle recommends that you use JDBC stores, which leverage the consistency, data protection, and high availability features of an Oracle database and makes resources available for all the servers in the cluster.

Follow these guidelines to ensure that you use JDBC stores, when you use static or dynamic clusters:

- **For static clusters**

If you have made the following selections in the High Availability Options screen, as recommended in this guide for static clusters, then JDBC persistent stores are already configured for both JMS and TLOGS:

- Set **JTA Transaction Log Persistence** to **JDBC TLog Store**.
- Set **JMS Server Persistence** to **JMS JDBC Store**.

- **For dynamic clusters**

You can configure only JMS Server persistence for dynamic clusters by using the Configuration Wizard. JTA Transaction Logs Persistence must be configured manually, if required. If you have made the following selections in the High Availability Options screen, as recommended in this guide for dynamic clusters, then JDBC persistent stores are already configured for JMS.

- Set **JMS Server Persistence** to **JMS JDBC Store**.
- Verify that **JTA Transaction Log Persistence** is set to **Default Persistent Store**.

Additional steps are needed to configure JTA Transaction Log with JDBC store. See [Roadmap for Configuring a JDBC Persistent Store for TLOGs](#).

In case you did not select JDBC for JMS and TLOGS persistent in the High Availability Options screen, you can still configure JDBC stores manually in a post step. For specific instructions to configure them manually, see [Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#).



Note:

The High Availability Options screen appears during the Configuration Wizard session for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. All subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.

Enabling Automatic Service Migration

To ensure high availability for the product installed in this chapter, you must configure service migration appropriately.

Follow these guidelines to ensure that you provide the required high availability for Weblogic services when you use static or dynamic clusters:

- **For static clusters**

Automatic Service Migration is already configured if you select **Enable Automatic Service Migration** with **Database Basis** in the High Availability Options screen.

The Database Leasing is already configured and the migratable targets are created with the appropriate policies for the cluster. If you have implemented these settings, validate the configuration, as described in [Validating Automatic Service Migration in Static Clusters](#).

In case you do not select this option during the Configuration Wizard session, you can configure automatic migration manually in a post step. For instructions to complete the steps for static clusters, see [Configuring Automatic Service Migration in an Enterprise Deployment](#).

- **For dynamic clusters**

You cannot configure Service Migration for dynamic clusters by using the Configuration Wizard, it needs to be configured manually. The following steps are needed:

- Configure the database leasing for the cluster.
- Set the appropriate migration policies for JTA Service and JMS Persistent Stores.

For instructions to complete the steps for dynamic clusters, see [Configuring Automatic Service Migration in an Enterprise Deployment](#).

 Note:

The High Availability Options screen appears during the Configuration Wizard session for the first time when you create a cluster that uses Automatic Service Migration or JDBC stores or both. All subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.

Extending the Domain to Include Inbound Refinery

You need to perform certain tasks in order to extend the enterprise deployment domain to include Inbound Refinery software.

- [Overview of Extending the Domain to Include Inbound Refinery](#)
Inbound Refinery is required for document conversion by Oracle WebCenter Content Server.
- [Extending the Domain for Inbound Refinery](#)
The instructions for extending the existing enterprise deployment domain with the Inbound Refinery software are detailed in this section.
- [Completing Postconfiguration and Verification Tasks for Inbound Refinery](#)
After extending the domain with the Inbound Refinery software, consider the following post-configuration and verification tasks.
- [Configuring the Inbound Refinery Managed Servers](#)
To initialize the configuration of an Inbound Refinery Managed Server, you need to access it only once through HTTP. You can do this directly at the Managed Server's listen address. An Inbound Refinery instance should not be placed behind an HTTP server.
- [Validating the Configuration of the Inbound Refinery Managed Servers](#)
To ensure that the Inbound Refinery Managed Servers you have created are properly configured, validate the configuration by logging in to Content Server and verifying that a file with an extension recognized as valid for conversion is correctly converted.

Overview of Extending the Domain to Include Inbound Refinery

Inbound Refinery is required for document conversion by Oracle WebCenter Content Server.

The actual number of Inbound Refinery Managed Servers varies depending on requirements. For availability reasons, Oracle recommends configuring at least two Inbound Refinery Managed Servers, each installed and configured on a separate machine. In the reference Oracle WebCenter Content enterprise deployment topology, Inbound Refinery will be configured on the same machine as Content Server.

Even though multiple Managed Servers are created in the process of extending the domain with Inbound Refinery in this enterprise deployment topology, each Inbound Refinery instance is completely independent. Inbound Refinery does not run in a cluster.

Extending the Domain for Inbound Refinery

The instructions for extending the existing enterprise deployment domain with the Inbound Refinery software are detailed in this section.

- [Starting the Configuration Wizard](#)
Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.
- [Navigating the Configuration Wizard Screens to Extend the Domain](#)

Starting the Configuration Wizard

Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.



Note:

If you added any customizations directly to the start scripts in the domain, those are overwritten by the configuration wizard. To customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it, for example, add custom libraries to the WebLogic Server classpath, specify Additional JAVA command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the **pack** and **unpack** commands.

To start the Configuration Wizard:

1. From the WebLogic Server Console, stop any managed servers that are modified by this domain extension. Managed Servers that are not effected can remain on-line.
2. For any managed servers to be modified, verify that the managed server shutdown has completed.
3. Stop the Administration Server once all managed servers are in a steady state.
4. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

Navigating the Configuration Wizard Screens to Extend the Domain

Follow the instructions in this section to update and configure the domain for the topology.

 Note:

You can use the same procedure described in this section to extend an existing domain. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the initial Administration Server domain home you created.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).

 Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Click **Next** to proceed.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Inbound Refinery - 12.2.1.3.0 [wccontent]**

The following additional templates should already be selected, because they were used to create the initial domain:

- **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
- **Oracle SOA Suite - 12.2.1.3.0 [soa]**
- **Oracle WebCenter Content - 12.2.1.3.0 [wcc]**
- **Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]**
- **Oracle JRF - 12.2.1.3.0 [oracle_common]**
- **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**

 Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Click **Next** to proceed.

Task 3 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, click **Next**.

Task 4 Testing the JDBC Connections

Click **Next** to continue.

Task 5 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following option on the Advanced Configuration screen:

Topology

Click **Next** to proceed.

Task 6 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Rename the default Managed Server to WLS_IBR1.
2. Click **Add** to create a new Managed Server and name it WLS_IBR2.

Tip:

The server names recommended here will be used throughout this document. If you choose different names be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Managed Server.

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Group
WLS_IBR1	WCCHOST1	16250	No	Disabled	IBR-MGD-SVR
WLS_IBR2	WCCHOST2	16250	No	Disabled	IBR-MGD-SVR

Tip:

More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Click **Next** to proceed.

Task 7 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle Inbound Refinery software.

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify IBR_Servers in the **Cluster Name** field.

3. From the **Dynamic Server Groups** drop-down list, select Unspecified.
4. Click **Next** to proceed to the next screen.

 Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

 Tip:

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 8 Assigning Server Templates

Click **Next** to proceed to the next screen.

Task 9 Configuring Dynamic Servers

Verify that all dynamic server options are disabled for clusters that are to remain as static clusters.

1. Confirm that the **Dynamic Cluster**, **Calculated Listen Port**, and **Calculated Machine Names** checkboxes on this screen are unchecked.
2. Confirm the **Server Template** selection is **Unspecified**.
3. Click **Next** to proceed.

Task 10 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign WLS_IBR1 and WLS_IBR2 to the new cluster IBR_Servers:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, IBR_Servers.
2. In the Servers pane, assign WLS_IBR1 to IBR_Servers by doing one of the following:
 - Click once on WLS_IBR1 Managed Server to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
 - Double-click WLS_IBR1 to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign WLS_IBR2 to IBR_Servers.

 Tip:

More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

4. Click **Next** to proceed.

Task 11 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 9991, as it was defined during the initial Infrastructure domain creation.

 Note:

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Click **Next** to proceed.

Task 12 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain.

Click **Next** to proceed.

Task 13 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Oracle Inbound Refinery Managed Servers you just created to the corresponding machines in the domain. Assign WLS_IBR1 to WCCHOST1, and assign WLS_IBR2 to WCCHOST2.

 Tip:

More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Click **Next** to proceed.

Task 14 Reviewing Virtual Targets

Click **Next** to proceed to the next screen.

Task 15 Reviewing Partitions

Click **Next** to proceed to the next screen.

Task 16 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane. Click **Update** to execute the domain extension.

 Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 17 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server. Click **Finish** to dismiss the Configuration Wizard.

Task 18 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

Completing Postconfiguration and Verification Tasks for Inbound Refinery

After extending the domain with the Inbound Refinery software, consider the following post-configuration and verification tasks.

- [Propagate the Domain Configuration Updates for Inbound Refinery](#)
- [Starting the Node Manager in the Managed Server Domain Directory](#)
- [Starting the Inbound Refinery Managed Servers](#)

Propagate the Domain Configuration Updates for Inbound Refinery

Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directory. To propagate the domain configuration to the Inbound Refinery Managed Servers:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.
2. Run the following pack command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin
```

```
./pack.sh -managed=true -domain=ASERVER_HOME -  
template=edgdomaintemplateExtIBR.jar -template_name=edgdomain_templateIBR
```

3. Run the following unpack command on WCCHOST1 to propagate the template created in the preceding step to the WLS_IBR1 domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateExtIBR.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

```
scp edgdomaintemplateIBR.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
```

5. Run the unpack command on WCCHOST2 to unpack the propagated template to the WLS_IBR1 domain directory.

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateExtIBR.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

Starting the Node Manager in the Managed Server Domain Directory

Follow these steps to start the Node Manager from the Managed Server home:

1. On WCCHOST1, navigate to the following directory:

```
MSERVER_HOME/bin
```

2. Use the following command to start the Node Manager:

```
nohup ./startNodeManager.sh > ./nodemanager.out 2>&1 &
```

3. Change directory to the following directory on WCCHOST2 and repeat the preceding step.

```
MSERVER_HOME/bin
```

For information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

Starting the Inbound Refinery Managed Servers

To start the WLS_IBR1 Managed Server on WCCHOST1:

1. Log in to the Oracle WebLogic Server Administration Console as the weblogic_wcc user at:

`http://admin.example.com/console`
2. Start the WLS_IBR1 Managed Server through the Administration Console, as follows:
 - a. Expand the **Environment** node in the **Domain Structure** tree on the left.
 - b. Click **Servers**.
 - c. On the Summary of Servers page, click the **Control** tab.
 - d. Select **WLS_IBR1** from the **Servers** column of the table.
 - e. Click **Start**.
3. Verify that the server status is reported as Running in the Administration Console.

- If the server is shown as Starting or Resuming, wait for the server status to change to Started.
 - If another status is reported (such as Admin or Failed), check the server output log files for errors.
4. Repeat the preceding steps to start the WLS_IBR2 Managed Server on WCCHOST2.

Configuring the Inbound Refinery Managed Servers

To initialize the configuration of an Inbound Refinery Managed Server, you need to access it only once through HTTP. You can do this directly at the Managed Server's listen address. An Inbound Refinery instance should not be placed behind an HTTP server.

All subsequent access to the Inbound Refinery instance is through the socket listener. This listener is protected through the incoming socket connection address security filter configured in the next section.

Oracle recommends configuring each Content Server instance with all Inbound Refinery instances. The process for configuring Content Server is to add each Inbound Refinery instance as a provider. You also need to perform some post-installation steps with Inbound Refinery.

The following sections describe the procedures for post-installation configuration of each Inbound Refinery instance.

- [Configuring Inbound Refinery Settings](#)
After starting the Inbound Refinery Managed Servers, configure the settings for each server on its post-installation configuration screen.
- [Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion](#)
Before Oracle WebCenter Content Server can send jobs to Inbound Refinery for conversion, you need to perform the setup tasks described in the following sections for each Inbound Refinery Managed Server.

Configuring Inbound Refinery Settings

After starting the Inbound Refinery Managed Servers, configure the settings for each server on its post-installation configuration screen.

To configure the settings for each Inbound Refinery instance, complete the following steps:

1. Create unique IBR directories on the *ORACLE_RUNTIME* shared filesystem for each IBR server as required for the Oracle WebCenter Content Inbound Refinery configuration. The Oracle WebCenter Content Inbound Refinery configuration requires a unique and separate directory for each IBR instance's runtime files. The EDG architecture recommends using the *ORACLE_RUNTIME* shared filesystem consistently for all runtime file-based data storage. The recommended base path for the Oracle WebCenter Content Inbound Refinery runtime file storage is *ORACLE_RUNTIME/domain_name/IBR_Servers/*

 Note:

The IBR servers do not share file-based data between instances. Unlike the Content Server instances, there is no product-specific requirement to implement a shared filesystem for the IBR data. Use of the shared filesystem for IBR data is for architectural consistency and DR replication efficiency.

Run the following commands to create the required unique subdirectories for each IBR managed server:

```
mkdir -p ORACLE_RUNTIME/domain_name/IBR_Servers/ibr1/vault
mkdir -p ORACLE_RUNTIME/domain_name/IBR_Servers/ibr1/weblayout
mkdir -p ORACLE_RUNTIME/domain_name/IBR_Servers/ibr1/data/users/
profiles
mkdir -p ORACLE_RUNTIME/domain_name/IBR_Servers/ibr2/vault
mkdir -p ORACLE_RUNTIME/domain_name/IBR_Servers/ibr2/weblayout
mkdir -p ORACLE_RUNTIME/domain_name/IBR_Servers/ibr2/data/users/
profiles
```

2. Access the Inbound Refinery post-installation configuration screen at the following URL for each WCCHOST:

`http://WCCHOSTN:16250/ibr/`

3. On the Configuration screen, you will see **Inbound Refinery Instance Identifier:** *name*. Set the remaining configuration settings for this instance as follows.

 Note:

Each Inbound Refinery instance and associated runtime file repository directory are unique and independent of the other instances. Use the specific directory paths just created in this section for the corresponding configuration settings of each instance. Inbound Refinery Instance Folder: Set this to `ORACLE_RUNTIME/domain_name/IBR_Servers/ibrN`

- **Inbound Refinery Instance Folder:** Set this to `ORACLE_RUNTIME/domain_name/IBR_Servers/ibrN`
For example: `/u01/oracle/runtime/wccedg_domain/IBR_Servers/ibr1`
- **Native File Repository Location:** Set this to `ORACLE_RUNTIME/domain_name/IBR_Servers/ibrN/vault`
For example: `/u01/oracle/runtime/wccedg_domain/IBR_Servers/ibr1/vault`
- **WebLayout Folder:** Set this to `ORACLE_RUNTIME/domain_name/IBR_Servers/ibrN/weblayout`
For example: `/u01/oracle/runtime/wccedg_domain/IBR_Servers/ibr1/weblayout`
- **User Profile Folders:** Set this to `ORACLE_RUNTIME/domain_name/IBR_Servers/ibrN/data/users/profiles`

For example: /u01/oracle/runtime/wccedg_domain/IBR_Servers/ibr1/data/users/profiles

- **Incoming Socket Connection Address Security Filter:** A pipe-delimited list of localhost and the server IP addresses:

```
127.0.0.1|0:0:0:0:0:0:0:1|WCCHOST1-IP|WCCHOST2-IP|WEBHOST1-IP|WEBHOST2-IP
```

This setting enables access from Content Server. The values for *WCCHOST1-IP* and *WCCHOST2-IP* should be the IP addresses of the machines with the Content Server instance or instances that will send jobs to Inbound Refinery, not necessarily the IP address of Inbound Refinery. (In the reference topology used in this enterprise deployment guide, however, these IP addresses are the same.)

The **Incoming Socket Connection Address Security Filter:** field accepts wildcards in the value; for example, 192.0.2.*.

You can change this value later by setting `SocketHostAddressSecurityFilter` in the /u02/oracle/runtime/wccedg_domain/IBR_Servers/ibrN/config/config.cfg file and then restarting the Inbound Refinery Managed Server.

Where *N* is 1 for `http://WCCHOST1:16250/ibr/` and *N* is 2 for `http://WCCHOST2:16250/ibr/`

- **Server Socket Port:** Enter an unused port number, such as 5555. This value is the number of the port for calling top-level services.

Take note of the port number because you need it later for configuring Oracle WebCenter Content.

Changing this field value changes the `IntradocServerPort` entry in /u01/oracle/runtime/wccedg_domain/IBR_Servers/ibrN/config/config.cfg

Where *N* is 1 for `http://WCCHOST1:16250/ibr/` and *N* is 2 for `http://WCCHOST2:16250/ibr/`

- **Server Instance Name:** Specify a name for the Inbound Refinery server instance.

You can accept the default value or change it to a name that is more useful to you. Take note of the server name because you will need it later for configuring Oracle WebCenter Content.

You can leave all other fields on the configuration page as they are.

Click **Submit**, and you should get the following message:

```
Post-install configuration complete. Please restart this node.
```

4. Restart the Inbound Refinery Managed Server, using the WebLogic Server Administration Console.
5. Repeat the preceding steps for each Inbound Refinery instance, using different names for the content folders.

Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion

Before Oracle WebCenter Content Server can send jobs to Inbound Refinery for conversion, you need to perform the setup tasks described in the following sections for each Inbound Refinery Managed Server.

- [Creating an Outgoing Provider](#)
Before Content Server can send files to Inbound Refinery for conversion, you must set up an outgoing provider from Content Server to each Inbound Refinery with the **Handles Inbound Refinery Conversion Jobs** option checked.
- [Enabling Components for Inbound Refinery on Content Server](#)
Some conversion types require *helper* components to be enabled on Content Server. The InboundRefinerySupport component must always be enabled on any Content Server instance that uses Inbound Refinery for document conversion. It is enabled by default on a new Content Server installation.
- [Selecting File Formats To Be Converted](#)
To tell Content Server which files to send to Inbound Refinery to be converted, you need to select file formats.

Creating an Outgoing Provider

Before Content Server can send files to Inbound Refinery for conversion, you must set up an outgoing provider from Content Server to each Inbound Refinery with the **Handles Inbound Refinery Conversion Jobs** option checked.

To create an outgoing provider for each Inbound Refinery instance:

1. Log in to Content Server at the following URL:
`http://WCCHOST1:16200/cs/`
2. Open the **Administration** tray or menu, then choose **Providers**.
3. In the **Create a New Provider** table of the Providers page, click **Add** in the **outgoing** row.
4. Enter the following values for the fields:
 - **Provider Name:** Any short name with no spaces. It is a good idea to use the same value as the **Instance Name** value
 - **Provider Description:** Any text string.
 - **Server Host Name:** The name of the host machine where the Inbound Refinery instance is running: WCCHOST1.
 - **HTTP Server Address:** The address of the Inbound Refinery instance: WCCHOST1:16250.
 - **Server Port:** The value of the **Server Socket Port** field for the Inbound Refinery instance as specified in [Configuring Inbound Refinery Settings](#); for example, 5555. This is the IntradocServerPort value in the InboundRefineryconfig.cfg file.

- **Instance Name:** The server instance name for Inbound Refinery as specified in [Configuring Inbound Refinery Settings](#). This is the IDC_Name value in the Inbound Refinery config.cfg file.
 - **Relative Web Root:** The web root of the Inbound Refinery instance: /ibr/
5. Under Conversion Options, check **Handles Inbound Refinery Conversion Jobs**. Do not check **Inbound Refinery Read Only Mode**.
 6. Click **Add**.
 7. Restart the Inbound Refinery Managed Server and Oracle WebCenter Content Server (WebCenter Content Managed Server), using the WebLogic Server Administration Console.
 8. Go back to the Providers page, and check that the **Connection State** value is good for the provider.

If the value is not good, double-check that you entered all the preceding entries correctly, and check that the Content Server and Inbound Refinery instances can ping each other.
 9. Complete steps 1 through 8 for the second IBR server.

For more information about setting up providers, see "Configuring Content Server and Refinery Communication" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

Enabling Components for Inbound Refinery on Content Server

Some conversion types require *helper* components to be enabled on Content Server. The InboundRefinerySupport component must always be enabled on any Content Server instance that uses Inbound Refinery for document conversion. It is enabled by default on a new Content Server installation.

To enable Inbound Refinery components on Content Server:

1. Log in to Content Server at the following URL:
`https://wcc.example.com/cs`
2. From the **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.
3. On the Component Manager page, select **Inbound Refinery**, then select components that you want to enable under Inbound Refinery, such as **XMLConverterSupport**, and then click **Update**.
4. Restart both Content Servers by restarting the WebCenter Content Managed Servers, using the WebLogic Server Administration Console.

Selecting File Formats To Be Converted

To tell Content Server which files to send to Inbound Refinery to be converted, you need to select file formats.

To select file formats to be converted:

1. Log in to Content Server at the following URL:
`https://wcc.example.com/cs/`

2. Open the **Administration** tray or menu, then choose **Refinery Administration**, and then **File Formats Wizard** to open the File Formats Wizard page.

This page specifies what file formats will be sent to Inbound Refinery for conversion when they are checked into Content Server.

3. Select the formats you want converted, such as **doc**, **dot**, **docx**, and **dotx** for Microsoft Word documents.
4. Click **Update**.

You can also select file formats with the Configuration Manager, with more fine-grained control, including file formats that the wizard does not list. See *Managing File Types* in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

Validating the Configuration of the Inbound Refinery Managed Servers

To ensure that the Inbound Refinery Managed Servers you have created are properly configured, validate the configuration by logging in to Content Server and verifying that a file with an extension recognized as valid for conversion is correctly converted.

For example, if you selected docx as a format to be converted, you can convert a Microsoft Word document with a .docx extension to PDF format.

For information about the check-in and check-out procedures, see "Uploading Documents" and "Checking Out and Downloading Files" in *Oracle Fusion Middleware Using Oracle WebCenter Content*.

For information about the conversion process, see "Configuring Content Servers to Send Jobs to Refineries" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

Extending the Domain to Include Capture

You need to perform certain tasks in order to extend the enterprise deployment domain with Oracle WebCenter Enterprise Capture software.

- [Overview of Extending the Domain to Include Capture](#)
Oracle WebCenter Enterprise Capture provides organizations with a single system to capture both paper and electronic documents.
- [Extending the Domain for Capture](#)
The instructions for extending the existing enterprise deployment domain with the Capture software are detailed in this section.
- [Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2](#)
You need to perform the following steps in order to propagate the domain configuration to the Capture Managed Servers.
- [Configuring Oracle HTTP Server for the Capture Cluster](#)
To enable Oracle HTTP Server to route to CPT_Cluster, which contains the WLS_CPT1 and WLS_CPT2 Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster.

Overview of Extending the Domain to Include Capture

Oracle WebCenter Enterprise Capture provides organizations with a single system to capture both paper and electronic documents.

Capture supports both centralized and distributed image capture from a user-friendly web interface capable of using high-volume, production-level scanners. Support for the industry-standard TWAIN scanning interface enables Capture to use a wide variety of industry-leading document imaging scanners to digitize paper content. Existing electronic document files can be easily captured by users or automatically captured through an importing process that can monitor an email server or network folder. Once captured, documents are organized and indexed by applying metadata through manual or automated processes that use bar code recognition technology. After documents are completed, they are committed into a content management system. Capture is fully integrated with Oracle WebCenter Content to provide organizations with one system to capture, store, manage and retrieve their mission critical business content.

Extending the Domain for Capture

The instructions for extending the existing enterprise deployment domain with the Capture software are detailed in this section.

Extending the domain involves the following tasks.

- [Starting the Configuration Wizard](#)
Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.

- [Navigating the Configuration Wizard Screens to Extend the Domain](#)

Starting the Configuration Wizard

Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.



Note:

If you added any customizations directly to the start scripts in the domain, those are overwritten by the configuration wizard. To customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it, for example, add custom libraries to the WebLogic Server classpath, specify Additional JAVA command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the **pack** and **unpack** commands.

To start the Configuration Wizard:

1. From the WebLogic Server Console, stop any managed servers that are modified by this domain extension. Managed Servers that are not effected can remain on-line.
2. For any managed servers to be modified, verify that the managed server shutdown has completed.
3. Stop the Administration Server once all managed servers are in a steady state.
4. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

Navigating the Configuration Wizard Screens to Extend the Domain

Follow the instructions in the following sections to create and configure the domain for the topology with static and dynamic clusters.

- [Extending the Domain with Static Clusters](#)
- [Extending the Domain with Dynamic Clusters](#)

Extending the Domain with Static Clusters

Follow the instructions in this section to create and configure the domain for the topology with static clusters.

 Note:

You can use the same procedure described in this section to extend an existing domain with static clusters. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying the Database Configuration Type](#)
- [Task 4, Specifying JDBC Component Schema Information](#)
- [Task 5, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 6, Testing the JDBC Connections](#)
- [Task 7, Selecting Advanced Configuration](#)
- [Task 8, Configuring Managed Servers](#)
- [Task 9, Configuring a Cluster](#)
- [Task 10, Assigning Server Templates](#)
- [Task 11, Configuring Dynamic Servers](#)
- [Task 12, Assigning Managed Servers to the Cluster](#)
- [Task 13, Configuring Coherence Clusters](#)
- [Task 14, Verifying the Existing Machines](#)
- [Task 15, Assigning Servers to Machines](#)
- [Task 16, Virtual Targets](#)
- [Task 17, Partitions](#)
- [Task 18, Configuring the JMS File Store](#)
- [Task 19, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 20, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 21, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#) and while extending the domain with WebCenter Content, SOA and Inbound Refinery. For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).



Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Enterprise Capture - 12.2.1.2.0 [wccapture]**

In addition, the following additional templates should already be selected, because they were used to create the initial domain. These templates are not required to run Capture. They are already selected as part of the enterprise deployment configuration.

- **Oracle Universal Content Management - Content Server - 12.2.1.2.0 [wccontent]**
- **Oracle SOA Suite - 12.2.1.2.0 [soa]**
- **Oracle Universal Content Management - Inbound Refinery - 12.2.1.2.0 [wccontent]**
- **Oracle Enterprise Manager - 12.2.1.2.0 [em]**
- **Oracle WSM Policy Manager - 12.2.1.2.0 [oracle_common]**
- **Oracle JRF - 12.2.1.2.0 [oracle_common]**
- **WebLogic Coherence Cluster Extension - 12.2.1.2.0 [wlserver]**



Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.

 Tip:

For more information about the **RCU Data** option, see Understanding the Service Table Schema in *Creating Schemas with the Repository Creation Utility*.
For more information about the other options on this screen, see Datasource Defaults in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 4 Specifying JDBC Component Schema Information

Click **Convert to GridLink** and click **Next**.

Task 5 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, perform the following tasks.

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **SCAN Port** field, enter the SCAN listening port for the database (for example, 1521).
4. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
5. In the **ONS Port** field, enter the ONS Remote port (for example, 6200).

Click **Next**.

Task 6 Testing the JDBC Connections

Click **Next** to continue.

Task 7 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File Store**

Task 8 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Rename the default Managed Server to WLS_CPT1.
2. Click **Add** to create a new Managed Server and name it WLS_CPT2.

 Tip:

The server names recommended here will be used throughout this document; if you choose different names, be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Capture Managed Server.

**Tip:**

More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WLS_CPT1	WCCHOST1	16400	No	Disabled	JRF-MAN-SVR CAPTURE-MGD-SVR
WLS_CPT2	WCCHOST2	16400	No	Disabled	JRF-MAN-SVR CAPTURE-MGD-SVR

Task 9 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Capture software.

You will also set the **Frontend Host** property for the cluster, which ensures that, when necessary, WebLogic Server will redirect Web services callbacks and other redirects to `wcc.example.com` on the load balancer rather than the address in the HOST header of each request.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `CPT_Cluster` in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select `Unspecified`.

**Note:**

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

**Tip:**

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 10 Assigning Server Templates

Click **Next** to proceed to the next screen.

Task 11 Configuring Dynamic Servers

Verify that all dynamic server options are disabled for clusters that are to remain as static clusters.

1. Confirm that the **Dynamic Cluster**, **Calculated Listen Port**, and **Calculated Machine Names** checkboxes on this screen are unchecked.
2. Confirm the **Server Template** selection is **Unspecified**.
3. Click **Next**.

Task 12 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign WLS_CPT1 and WLS_CPT2 to the new cluster, CPT_Cluster:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, CPT_Cluster.
2. In the Servers pane, assign WLS_CPT1 to CPT_Cluster by doing one of the following:
 - Click the WLS_CPT1 Managed Server once to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
 - Double-click WLS_CPT1 to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign WLS_CPT2 to CPT_Cluster.

**Tip:**

More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 13 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 0, as it was defined during the initial Infrastructure domain creation. Oracle Enterprise Capture does not use Coherence Clusters. This step is a part of the domain extension process.

**Note:**

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 14 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain. Click **Next** to proceed.

Task 15 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Capture Managed Servers you just created to the corresponding machines in the domain.

Assign WLS_CPT1 to WCCHOST1, and assign WLS_CPT2 to WCCHOST2.



Tip:

More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 16 Virtual Targets

Click **Next** to proceed to the next screen.

Task 17 Partitions

Click **Next** to proceed to the next screen.

Task 18 Configuring the JMS File Store

In the JMS File Stores screen, assign the following directory for each of the WCC Persistence stores including UMS and BPM file stores:

`ORACLE_RUNTIME/CPT_Cluster/jms`

In this example, replace `ASERVER_HOME` with the value of the variable for you environment. Replace `CPT_Cluster` with the name you assigned to the Capture cluster.

Task 19 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.



Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 20 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the Configuration Wizard.

Task 21 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

After you have completed extending the domain with static clusters, go to [Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2](#).

Extending the Domain with Dynamic Clusters

Follow the instructions in this section to create and configure the domain for the topology with dynamic clusters.

Note:

You can use the same procedure described in this section to extend an existing domain with Dynamic Clusters. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying the Database Configuration Type](#)
- [Task 4, Specifying JDBC Component Schema Information](#)
- [Task 5, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 6, Testing the JDBC Connections](#)
- [Task 7, Selecting Advanced Configuration](#)
- [Task 8, Configuring Managed Servers](#)
- [Task 9, Configuring a Cluster](#)
- [Task 10, Assigning Server Templates](#)
- [Task 11, Configuring Dynamic Servers](#)
- [Task 12, Assigning Managed Servers to the Cluster](#)
- [Task 13, Configuring Coherence Clusters](#)
- [Task 14, Verifying the Existing Machines](#)
- [Task 15, Assigning Servers to Machines](#)
- [Task 16, Virtual Targets](#)
- [Task 17, Partitions](#)
- [Task 18, Configuring the File Stores](#)
- [Task 19, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 20, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 21, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#) and while extending the domain with WebCenter Content, SOA and Inbound Refinery.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).



Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Enterprise Capture - 12.2.1.3.0 [wccapture]**
In addition, the following additional templates should already be selected, because they were used to create the initial domain. These templates are not required to run Capture. They are already selected as part of the enterprise deployment configuration.
 - **Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]**
 - **Oracle SOA Suite - 12.2.1.3.0 [soa]**
 - **Oracle Universal Content Management - Inbound Refinery - 12.2.1.3.0 [wccontent]**
 - **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
 - **Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]**
 - **Oracle JRF - 12.2.1.3.0 [oracle_common]**
 - **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**



Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.

 Tip:

For more information about the **RCU Data** option, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.

For more information about the other options on this screen, see "Datasource Defaults" in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 4 Specifying JDBC Component Schema Information

Click **Convert to GridLink** and click **Next**.

Task 5 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, perform the following tasks.

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **SCAN Port** field, enter the SCAN listening port for the database (for example, 1521).
4. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
5. In the **ONS Port** field, enter the ONS Remote port (for example, 6200).

Click **Next**.

Task 6 Testing the JDBC Connections

Click **Next** to continue.

Task 7 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File Store**

Task 8 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Delete the default Managed Server.
2. Click **Next** to proceed to the next screen.

Task 9 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Capture software.

You will also set the **Frontend Host** property for the cluster, which ensures that, when necessary, WebLogic Server will redirect Web services callbacks and other redirects to `wcc.example.com` on the load balancer rather than the address in the HOST header of each request.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `CPT_Cluster` in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select `ODDC-DYN-CLUSTER`.

**Note:**

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

**Tip:**

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 10 Assigning Server Templates

Use the Server Templates screen to add a template:

1. Specify `CPT-server-template` in the **Name** field.
2. Specify `16400` in the **Listen Port** field.
3. Leave the **Enable SSL** option unchecked.
4. From the **Cluster** drop-down list, select `CPT_Cluster`.
5. Click **Next** to proceed to the next screen.

Task 11 Configuring Dynamic Servers

Use the Dynamic Clusters screen to configure the required clusters:

1. Specify `CPT_Cluster` in the **Cluster Name** field.
2. Specify `WLS_CPT` in the **Server Name Prefix** field.
3. From the **Server Template** drop-down list, select `CPT-server-template`.
4. Specify `2` in the **Maximum Dynamic Server Count** field.
5. Specify `WCCHOST*` in the **Machine Name Match Expression** field.
6. Select the **Calculated Machine Names** and **Dynamic Cluster** fields.
7. Select the **Calculated Listen Ports** field.
8. Click **Next** to proceed to the next screen.

Task 12 Assigning Managed Servers to the Cluster

Click **Next** to proceed to the next screen.

Task 13 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 0, as it was defined during the initial Infrastructure domain creation. Oracle Enterprise Capture does not use Coherence Clusters. This step is a part of the domain extension process.

Note:

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 14 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain.
Click **Next** to proceed to the next screen.

Task 15 Assigning Servers to Machines

Click **Next** to proceed to the next screen.

Task 16 Virtual Targets

Click **Next** to proceed to the next screen.

Task 17 Partitions

Click **Next** to proceed to the next screen.

Task 18 Configuring the File Stores

In the JMS File Stores screen, assign the following directory for each of the WCC Persistence stores including UMS and BPM file stores:

`ORACLE_RUNTIME/CPT_Cluster/jms`

In this example, replace `ASERVER_HOME` with the value of the variable for your environment. Replace `CPT_Cluster` with the name you assigned to the Capture cluster.

Task 19 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.

**Tip:**

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 20 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server. Click **Finish** to dismiss the Configuration Wizard.

Task 21 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2

You need to perform the following steps in order to propagate the domain configuration to the Capture Managed Servers.

To propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directory:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.
2. Run the following pack command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ASERVER_HOME -
template=edgdomaintemplateExtCPT.jar -template_name=edgdomain_templateCPT
```

3. Run the following unpack command on WCCHOST1 to propagate the template created in the preceding step to the WLS_CPT1 domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateExtCPT.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

```
scp edgdomaintemplateCPT.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
```

5. Run the unpack command on WCCHOST2 to unpack the propagated template to the WLS_CPT2 domain directory.


```
cd ORACLE_COMMON_HOME/common/bin
```

```
./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateExtCPT.jar -  
app_dir=APPLICATION_HOME -overwrite_domain=true
```

6. Restart the Administration Server to make these changes take effect, stopping it with the `nmKill` command, or with the Administration Console, and then starting it with the `nmStart` command. Before the restart, stop all Managed Servers in the domain through the Administration Console, and then start them after the restart. Log in to the Administration Console using the credentials for the `weblogic` user.

Configuring Oracle HTTP Server for the Capture Cluster

To enable Oracle HTTP Server to route to CPT_Cluster, which contains the WLS_CPT1 and WLS_CPT2 Managed Servers, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster.

This section includes the following topics.

- [Configuring Oracle HTTP Server for the WLS_CPT Managed Servers](#)
- [Setting the Front-End HTTP Host and Port for the Capture Cluster](#)
- [Validating Access Through the Load Balancer](#)

Configuring Oracle HTTP Server for the WLS_CPT Managed Servers

To configure Oracle HTTP Server for the WLS_CPT Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the `ORACLE_INSTANCE/config/OHS/ohs1/moduleconf/wcc_vh.conf` and `ORACLE_INSTANCE/config/OHS/ohs2/moduleconf/wcc_vh.conf` files:

```
#DC-Console
<Location /dc-console>
    WebLogicCluster WCCHOST1:16400,WCCHOST2:16400
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

#DC-Client
<Location /dc-client>
    WebLogicCluster WCCHOST1:16400,WCCHOST2VHN316400
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

2. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2:

```
./stopComponent.sh ohsn
./startComponent.sh ohsn
```

For WEBHOST1, use ohs1 (where n=1) and for WEBHOST2, use ohs2 (where n=2).

Setting the Front-End HTTP Host and Port for the Capture Cluster

To set the front-end HTTP host and port for the Capture cluster:

1. Log in to the WebLogic Server Administration Console.
2. Go to the Change Center section and click **Lock & Edit**.
3. Expand the **Environment** node in the **Domain Structure** tree on the left.
4. Click **Clusters**.
5. On the Summary of Clusters page, select **CPT_Cluster**.
6. Open the **HTTP** tab.
7. Set the following values:
 - **Frontend Host:** `wcc.example.com`
 - **Frontend HTTPS Port:** 443
 - **Frontend HTTP Port:** 80
8. Click **Save**.
9. Click **Activate Changes** in the Change Center section of the Administration Console.
10. Restart the servers to make the front-end host directive in the cluster take effect.

Validating Access Through the Load Balancer

Verify URLs to ensure that appropriate routing and failover is working from the HTTP Server to CPT_Cluster. To verify the URLs:

1. While WLS_CPT2 is running, stop WLS_CPT1 from the WebLogic Server Administration Console.
2. Access `https://wcc.example.com/dc-console` to verify that it is functioning properly. (You will not be able to retrieve reports or data because the Capture server is down.)
3. Start WLS_CPT1 from the WebLogic Server Administration Console.
4. Stop WLS_CPT2 from the WebLogic Server Administration Console.
5. Access `https://wcc.example.com/dc-console` to verify that it is functioning properly.
6. Start WLS_CPT2 from the WebLogic Server Administration Console.

Extending the Domain to Include Imaging

You need to perform certain tasks in order to extend the enterprise deployment domain with Oracle WebCenter Enterprise Imaging software.

- [Overview of Extending the Domain to Include Imaging](#)
Oracle WebCenter Enterprise Imaging provides organizations with a single system to capture both paper and electronic documents.
- [Extending the Domain for Imaging](#)
The instructions for extending the existing enterprise deployment domain with the Imaging software are detailed in this section.
- [Navigating the Configuration Wizard Screens to Extend the Domain](#)
Follow the instructions in the following sections to create and configure the domain for the topology with static and dynamic clusters.
- [Propagating the Domain Configuration to WLS_IPM1 and WLS_IPM2](#)
You need to perform the following steps in order to propagate the domain configuration to the Imaging Managed Servers.
- [Configuring Oracle HTTP Server for the Imaging Cluster](#)
To enable Oracle HTTP Server to route to IPM_Cluster, which contains the WLS_IPM1 and WLS_IPM2 Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster.

Overview of Extending the Domain to Include Imaging

Oracle WebCenter Enterprise Imaging provides organizations with a single system to capture both paper and electronic documents.

Oracle WebCenter Content: Imaging provides organizations with a scalable solution upon which to develop process-oriented imaging applications and image-enablement solutions for enterprise applications. It enables image capture through Oracle WebCenter Capture, annotation and markup of images, routing and approval automation, and support for high-volume applications for billions of items. With Imaging, organizations can quickly integrate their content and processes directly with Oracle enterprise applications, such as Oracle E-Business Suite, PeopleSoft Enterprise, and JD Edwards EnterpriseOne. Users benefit by having a single source for all transaction-based content, eliminating the need for double entry.

Extending the Domain for Imaging

The instructions for extending the existing enterprise deployment domain with the Imaging software are detailed in this section.

Extending the domain involves the following tasks.

Navigating the Configuration Wizard Screens to Extend the Domain

Follow the instructions in the following sections to create and configure the domain for the topology with static and dynamic clusters.

- [Extending the Domain with Static Clusters](#)
- [Extending the Domain with Dynamic Clusters](#)

Extending the Domain with Static Clusters

Follow the instructions in this section to create and configure the domain for the topology with static clusters.



Note:

You can use the same procedure described in this section to extend an existing domain with static clusters. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying the Database Configuration Type](#)
- [Task 4, Specifying JDBC Component Schema Information](#)
- [Task 5, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 6, Testing the JDBC Connections](#)
- [Task 7, Selecting Advanced Configuration](#)
- [Task 8, Configuring Managed Servers](#)
- [Task 9, Configuring a Cluster](#)
- [Task 10, Assigning Server Templates](#)
- [Task 11, Configuring Dynamic Servers](#)
- [Task 12, Assigning Managed Servers to the Cluster](#)
- [Task 13, Configuring Coherence Clusters](#)
- [Task 14, Verifying the Existing Machines](#)
- [Task 15, Assigning Servers to Machines](#)
- [Task 16, Virtual Targets](#)
- [Task 17, Partitions](#)

- [Task 18, Configuring the JMS File Store](#)
- [Task 19, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 20, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 21, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#) and while extending the domain with WebCenter Content, SOA, and Inbound Refinery.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).

Tip:

For more information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Content: Imaging - 12.2.1.3.0 [wccontent]**
- In addition, the following additional templates should already be selected, because they were used to create the initial domain. These templates are not required to run Imaging. They are already selected as part of the enterprise deployment configuration.
 - **Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]**
 - **Oracle SOA Suite - 12.2.1.3.0 [soa]**
 - **Oracle Universal Content Management - Inbound Refinery - 12.2.1.3.0 [wccontent]**
 - **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
 - **Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]**
 - **Oracle JRF - 12.2.1.3.0 [oracle_common]**
 - **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**

Tip:

For more information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Providing the GridLink DS Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, perform the following tasks.

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **SCAN Port** field, enter the SCAN listening port for the database (for example, 1521).
4. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
5. In the **ONS Port** field, enter the ONS Remote port (for example, 6200).
6. Click **Next**.

Task 4 Testing the JDBC DS Connections

Click **Next** to continue.

Task 5 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the imaging domain. Verify and ensure that credentials in all the fields are the same that you have provided while configuring Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.



Tip:

For more information about the **RCU Data** option, see Understanding the Service Table Schema in *Creating Schemas with the Repository Creation Utility*.
For more information about the other options on this screen, see Datasource Defaults in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 6 Specifying JDBC Component Schema Information

Click **Convert to GridLink** and click **Next**.

Task 7 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, perform the following tasks.

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **SCAN Port** field, enter the SCAN listening port for the database (for example, 1521).
4. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.

5. In the **ONS Port** field, enter the ONS Remote port (for example, 6200).
6. Click **Next**.

Task 8 Testing the JDBC Connections

Click **Next** to continue.

Task 9 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File Store**

Task 10 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Rename the default Managed Server to WLS_IPM1.
2. Click **Add** to create a new Managed Server and name it WLS_IPM2.



Tip:

The server names recommended here will be used throughout this document. If you choose different names, be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Imaging Managed Server.



Tip:

For more information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WLS_IPM1	WCCHOST1	16000	No	Disabled	IPM-MGD-SVR
WLS_IPM2	WCCHOST2	16000	No	Disabled	IPM-MGD-SVR

Task 11 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Imaging software.

You will also set the **Frontend Host** property for the cluster, which ensures that, when necessary, WebLogic Server will redirect Web services callbacks and other redirects to `wcc.example.com` on the load balancer rather than the address in the HOST header of each request.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify IPM_Cluster in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select Unspecified.



Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to Considerations for Choosing Unicast or Multicast in *Administering Clusters for Oracle WebLogic Server*.



Tip:

For more information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 12 Assigning Server Templates

Click **Next** to proceed to the next screen.

Task 13 Configuring Dynamic Servers

Verify that all dynamic server options are disabled for clusters that are to remain as static clusters.

1. Confirm that the **Dynamic Cluster**, **Calculated Listen Port**, and **Calculated Machine Names** checkboxes on this screen are unchecked.
2. Confirm the **Server Template** selection is **Unspecified**.
3. Click **Next**.

Task 14 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign WLS_IPM1 and WLS_IPM2 to the new cluster, IPM_Cluster:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, IPM_Cluster.
2. In the Servers pane, assign WLS_IPM1 to IPM_Cluster by doing one of the following:
 - Click the WLS_IPM1 Managed Server once to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
 - Double-click WLS_IPM1 to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign WLS_IPM2 to IPM_Cluster.

 Tip:

For more information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 15 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 0, as it was defined during the initial Infrastructure domain creation. Oracle Enterprise Imaging does not use Coherence Clusters. This step is a part of the domain extension process.

 Note:

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 16 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain. Click **Next** to proceed.

Task 17 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Imaging Managed Servers you just created to the corresponding machines in the domain. Assign WLS_IPM1 to WCCHOST1, and assign WLS_IPM2 to WCCHOST2.

 Tip:

For more information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 18 Virtual Targets

Click **Next** to proceed to the next screen.

Task 19 Partitions

Click **Next** to proceed to the next screen.

Task 20 Configuring the JMS File Store

In the JMS File Stores screen, assign the following directory for each of the WCC Persistence stores including UMS and BPM file stores:

`ORACLE_RUNTIME/IPM_Cluster/jms`

In this example, replace `ASERVER_HOME` with the value of the variable for you environment. Replace `IPM_Cluster` with the name you assigned to the Imaging cluster.

Task 21 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.



Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 22 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the Configuration Wizard.

Task 23 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

After you have completed extending the domain with static clusters, go to [Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2](#).

Extending the Domain with Dynamic Clusters

Follow the instructions in this section to create and configure the domain for the topology with dynamic clusters.



Note:

You can use the same procedure described in this section to extend an existing domain with Dynamic Clusters. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying the Database Configuration Type](#)

- [Task 4, Specifying JDBC Component Schema Information](#)
- [Task 5, Providing the GridLink Oracle RAC Database Connection Details](#)
- [Task 6, Testing the JDBC Connections](#)
- [Task 7, Selecting Advanced Configuration](#)
- [Task 8, Configuring Managed Servers](#)
- [Task 9, Configuring a Cluster](#)
- [Task 10, Assigning Server Templates](#)
- [Task 11, Configuring Dynamic Servers](#)
- [Task 12, Assigning Managed Servers to the Cluster](#)
- [Task 13, Configuring Coherence Clusters](#)
- [Task 14, Verifying the Existing Machines](#)
- [Task 15, Assigning Servers to Machines](#)
- [Task 16, Virtual Targets](#)
- [Task 17, Partitions](#)
- [Task 18, Configuring the File Stores](#)
- [Task 19, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 20, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 21, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#) and while extending the domain with WebCenter Content, SOA and Inbound Refinery.

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).



Tip:

For more information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Content: Imaging - 12.2.1.3.0 [wccontent]**
- In addition, the following additional templates should already be selected, because they were used to create the initial domain. These templates are not required to run Imaging. They are already selected as part of the enterprise deployment configuration.

- Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]
- Oracle SOA Suite - 12.2.1.3.0 [soa]
- Oracle Universal Content Management - Inbound Refinery - 12.2.1.3.0 [wccontent]
- Oracle Enterprise Manager - 12.2.1.3.0 [em]
- Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]
- Oracle JRF - 12.2.1.3.0 [oracle_common]
- WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]



Tip:

For more information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Providing the GridLink DS Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, perform the following tasks.

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **SCAN Port** field, enter the SCAN listening port for the database (for example, 1521).
4. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
5. In the **ONS Port** field, enter the ONS Remote port (for example, 6200).
6. Click **Next**.

Task 4 Testing the JDBC DS Connections

Click **Next** to continue.

Task 5 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the imaging domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.

 Tip:

For more information about the **RCU Data** option, see Understanding the Service Table Schema in *Creating Schemas with the Repository Creation Utility*.
For more information about the other options on this screen, see Datasource Defaults in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 6 Specifying JDBC Component Schema Information

Click **Convert to GridLink** and click **Next**.

Task 7 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, perform the following tasks.

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **SCAN Port** field, enter the SCAN listening port for the database (for example, 1521).
4. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
5. In the **ONS Port** field, enter the ONS Remote port (for example, 6200).
6. Click **Next**.

Task 8 Testing the JDBC Connections

Click **Next** to continue.

Task 9 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File Store**

Task 10 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Delete the default Managed Server.
2. Click **Next** to proceed to the next screen.

Task 11 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Imaging software.

You will also set the **Frontend Host** property for the cluster, which ensures that, when necessary, WebLogic Server will redirect Web services callbacks and other redirects to `wcc.example.com` on the load balancer rather than the address in the **HOST** header of each request.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).
Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `IPM_Cluster` in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select `IPM-DYN-CLUSTER`.



Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to Considerations for Choosing Unicast or Multicast in *Administering Clusters for Oracle WebLogic Server*.



Tip:

For more information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 12 Assigning Server Templates

Use the Server Templates screen to add a template:

1. Specify `IPM-server-template` in the **Name** field.
2. Specify `7100` in the **Listen Port** field.
3. Leave the **Enable SSL** option unchecked.
4. From the **Cluster** drop-down list, select `IPM_Cluster`.
5. Click **Next** to proceed to the next screen.

Task 13 Configuring Dynamic Servers

Use the Dynamic Clusters screen to configure the required clusters:

1. Specify `IPM_Cluster` in the **Cluster Name** field.
2. Specify `WLS_IPM` in the **Server Name Prefix** field.
3. From the **Server Template** drop-down list, select `IPM-server-template`.
4. Specify `2` in the **Dynamic Cluster Size** field.
5. Specify `WCCHOST*` in the **Machine Name Match Expression** field.
6. Select the **Calculated Machine Names** and **Dynamic Cluster** fields.
7. Select the **Calculated Listen Ports** field.
8. Click **Next** to proceed to the next screen.

Task 14 Assigning Managed Servers to the Cluster

Click **Next** to proceed to the next screen.

Task 15 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 0, as it was defined during the initial Infrastructure domain creation. Oracle Enterprise Imaging does not use Coherence Clusters. This step is a part of the domain extension process.

Note:

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 16 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain. Click **Next** to proceed to the next screen.

Task 17 Assigning Servers to Machines

Click **Next** to proceed to the next screen.

Task 18 Virtual Targets

Click **Next** to proceed to the next screen.

Task 19 Partitions

Click **Next** to proceed to the next screen.

Task 20 Configuring the File Stores

In the JMS File Stores screen, assign the following directory for each of the WCC Persistence stores including UMS and BPM file stores:

`ORACLE_RUNTIME/IPM_Cluster/jms`

In this example, replace `ASERVER_HOME` with the value of the variable for you environment. Replace `IPM_Cluster` with the name you assigned to the Imaging cluster.

Task 21 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.

Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 22 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the Configuration Wizard.

Task 23 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

Propagating the Domain Configuration to WLS_IPM1 and WLS_IPM2

You need to perform the following steps in order to propagate the domain configuration to the Imaging Managed Servers.

To propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directory:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following pack command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ASERVER_HOME -
template=edgdomaintemplateExtIPM.jar -template_name=edgdomain_templateIPM
```

3. Run the following unpack command on WCCHOST1 to propagate the template created in the preceding step to the WLS_IPM1 domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateExtIPM.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

```
scp edgdomaintemplateIPM.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
```

5. Run the unpack command on WCCHOST2 to unpack the propagated template to the WLS_IPM2 domain directory.

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateExtIPM.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

6. Restart the Administration Server to make these changes take effect, stopping it with the nmKill command, or with the Administration Console, and then starting it with the nmStart command. Before the restart, stop all Managed Servers in the

domain through the Administration Console, and then start them after the restart. Log in to the Administration Console using the credentials for the weblogic user.

Configuring Oracle HTTP Server for the Imaging Cluster

To enable Oracle HTTP Server to route to IPM_Cluster, which contains the WLS_IPM1 and WLS_IPM2 Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster.

This section includes the following topics.

- [Configuring Oracle HTTP Server for the WLS_IPM Managed Servers](#)
- [Setting the Front-End HTTP Host and Port for the Imaging Cluster](#)
- [Validating Access Through the Load Balancer](#)

Configuring Oracle HTTP Server for the WLS_IPM Managed Servers

To configure Oracle HTTP Server for the WLS_IPM Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the ORACLE_INSTANCE/config/OHS/ohs1/moduleconf/wcc_vh.conf and ORACLE_INSTANCE/config/OHS/ohs2/moduleconf/wcc_vh.conf files:

```
#Imaging
<Location /imaging>
    WebLogicCluster WCCHOST1:16000,WCCHOST2:16000
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```



Note:

If AXF webservices are used, then you have to add the following lines to the wcc_vh.conf file:

```
#AXF Webservices
<Location /axf-ws>
    WebLogicCluster WCCHOST1:16000,WCCHOST2:16000
    WLSRequest ON
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

2. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2:

```
./stopComponent.sh ohsn  
./startComponent.sh ohsn
```

For WEBHOST1, use ohs1 (where n=1) and for WEBHOST2, use ohs2 (where n=2).

Setting the Front-End HTTP Host and Port for the Imaging Cluster

To set the front-end HTTP host and port for the Imaging cluster:

1. Log in to the WebLogic Server Administration Console.
2. Go to the Change Center section and click **Lock & Edit**.
3. Expand the **Environment** node in the **Domain Structure** tree on the left.
4. Click **Clusters**.
5. On the Summary of Clusters page, select **IPM_Cluster**.
6. Open the **HTTP** tab.
7. Set the following values:
 - **Frontend Host:** `wcc.example.com`
 - **Frontend HTTPS Port:** 443
 - **Frontend HTTP Port:** 80
8. Click **Save**.
9. Click **Activate Changes** in the Change Center section of the Administration Console.
10. Restart the servers to make the front-end host directive in the cluster take effect.

Validating Access Through the Load Balancer

Verify URLs to ensure that appropriate routing and failover is working from the HTTP Server to IPM_Cluster. To verify the URLs:

1. While WLS_IPM2 is running, stop WLS_IPM1 from the WebLogic Server Administration Console.
2. Access `https://wcc.example.com/imaging` to verify that it is functioning properly. (You will not be able to retrieve reports or data because the Imaging server is down.)
3. Start WLS_IPM1 from the WebLogic Server Administration Console.
4. Stop WLS_IPM2 from the WebLogic Server Administration Console.
5. Access `https://wcc.example.com/imaging` to verify that it is functioning properly.
6. Start WLS_IPM2 from the WebLogic Server Administration Console.

Extending the Domain to Include WebCenter Content User Interface

You need to perform certain tasks in order to extend the enterprise deployment domain to include Oracle WebCenter Content User Interface software.

This chapter provides information on modifying system-level setting through MBeans and configuring http server with the WebCenter Content user interface cluster.

- [Extending the Domain for WebCenter Content User Interface](#)
The instructions for extending the existing enterprise deployment domain with the Oracle WebCenter Content user interface software are detailed in this section.
- [Propagating the Domain Configuration to WLS_WCCUI1 and WLS_WCCUI2](#)
You need to perform the following steps in order to propagate the domain configuration to the WebCenter Content user interface Managed Servers.
- [Modifying System-Level Settings Through MBeans](#)
To ensure high availability, modify system-level configuration settings for WebCenter Content user interface through the System Configuration page in Fusion Middleware Control. The settings on this page configure the WebCenter Content user interface MBeans for the domain.
- [Configuring Oracle HTTP Server with the WebCenter Content User Interface Cluster](#)
Configure Oracle HTTP Server with the WebCenter Content User Interface Cluster, set the front-end HTTP Host and Port for the cluster, and validate access through the load balancer.
- [Completing the Workflow Configuration](#)
To complete the workflow configuration for the WebCenter Content user interface, you need to restart the Managed Servers and verify the configuration. The `UseDatabasewfInQueue` configuration variable enables the WebCenter Content user interface to filter workflows assigned to a user. The `EmailNotificationType` configuration variable specifies where the links in notification emails point for workflows and subscriptions in different Content Server user interfaces, and its default value is `NativeWebUI`.

Extending the Domain for WebCenter Content User Interface

The instructions for extending the existing enterprise deployment domain with the Oracle WebCenter Content user interface software are detailed in this section.

Extending the domain involves the following tasks.

- [Starting the Configuration Wizard](#)
Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.

- [Navigating the Configuration Wizard Screens to Extend the Domain](#)

Starting the Configuration Wizard

Start the Configuration Wizard as the first step to extend the existing enterprise deployment domain.



Note:

If you added any customizations directly to the start scripts in the domain, those are overwritten by the configuration wizard. To customize server startup parameters that apply to all servers in a domain, you can create a file called `setUserOverridesLate.sh` and configure it, for example, add custom libraries to the WebLogic Server classpath, specify Additional JAVA command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the **pack** and **unpack** commands.

To start the Configuration Wizard:

1. From the WebLogic Server Console, stop any managed servers that are modified by this domain extension. Managed Servers that are not effected can remain on-line.
2. For any managed servers to be modified, verify that the managed server shutdown has completed.
3. Stop the Administration Server once all managed servers are in a steady state.
4. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

Navigating the Configuration Wizard Screens to Extend the Domain

Follow the instructions in the following sections to create and configure the domain for the topology with static or dynamic clusters.

- [Extending the Domain with Static Clusters](#)
- [Extending the Domain with Dynamic Clusters](#)

Extending the Domain with Static Clusters

Follow the instructions in this section to create and configure the domain for the topology.

 Note:

You can use the same procedure described in this section to extend an existing domain. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying JDBC Data Sources Information](#)
- [Task 4, Providing the GridLink Oracle RAC Data Sources Details](#)
- [Task 5, Testing the JDBC Data Sources](#)
- [Task 6, Providing the GridLink Oracle RAC Component Schema Details](#)
- [Task 7, Testing the JDBC Component Schema](#)
- [Task 8, Specifying Credentials for wccadfConnectUser](#)
- [Task 9, Selecting Advanced Configuration](#)
- [Task 10, Configuring Managed Servers](#)
- [Task 11, Configuring a Cluster](#)
- [Task 12, Assigning Server Templates](#)
- [Task 13, Configuring Dynamic Servers](#)
- [Task 14, Assigning Managed Servers to the Cluster](#)
- [Task 15, Configuring Coherence Clusters](#)
- [Task 16, Verifying the Existing Machines](#)
- [Task 17, Assigning Servers to Machines](#)
- [Task 18, Configuring Virtual Targets](#)
- [Task 19, Configuring Partitions](#)
- [Task 20, Reviewing Configuration Summary](#)
- [Task 21, Reviewing Configuration Progress](#)
- [Task 22, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 23, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 24, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#).

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).



Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Content - Web UI - 12.2.1.3.0 [wccontent]**
In addition, the following additional templates should already be selected, because they were used to create the initial domain:
 - **Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]**
 - **Oracle SOA Suite - 12.2.1.3.0 [soa]**
 - **Oracle Universal Content Management - Inbound Refinery - 12.2.1.3.0 [wccontent]**
 - **Oracle WebCenter Enterprise Capture - 12.2.1.3.0 [wccapture]**
 - **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
 - **Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]**
 - **Oracle JRF - 12.2.1.3.0 [oracle_common]**
 - **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**



Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Specifying JDBC Data Sources Information

Click **Convert to GridLink**, update the required database details, and then click **Next**.

Task 4 Providing the GridLink Oracle RAC Data Sources Details

On the GridLink Oracle RAC Data Sources screen, perform the following tasks. In the SCAN, Host Name, and Port section:

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **Port** field, enter the SCAN listening port for the database (for example, 1521).

In the ONS Host and Port section:

1. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
2. In the **Port** field, enter the ONS Remote port (typically, 6200).

Click **Next**.

Task 5 Testing the JDBC Data Sources

Click **Next** to continue.

Task 6 Providing the GridLink Oracle RAC Component Schema Details

Click **Next** to continue.

Task 7 Testing the JDBC Component Schema

Click **Next** to continue.

Task 8 Specifying Credentials for wccadfConnectUser

On the Credentials screen, enter the WebLogic user name(not weblogic_wcc) and password.

Click **Next** to continue.

Task 9 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

Topology

Task 10 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Rename the default Managed Server to WLS_WCCUI1.
2. Click **Add** to create a new Managed Server and name it WLS_WCCUI2.



Tip:

The server names recommended here will be used throughout this document; if you choose different names, be sure to replace them as needed.

3. Use the following table to fill in the rest of the columns for each Oracle WebCenter Content user interface Managed Server.



Tip:

More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WLS_WCCUI1	WCCHOST1	16225	No	Disabled	UCM-ADF-MGD-SVR

Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
WLS_WCCUI2	WCCHOST2	16225	No	Disabled	UCM-ADF-MGD-SVR

Task 11 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle WebCenter Content software.

You will also set the **Frontend Host** property for the cluster, which ensures that, when necessary, WebLogic Server will redirect Web services callbacks and other redirects to `wcc.example.com` on the load balancer rather than the address in the HOST header of each request.

For more information about the `wcc.example.com` virtual server address, see [Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `WCCUI_Cluster` in the **Cluster Name** field.
3. From the **Dynamic Server Groups** drop-down list, select **Unspecified**.



Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.



Tip:

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 12 Assigning Server Templates

Click **Next** to proceed to the next screen.

Task 13 Configuring Dynamic Servers

Verify that all dynamic server options are disabled for clusters that are to remain as static clusters.

1. Confirm that the **Dynamic Cluster**, **Calculated Listen Port**, and **Calculated Machine Names** checkboxes on this screen are unchecked.
2. Confirm the **Server Template** selection is **Unspecified**.
3. Click **Next**.

Task 14 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign `WLS_WCCUI1` and `WLS_WCCUI2` to the new cluster, `WCCUI_Cluster`:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, WCCUI_Cluster.
2. In the Servers pane, assign WLS_WCCUI1 to WCCUI_Cluster by doing one of the following:
 - Click the WLS_WCCUI1 Managed Server once to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
 - Double-click WLS_WCCUI1 to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign WLS_WCCUI2 to WCCUI_Cluster.

 Tip:

More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 15 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 0, as it was defined during the initial Infrastructure domain creation.

 Note:

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 16 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain.
Click **Next** to proceed.

Task 17 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Oracle WebCenter Content user interface Managed Servers you just created to the corresponding machines in the domain.

Assign WLS_WCCUI1 to WCCHOST1, and assign WLS_WCCUI2 to WCCHOST2.

 Tip:

More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 18 Configuring Virtual Targets

Click **Next** to proceed to the next screen.

Task 19 Configuring Partitions

Click **Next** to proceed to the next screen.

Task 20 Reviewing Configuration Summary

Click **Update** to proceed to the next screen.

Task 21 Reviewing Configuration Progress

After all the processes are complete, click **Next** to proceed to the next screen.

Task 22 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.



Tip:

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 23 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

Task 24 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

After you have completed extending the domain with static clusters, go to [Propagating the Domain Configuration to WLS_WCCUI1 and WLS_WCCUI2](#).

Extending the Domain with Dynamic Clusters

Follow the instructions in this section to create and configure the domain for the topology with Dynamic Clusters.

 Note:

You can use the same procedure described in this section to extend an existing domain with Dynamic Clusters. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain creation and configuration includes the following tasks:

- [Task 1, Selecting the Domain Type and Domain Home Location](#)
- [Task 2, Selecting the Configuration Template](#)
- [Task 3, Specifying JDBC Data Sources Information](#)
- [Task 4, Providing the GridLink Oracle RAC Data Sources Details](#)
- [Task 5, Testing the JDBC Data Sources](#)
- [Task 6, Providing the GridLink Oracle RAC Component Schema Details](#)
- [Task 7, Testing the JDBC Component Schema](#)
- [Task 8, Specifying Credentials for wccadfConnectUser](#)
- [Task 9, Selecting Advanced Configuration](#)
- [Task 10, Configuring Managed Servers](#)
- [Task 11, Configuring a Cluster](#)
- [Task 12, Assigning Server Templates](#)
- [Task 13, Configuring Dynamic Servers](#)
- [Task 14, Assigning Managed Servers to the Cluster](#)
- [Task 15, Configuring Coherence Clusters](#)
- [Task 16, Verifying the Existing Machines](#)
- [Task 17, Assigning Servers to Machines](#)
- [Task 18, Configuring Virtual Targets](#)
- [Task 19, Configuring Partitions](#)
- [Task 20, Reviewing Configuration Summary](#)
- [Task 21, Reviewing Configuration Progress](#)
- [Task 22, Reviewing Your Configuration Specifications and Configuring the Domain](#)
- [Task 23, Writing Down Your Domain Home and Administration Server URL](#)
- [Task 24, Start the Administration Server](#)

Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the `ASERVER_HOME` variable, which represents the complete path to the Administration Server domain home you created in [Creating the Initial Infrastructure Domain for an Enterprise Deployment](#).

For more information about the directory location variables, see [File System and Directory Variables Used in This Guide](#).



Tip:

More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Content - Web UI - 12.2.1.3.0 [wccontent]**
In addition, the following additional templates should already be selected, because they were used to create the initial domain:
 - **Oracle Universal Content Management - Content Server - 12.2.1.3.0 [wccontent]**
 - **Oracle SOA Suite - 12.2.1.3.0 [soa]**
 - **Oracle Universal Content Management - Inbound Refinery - 12.2.1.3.0 [wccontent]**
 - **Oracle WebCenter Enterprise Capture - 12.2.1.3.0 [wccapture]**
 - **Oracle Enterprise Manager - 12.2.1.3.0 [em]**
 - **Oracle WSM Policy Manager - 12.2.1.3.0 [oracle_common]**
 - **Oracle JRF - 12.2.1.3.0 [oracle_common]**
 - **WebLogic Coherence Cluster Extension - 12.2.1.3.0 [wlserver]**



Tip:

More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 3 Specifying JDBC Data Sources Information

Click **Convert to GridLink**, update the required database details, and then click **Next**.

Task 4 Providing the GridLink Oracle RAC Data Sources Details

On the GridLink Oracle RAC Data Sources screen, perform the following tasks. In the SCAN, Host Name, and Port section:

1. Select the **SCAN** check box.
2. In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.
3. In the **Port** field, enter the SCAN listening port for the database (for example, 1521).

In the ONS Host and Port section:

1. In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.
2. In the **Port** field, enter the ONS Remote port (typically, 6200).

Click **Next**.

Task 5 Testing the JDBC Data Sources

Click **Next** to continue.

Task 6 Providing the GridLink Oracle RAC Component Schema Details

Click **Next** to continue.

Task 7 Testing the JDBC Component Schema

Click **Next** to continue.

Task 8 Specifying Credentials for wccadfConnectUser

On the Credentials screen, enter the WebLogic user name (not weblogic_wcc) and password.

Click **Next** to continue.

Task 9 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

Topology

Task 10 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Delete the default Managed Server.
2. Click **Next** to proceed to the next screen.

Task 11 Configuring a Cluster

In this task, you create a cluster of Managed Servers to which you can target the Oracle WebCenter Content software.

You will also set the **Frontend Host** property for the cluster, which ensures that, when necessary, WebLogic Server will redirect Web services callbacks and other redirects to `wcc.example.com` on the load balancer rather than the address in the HOST header of each request.

For more information about the `wcc.example.com` virtual server address, see

[Configuring Virtual Hosts on the Hardware Load Balancer](#).

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `WCCUI_Cluster` in the **Cluster Name** field.
3. From the Dynamic Server Groups drop-down list, select `WCCADF-DYN-CLUSTER`.

Note:

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.



Tip:

More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 12 Assigning Server Templates

Use the Server Templates screen to add a template:

1. Specify WCCADF-server-template in the **Name** field.
2. Specify 16225 in the **Listen Port** field.
3. Leave the **Enable SSL** option unchecked.
4. From the **Cluster** drop-down list, select Unspecified.
5. Click **Next** to proceed to the next screen.

Task 13 Configuring Dynamic Servers

Use the Dynamic Clusters screen to configure the required clusters:

1. Specify WCCUI_Cluster in the **Cluster Name** field.
2. Specify WLS_WCCUI in the **Server Name Prefix** field.
3. From the **Server Template** drop-down list, select WCCADF-server-template.
4. Specify 2 in the **Maximum Dynamic Server Count** field.
5. Specify WCCHOST* in the **Machine Name Match Expression** field.
6. Select the **Calculated Machine Names** and **Dynamic Cluster** fields.
7. Select the **Calculated Listen Ports** field.
8. Click **Next** to proceed to the next screen.

Task 14 Assigning Managed Servers to the Cluster

Click **Next** to proceed to the next screen.

Task 15 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 0, as it was defined during the initial Infrastructure domain creation.



Note:

For Coherence licensing information, refer to *Oracle Coherence* in [Oracle Fusion Middleware Licensing Information](#).

Task 16 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain.
Click **Next** to proceed to the next screen.

Task 17 Assigning Servers to Machines

Click **Next** to proceed to the next screen.

Task 18 Configuring Virtual Targets

Click **Next** to proceed to the next screen.

Task 19 Configuring Partitions

Click **Next** to proceed to the next screen.

Task 20 Reviewing Configuration Summary

Click **Update** to proceed to the next screen.

Task 21 Reviewing Configuration Progress

After all the processes are complete, click **Next** to proceed to the next screen.

Task 22 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.

**Tip:**

More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Task 23 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

Task 24 Start the Administration Server

Start the Administration Server to ensure the changes you have made to the domain have been applied.

Propagating the Domain Configuration to WLS_WCCUI1 and WLS_WCCUI2

You need to perform the following steps in order to propagate the domain configuration to the WebCenter Content user interface Managed Servers.

To propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directory:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following pack command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ASERVER_HOME -
template=edgdomaintemplateWCCUI.jar -template_name=edgdomain_templateWCCUI
```

3. Run the following unpack command on WCCHOST1 to propagate the template created in the preceding step to the WLS_WCCUI1 domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateWCCUI.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

```
scp edgdomaintemplateWCCUI.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
```

5. Run the unpack command on WCCHOST2 to unpack the propagated template to the WLS_WCCUI2 domain directory.

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateWCCUI.jar -
app_dir=APPLICATION_HOME -overwrite_domain=true
```

6. Restart the Administration Server to make these changes take effect, stopping it with the nmKill command, or with the Administration Console, and then starting it with the nmStart command. Before the restart, stop all Managed Servers in the domain through the Administration Console, and then start them after the restart. Log in to the Administration Console using the credentials for the weblogic user.

Modifying System-Level Settings Through MBeans

To ensure high availability, modify system-level configuration settings for WebCenter Content user interface through the System Configuration page in Fusion Middleware Control. The settings on this page configure the WebCenter Content user interface MBeans for the domain.

For information about how to modify system-level settings in Fusion Middleware control, see *Modifying System Configuration Settings in Oracle Fusion Middleware Administering Oracle WebCenter Capture*.

Modify the required parameters:

1. To set the AdfScopeHaSupport parameter, complete the following steps:
 - a. From the **WebLogic Domain** menu, select **System MBean Browser**.
 - b. From the left navigation, go to **Application Defined MBeans** > **oracle.adf.share.config** > **Domain:WCC server name** > **Application: Oracle WebCenter Content - Web UI** > **ADFConfig** > **ADFConfig** > **ADFConfig** > **ADFConfiguration**.
 - c. Set the AdfScopeHaSupport parameter to true.
 - d. Click **Apply**.
2. To set the ClusterCompatible and TemporaryDirectory parameters, complete the following steps:

- a. From the **WebLogic Domain** menu, select **System MBean Browser**.
 - b. From the left navigation, go to **Application Defined MBeans** > **oracle.adf.share.config** > **Domain:WCC server name** > **Application: Oracle WebCenter Content - Web UI** > **ADFConfig** > **ADFConfig** > **ADFConfig** > **WccAdfConfiguration**.
 - c. Set the `ClusterCompatible` parameter to `true`.
 - d. Set the `TemporaryDirectory` parameter to `/u01/oracle/config/domains/WCCDomain/WCCUI_Cluster/tempdir`.
 - e. Click **Apply**.
3. To set the `PropConnectionUrl` parameter, complete the following steps:
 - a. From the **WebLogic Domain** menu, select **System MBean Browser**.
 - b. From the left navigation, go to **Application Defined MBeans** > **oracle.adf.share.connections** > **Domain:WCC server name** > **Application: Oracle WebCenter Content - Web UI** > **ADFConnections** > **ADFConnections** > **WccConnection** > **WccAdfServerConnection**.
 - c. Set the `PropConnectionUrl` parameter to `idc://wccinternal.example.com:6300`.
 - d. Click **Apply**.
4. To set the `ApplicationUrl` parameter, complete the following steps:
 - a. From the **WebLogic Domain** menu, select **System MBean Browser**.
 - b. From the left navigation, go to **Application Defined MBeans** > **oracle.adf.share.connections** > **Domain:WCC server name** > **Application: Oracle WebCenter Content - Web UI** > **ADFConfig** > **ADFConfig** > **ADFConfig** > **WccAdfConfiguration**.
 - c. Set the `ApplicationUrl` parameter to `https://wcc.example.com:443`.
 - d. Click **Apply**.

Configuring Oracle HTTP Server with the WebCenter Content User Interface Cluster

Configure Oracle HTTP Server with the WebCenter Content User Interface Cluster, set the front-end HTTP Host and Port for the cluster, and validate access through the load balancer.

This section contains the following tasks.

- [Configuring Oracle HTTP Server for the WLS_WCCUI Managed Servers](#)
- [Setting the Front-End HTTP Host and Port for the WebCenter Content User Interface Cluster](#)
- [Validating Access Through the Load Balancer](#)

Configuring Oracle HTTP Server for the WLS_WCCUI Managed Servers

To configure Oracle HTTP Server for the WLS_WCCUI Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the ORACLE_INSTANCE/config/OHS/ohs1/moduleconf/wcc_vh.conf and ORACLE_INSTANCE/config/OHS/ohs2/moduleconf/wcc_vh.conf files:

```
# ADF UI
<Location /wcc>
  WebLogicCluster WCCHOST1:16225,WCCHOST2:16225
  WLSRequest ON
  WLCookieName WCCSID
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>
```

2. Restart both Oracle HTTP Servers.

Setting the Front-End HTTP Host and Port for the WebCenter Content User Interface Cluster

To set the front-end HTTP host and port for the WCC UI cluster:

1. Log in to the WebLogic Server Administration Console.
2. Go to the Change Center section and click **Lock & Edit**.
3. Expand the **Environment** node in the **Domain Structure** tree on the left.
4. Click **Clusters**.
5. On the Summary of Clusters page, select **WCCUI_Cluster**.
6. Open the **HTTP** tab.
7. Set the following values:
 - **Frontend Host:** wcc.example.com
 - **Frontend HTTPS Port:** 443
 - **Frontend HTTP Port:** 80
8. Click **Save**.
9. Click **Activate Changes** in the Change Center section of the Administration Console.
10. Restart the servers to make the front-end host directive in the cluster take effect.

Validating Access Through the Load Balancer

Verify URLs to ensure that appropriate routing and failover is working from the HTTP Server to WCCUI_Cluster. To verify the URLs:

1. While WLS_WCCUI2 is running, stop WLS_WCCUI1 from the WebLogic Server Administration Console.
2. Access `https://wcc.example.com/wcc` to verify that it is functioning properly. (You will not be able to retrieve reports or data because the Capture server is down.)
3. Start WLS_WCCUI1 from the WebLogic Server Administration Console.
4. Stop WLS_WCCUI2 from the WebLogic Server Administration Console.
5. Access `https://wcc.example.com/wcc` to verify that it is functioning properly.

You can verify the cluster node to which you were directed after the traffic balancing provided through your load balancer and then again through the web tier.

Completing the Workflow Configuration

To complete the workflow configuration for the WebCenter Content user interface, you need to restart the Managed Servers and verify the configuration. The `UseDatabaseWfInQueue` configuration variable enables the WebCenter Content user interface to filter workflows assigned to a user. The `EmailNotificationType` configuration variable specifies where the links in notification emails point for workflows and subscriptions in different Content Server user interfaces, and its default value is `NativeWebUI`.

To complete the workflow configuration:

1. Make sure that the `WCCHOST1/ucm/cs/config/config.cfg` file contains the `EmailNotificationType` variable with either of the following settings:
 - To generate emails with links that point only to the WebCenter Content user interface, set `EmailNotificationType=ContentUI` in `config.cfg`.
 - To generate emails with links that point to both the WebCenter Content user interface and the native 11g user interface, set `EmailNotificationType=ContentUI,NativeWebUI` in `config.cfg`.
2. Restart the Content Server Managed Server, using the WebLogic Server Administration Console.
3. Click the alert that appears on the Content Server home page after restart: **Click to complete workflow setup**.

Ensure that Content Server returns a success message: The setup for workflow in queue was successful.
4. Restart the WebCenter Content user interface Managed Server, using the WebLogic Server Administration Console for the WebCenter Content user interface domain.

or more information about workflows, see "Managing Workflows" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

Part IV

Common Configuration and Management Procedures for an Enterprise Deployment

There are certain configuration and management procedures that are recommended for a typical enterprise deployment.

The following topics contain configuration and management procedures that are required for a typical enterprise deployment.

- [Common Configuration and Management Tasks for an Enterprise Deployment](#)
The configuration and management tasks that may need to be performed on the enterprise deployment environment are detailed in this section.
- [Using Whole Server Migration and Service Migration in an Enterprise Deployment](#)
The Oracle WebLogic Server migration framework supports Whole Server Migration and Service Migration. The following sections explain how these features can be used in an Oracle Fusion Middleware enterprise topology.
- [Configuring Single Sign-On for an Enterprise Deployment](#)
You need to configure the Oracle HTTP Server WebGate in order to enable single sign-on with Oracle Access Manager.

Common Configuration and Management Tasks for an Enterprise Deployment

The configuration and management tasks that may need to be performed on the enterprise deployment environment are detailed in this section.

- [Verifying Appropriate Sizing and Configuration for the WLSSchemaDataSource](#)
WLSSchemaDataSource is the common datasource that is reserved for use by the FMW components for JMS JDBC Stores, JTA JDBC stores, and Leasing services. WLSSchemaDataSource is used to avoid contention in critical WLS infrastructure services and to guard against dead-locks.
- [Verifying Manual Failover of the Administration Server](#)
In case a host computer fails, you can fail over the Administration Server to another host. The steps to verify the failover and failback of the Administration Server from WCCHOST1 and WCCHOST2 are detailed in the following sections.
- [Configuring Listen Addresses in Dynamic Cluster Server Templates](#)
The default configuration for dynamic managed servers in dynamic clusters is to listen on all available network interfaces. In most cases, this may be undesirable.
- [Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer](#)
It is important to understand how to enable SSL communication between the middle tier and the hardware load balancer.
- [Configuring Roles for Administration of an Enterprise Deployment](#)
In order to manage each product effectively within a single enterprise deployment domain, you must understand which products require specific administration roles or groups, and how to add a product-specific administration role to the Enterprise Deployment Administration group.
- [Using Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#)
The persistent store provides a built-in, high-performance storage solution for WebLogic Server subsystems and services that require persistence.
- [Performing Backups and Recoveries for an Enterprise Deployment](#)
It is recommended that you follow the below mentioned guidelines to make sure that you back up the necessary directories and configuration data for an Oracle WebCenter Content enterprise deployment.
- [Modifying the Upload and Stage Directories to an Absolute Path in an Enterprise Deployment](#)
After you configure the domain and unpack it to the Managed Server domain directories on all the hosts, verify and update the upload and stage directories for Managed Servers in the new clusters. Also, update the upload directory for the AdminServer to have the same absolute path instead of relative, otherwise deployment issues can occur. If you implement dynamic clusters, the configuration of the server template assigned to each newly added cluster should be verified and updated, otherwise, verify and update every statically-defined Managed Server for the newly added clusters.

- [Starting and Stopping Servers in Dynamic Clusters](#)
You can start and stop server instances in dynamic clusters by using the same methods you use to start and stop server instances in configured static clusters.
- [Expanding or Reducing Dynamic Clusters](#)
When you create a dynamic cluster, WebLogic Server generates the number of dynamic servers you specify. Before you decide upon the number of server instances, ensure you have the performance capacity to handle the desired number.

Verifying Appropriate Sizing and Configuration for the WLSSchemaDataSource

WLSSchemaDataSource is the common datasource that is reserved for use by the FMW components for JMS JDBC Stores, JTA JDBC stores, and Leasing services. WLSSchemaDataSource is used to avoid contention in critical WLS infrastructure services and to guard against dead-locks.

To reduce the WLSSchemaDataSource connection usage, you can change the JMS JDBC and TLOG JDBC stores connection caching policy from *Default* to *Minimal* by using the respective connection caching policy settings. When there is a need to reduce connections in the back-end database system, Oracle recommends that you set the caching policy to *Minimal*. Avoid using the caching policy *None* because it causes a potential degradation in performance. For a detailed tuning advice about connections that are used by JDBC stores, see *Configuring a JDBC Store Connection Caching Policy* in *Oracle Fusion Middleware Administering the WebLogic Persistent Store*.

The default WLSSchemaDataSource connection pool size is 75 (size is double in the case of a GridLink DataSource). You can tune this size to a higher value depending on the size of the different FMW clusters and the candidates that are configured for migration. For example, consider a typical SOA EDG deployment with the default number of worker threads per store. If more than 25 JDBC Stores or TLOG-in-DB instances or both can fail over to the same Weblogic server, and the Connection Caching Policy is not changed from *Default* to *Minimal*, possible connection contention issues could arise. In these cases, increasing the default WLSSchemaDataSource pool size (maximum capacity) becomes necessary (each JMS store uses a minimum of two connections, and leasing and JTA are also added to compete for the pool).

Verifying Manual Failover of the Administration Server

In case a host computer fails, you can fail over the Administration Server to another host. The steps to verify the failover and failback of the Administration Server from WCCHOST1 and WCCHOST2 are detailed in the following sections.

Assumptions:

- The Administration Server is configured to listen on ADMINVHN, and not on localhost or on any other host's address.
For more information about the ADMINVHN virtual IP address, see [Reserving the Required IP Addresses for an Enterprise Deployment](#).
- These procedures assume that the Administration Server domain home (ASERVER_HOME) has been mounted on both host computers. This ensures that

the Administration Server domain configuration files and the persistent stores are saved on the shared storage device.

- The Administration Server is failed over from WCCHOST1 to WCCHOST2, and the two nodes have these IPs:
 - WCCHOST1: 100.200.140.165
 - WCCHOST2: 100.200.140.205
 - ADMINVHN : 100.200.140.206. This is the Virtual IP where the Administration Server is running, assigned to a virtual sub-interface (for example, eth0:1), to be available on WCCHOST1 or WCCHOST2.
- Oracle WebLogic Server and Oracle Fusion Middleware components have been installed in WCCHOST2 as described in the specific configuration chapters in this guide.

Specifically, both host computers use the exact same path to reference the binary files in the Oracle home.

The following topics provide details on how to perform a test of the Administration Server failover procedure.

- [Failing Over the Administration Server to a Different Host](#)
The following procedure shows how to fail over the Administration Server to a different node (WCCHOST2). Note that even after failover, the Administration Server will still use the same Oracle WebLogic Server *machine* (which is a logical machine, not a physical machine).
- [Validating Access to the Administration Server on WCCHOST2 Through Oracle HTTP Server](#)
If you have configured the web tier to access AdminServer, it is important to verify that you can access the Administration Server after you perform a manual failover of the Administration Server, by using the standard administration URLs.
- [Failing the Administration Server Back to WCCHOST1](#)
After you have tested a manual Administration Server failover, and after you have validated that you can access the administration URLs after the failover, you can then migrate the Administration Server back to its original host.

Failing Over the Administration Server to a Different Host

The following procedure shows how to fail over the Administration Server to a different node (WCCHOST2). Note that even after failover, the Administration Server will still use the same Oracle WebLogic Server *machine* (which is a logical machine, not a physical machine).

This procedure assumes you've configured a per domain Node Manager for the enterprise topology. See [About the Node Manager Configuration in a Typical Enterprise Deployment](#)

To fail over the Administration Server to a different host:

1. Stop the Administration Server.
2. Stop the Node Manager in the Administration Server domain directory (ASERVER_HOME).
3. Migrate the ADMINVHN virtual IP address to the second host:

- a. Run the following command as root on WCCHOST1 to check the virtual IP address at its CIDR:

```
ip addr show dev ethX
```

Where, X is the current interface used by ADMINVHN.

For example:

```
ip addr show dev eth0
```

- b. Run the following command as root on WCCHOST1 (where X:Y is the current interface used by ADMINVHN):

```
ip addr del ADMINVHN/CIDR dev ethX:Y
```

Where, X:Y is the current interface used by ADMINVHN.

For example:

```
ip addr del 100.200.140.206/24 dev eth0:1
```

- c. Run the following command as root on WCCHOST2:

```
ip addr add ADMINVHN/CIDR dev ethX:Y
```

Where, X:Y is the current interface used by ADMINVHN.

For example:

```
ip addr add 100.200.140.206/24 dev eth0:1
```

 Note:

Ensure that the CIDR representing the netmask and interface to be used to match the available network configuration in WCCHOST2.

The name of the network interface device may something other than ethX, especially on systems with redundant bonded interfaces.

4. Update the routing tables using arping, for example:

```
arping -b -A -c 3 -I eth0 100.200.140.206
```
5. Start the Node Manager in the Administration Server domain home on WCCHOST2.
6. Start the Administration Server on WCCHOST2.
7. Test that you can access the Administration Server on WCCHOST2 as follows:
 - a. Ensure that you can access the Oracle WebLogic Server Administration Console using the following URL:

```
http://ADMINVHN:7001/console
```
 - b. Check that you can access and verify the status of components in Fusion Middleware Control using the following URL:

```
http://ADMINVHN:7001/em
```


Validating Access to the Administration Server on WCCHOST2 Through Oracle HTTP Server

If you have configured the web tier to access AdminServer, it is important to verify that you can access the Administration Server after you perform a manual failover of the Administration Server, by using the standard administration URLs.

From the load balancer, access the following URLs to ensure that you can access the Administration Server when it is running on WCCHOST2:

- `http://admin.example.com/console`
This URL should display the WebLogic Server Administration console.
- `http://admin.example.com/em`
This URL should display Oracle Enterprise Manager Fusion Middleware Control.

Failing the Administration Server Back to WCCHOST1

After you have tested a manual Administration Server failover, and after you have validated that you can access the administration URLs after the failover, you can then migrate the Administration Server back to its original host.

1. Stop the Administration Server.
2. Stop the Node Manager in the Administration Server domain directory (ASERVER_HOME).
3. Migrate the ADMINVHN virtual IP address to the second host:
 - a. Run the following command as root on WCCHOST2 to check the virtual IP address at its CIDR:

```
ip addr show dev ethX
```

Where, X is the current interface used by ADMINVHN.
For example:

```
ip addr show dev eth0
```
 - b. Run the following command as root on WCCHOST2 (where X:Y is the current interface used by ADMINVHN):

```
ip addr del ADMINVHN/CIDR dev ethX:Y
```

Where, X:Y is the current interface used by ADMINVHN.
For example:

```
ip addr del 100.200.140.206/24 dev eth0:1
```
 - c. Run the following command as root on WCCHOST1:

```
ip addr add ADMINVHN/CIDR dev ethX:Y
```

Where, X:Y is the current interface used by ADMINVHN.
For example:

```
ip addr add 100.200.140.206/24 dev eth0:1
```

 Note:

Ensure that the CIDR representing the netmask and interface to be used to match the available network configuration in WCCHOST1.

4. Update the routing tables using arping, for example:

```
arping -b -A -c 3 -I eth0 100.200.140.206
```
5. Start the Node Manager in the Administration Server domain home on WCCHOST1.
6. Start the Administration Server on WCCHOST1.
7. Test that you can access the Administration Server on WCCHOST1 as follows:
 - a. Ensure that you can access the Oracle WebLogic Server Administration Console using the following URL:

```
http://ADMINVHN:7001/console
```
 - b. Check that you can access and verify the status of components in Fusion Middleware Control using the following URL:

```
http://ADMINVHN:7001/em
```

Configuring Listen Addresses in Dynamic Cluster Server Templates

The default configuration for dynamic managed servers in dynamic clusters is to listen on all available network interfaces. In most cases, this may be undesirable.

In preparation for disaster recovery, Oracle recommends that you use host name aliases that can be mapped to different IPs in different data centers (for example, WCCHOST1, WCCHOST2) to set each server's listen address to a specific network interface. With dynamic clusters, each server cannot be configured specifically. There is only one listen address configuration in the cluster's server-template. To effectively set the listen-address properly for each dynamic server in the cluster, a calculated macro must be used.

WebLogic Server provides the "\${id}" macro which corresponds to the index number of the dynamic server in the cluster. This index starts at the numeral one ("1") and increments to the current managed server count for the cluster. This sequentially-numbered server ID macro can be used with the recommended host naming pattern to have the Listen address calculated for each Dynamic Server to listen on a specific network interface.

This approach is recommended for enterprise deployment environments where there is only one managed server per host per cluster and the cluster is expected to scale-out horizontally only.

To configure the server-template Listen Address using the \${id} macro:

1. Verify that the required WCCHOST n , WEBHOST n , entries in /etc/hosts are configured to the appropriate IP address for the intended machines.

For example:

```
10.229.188.205 host1.example.com host1 WCCHOST1
10.229.188.206 host2.example.com host2 WCCHOST2
10.229.188.207 host3.example.com host5 WEBHOST1
10.229.188.208 host4.example.com host6 WEBHOST2
```

For information about the requirements for name resolution, see [Verifying IP Addresses and Host Names in DNS or hosts File](#).

2. Browse to the Oracle WebLogic Server Administration console, and sign in with your administrative credentials.

`http://adminvhn:7001/console`
3. **Lock & Edit** the domain.
4. Navigate to **Clusters > Server Templates**, and select the server template to be modified.
5. Set the Listen Address value to the appropriate abstracted listener hostname, with the variable assignment as written.

For example:

```
wmpm-server-template : Listen Address = WCCHOST${id}
UCM-server-template  : Listen Address = WCCHOST${id}
soa-server-template   : Listen Address = WCCHOST${id}
CPT-server-template   : Listen Address = WCCHOST${id}
IPM-server-template   : Listen Address = WCCHOST${id}
```

6. Click **Save**.
 7. Repeat from step 4 if additional server templates need to be modified.
 8. Click **Activate Changes**.
 9. Restart the servers that use the template, for the changes to be effective.
- [Configuring Server Template Listen Addresses Using the Machine Name](#)

Configuring Server Template Listen Addresses Using the Machine Name

If your host naming or aliasing convention does not follow a sequential numbering pattern starting at 1, to correlate to the internal ID number of each dynamic server, or you desire the cluster to scale-up with multiple managed servers per host per cluster, then an alternative configuration may be preferred. In this case, you can use the `${machineName}` macro value to specify the listen address instead of using a host name prefix and server ID macro pattern. The `${machineName}` macro will use the display name of the machine that is dynamically assigned to the server, and requires that the machine name be resolvable to an IP address.

To configure the server-template Listen Address with the `${machineName}` macro:

1. Browse to the Oracle WebLogic Server Administration console, and sign in with your administrative credentials:

```
http://adminvhn:7001/console
```

2. Navigate to **Machines** to review the list of machine names.
3. Validate to ensure that these names are resolvable as network addresses, using the OS commands such as `ping`.
4. **Lock & Edit** the domain.
5. Navigate to **Clusters** and then **Server Templates**, and select the server-template that you want to modify.
6. Set the Listen Address value to `${machineName}` as written here. Do not substitute any other value.
7. Click **Save**.
8. Repeat from step 5 if you want to modify additional server-templates.
9. Click **Activate Changes**.
10. Restart the servers that use the modified server-template, for the changes to be effective.

Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer

It is important to understand how to enable SSL communication between the middle tier and the hardware load balancer.



Note:

The following steps are applicable if the hardware load balancer is configured with SSL and the front-end address of the system has been secured accordingly.

- [When is SSL Communication Between the Middle Tier and Load Balancer Necessary?](#)
- [Generating Self-Signed Certificates Using the `utils.CertGen` Utility](#)
- [Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility](#)
- [Creating a Trust Keystore Using the `Keytool` Utility](#)
- [Importing the Load Balancer Certificate into the Truststore](#)
- [Adding the Updated Trust Store to the Oracle WebLogic Server Start Scripts](#)
- [Configuring Node Manager to Use the Custom Keystores](#)
- [Configuring WebLogic Servers to Use the Custom Keystores](#)
- [Testing Composites Using SSL Endpoints](#)

When is SSL Communication Between the Middle Tier and Load Balancer Necessary?

In an enterprise deployment, there are scenarios where the software running on the middle tier must access the front-end SSL address of the hardware load balancer. In these scenarios, an appropriate SSL handshake must take place between the load balancer and the invoking servers. This handshake is not possible unless the Administration Server and Managed Servers on the middle tier are started by using the appropriate SSL configuration.

Generating Self-Signed Certificates Using the utils.CertGen Utility

This section describes the procedure to create self-signed certificates on WCCHOST1. Create certificates for every app-tier host by using the network name or alias of each host.

The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends that you use central or shared stores for the certificates used for different purposes (for example, SSL set up for HTTP invocations). See the information on filesystem specifications for the KEYSTORE_HOME location provided in [Understanding the Recommended Directory Structure for an Enterprise Deployment](#).

For information on using trust CA certificates instead, see the information about configuring identity and trust in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

About Passwords

The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that include both uppercase and lowercase characters as well as numbers.

To create self-signed certificates:

1. Temporarily, set up your environment by running the following script:

```
. WL_HOME/server/bin/setWLSEnv.sh
```

Note that there is a dot(.) and space() preceding the script name in order to source the shell script in the current shell.

2. Verify that the `CLASSPATH` environment variable is set:

```
echo $CLASSPATH
```
3. Verify that the shared configuration directory folder has been created and mounted to shared storage correctly, as described in [Preparing the File System for an Enterprise Deployment](#).

For example, use the following command to verify that the shared configuration directory is available to each host:

```
df -h | grep -B1 SHARED_CONFIG_DIR
```

Replace `SHARED_CONFIG_DIR` with the actual path to your shared configuration directory.

You can also do a listing of the directory to ensure that it is available to the host:

```
ls -al SHARED_CONFIG_DIR
```

4. Create the keystore home folder structure if does not already exist.

For example:

```
cd SHARED_CONFIG_DIR
mkdir keystores
chown oracle:oinstall keystores
chmod 750 keystores
export KEYSTORE_HOME=SHARED_CONFIG_DIR/keystores
```

5. Change directory to the keystore home:

```
cd KEYSTORE_HOME
```

6. Run the `utils.CertGen` tool to create the certificates for hostnames or aliases used by the managed servers and node managers, one per host.

 Note:

You must run the `utils.CertGen` tool to create certificates for all the other hosts that run the Manager Servers.

Syntax:

```
java utils.CertGen key_passphrase cert_file_name key_file_name [export | domestic] [hostname]
```

Examples:

```
java utils.CertGen password ADMINVHN.example.com_cert \
ADMINVHN.example.com_key domestic ADMINVHN.example.com
```

```
java utils.CertGen password WCCHOST1.example.com_cert \
WCCHOST1.example.com_key domestic WCCHOST1.example.com
```

7. Repeat the above step for all the remaining hosts used in the system (for example, `WCCHOST2`, `WCCHOST1`, and `WCCHOST2`).
8. For Dynamic clusters, in addition to `ADMINVHN` and one certificate for each host, a certificate matching a wildcard URL should also be generated.

For example:

```
java utils.CertGen password WILDCARD.example.com_cert \
WILDCARD.example.com_key domestic *.example.com
```

Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility

This section describes how to create an Identity Keystore on `WCCHOST1.example.com`.

In previous sections you have created certificates and keys that reside on shared storage. In this section, the certificate and private keys created earlier for all hosts and ADMINVHN are imported into a new Identity Store. Make sure that you use a different alias for each of the certificate and key pair imported.

 Note:

The Identity Store is created (if none exists) when you import a certificate and the corresponding key into the Identity Store by using the `utils.ImportPrivateKey` utility.

1. Import the certificate and private key for ADMINVHN and WCCHOST1 into the Identity Store. Make sure that you use a different alias for each of the certificate and key pair imported.

Syntax:

```
java utils.ImportPrivateKey
  -certfile cert_file
  -keyfile private_key_file
  [-keyfilepass private_key_password]
  -keystore keystore
  -storepass storepass
  [-storetype storetype]
  -alias alias
  [-keypass keypass]
```

 Note:

The default `keystore_type` is `jks`.

Examples:

```
java utils.ImportPrivateKey\
  -certfile KEYSTORE_HOME/ADMINVHN.example.com_cert.pem\
  -keyfile KEYSTORE_HOME/ADMINVHN.example.com_key.pem\
  -keyfilepass password\
  -keystore appIdentityKeyStore.jks\
  -storepass password\
  -alias ADMINVHN\
  -keypass password
```

```
java utils.ImportPrivateKey\
  -certfile KEYSTORE_HOME/WCCHOST1.example.com_cert.pem\
  -keyfile KEYSTORE_HOME/WCCHOST1.example.com_key.pem\
  -keyfilepass password\
  -keystore appIdentityKeyStore.jks\
  -storepass password\
```

```
-alias WCCHOST1\  
-keypass password
```

2. Repeat the `java importPrivateKey` command for each of the remaining host-specific certificate and key pairs. (for example, for WCCHOST1, WCCHOST2).

 Note:

Make sure to use a unique alias for each certificate and key pair imported.

3. For Dynamic clusters, import the wildcard certificate and private key pair by using the custom id alias of WILDCARD.

Example:

```
${JAVA_HOME}/bin/java utils.ImportPrivateKey \  
-certfile ${KEYSTORE_HOME}/WILDCARD.example.com_cert.pem \  
-keyfile ${KEYSTORE_HOME}/WILDCARD.example.com_key.pem \  
-keyfilepass password \  
-keystore ${KEYSTORE_HOME}/appIdentityKeyStore.jks \  
-storepass password \  
-alias WILDCARD \  
-keypass password
```

Creating a Trust Keystore Using the Keytool Utility

To create the Trust Keystore on WCCHOST1.example.com:

1. Copy the standard java keystore to create the new trust keystore since it already contains most of the root CA certificates needed.

Oracle does not recommend modifying the standard Java trust key store directly. Copy the standard Java keystore CA certificates located under the `WL_HOME/server/lib` directory to the same directory as the certificates. For example:

```
cp WL_HOME/server/lib/cacerts KEystore_HOME/appTrustKeyStore.jks
```

2. Use the keytool utility to change the default password.

The default password for the standard Java keystore is `changeit`. Oracle recommends that you always change the default password, as follows:

```
keytool -storepasswd -new NewPassword -keystore TrustKeyStore -storepass  
Original_Password
```

For example:

```
keytool -storepasswd -new password -keystore appTrustKeyStore.jks -storepass  
changeit
```

3. Import the CA certificate into the `appTrustKeyStore` by using the keytool utility.

The CA certificate `CertGenCA.der` is used to sign all certificates generated by the `utils.CertGen` tool and is located at `WL_HOME/server/lib` directory.

Use the following syntax to import the certificate:


```
keytool -import -v -noprompt -trustcacerts -alias AliasName -file
CAFileLocation -keystore KeyStoreLocation -storepass KeyStore_Password
```

For example:

```
keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_HOME/
server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass password
```

Importing the Load Balancer Certificate into the Truststore

For the SSL handshake to act properly, the load balancer's certificate must be added to the WLS servers truststore. To add a load balancer's certificate:

1. Access the site on SSL with a browser (this adds the server's certificate to the browser's repository).
2. From the browser's certificate management tool, export the certificate to a file that is on the server's file system (with a file name such as `soa.example.com.crt`).
3. Use the keytool to import the load balancer's certificate into the truststore:

For example:

```
keytool -import -file /oracle/certificates/soa1.cz.example.com -v -keystore
appTrustKeyStore.jks -alias aliasSOA -storepass password
keytool -import -file /oracle/certificates/soa1-osb.cz.example.com.crt -v -
keystore appTrustKeyStore.jks -alias aliasOSB -storepass password
```

Note:

The need to add the load balancer certificate to the WLS server truststore applies only to self-signed certificates. If the load balancer certificate is issued by a third-party CA, you have to import the public certificates of the root and the intermediate CAs into the truststore.

Adding the Updated Trust Store to the Oracle WebLogic Server Start Scripts

The `setDomainEnv.sh` script is provided by Oracle WebLogic Server and is used to start the Administration Server and the Managed Servers in the domain. To ensure that each server accesses the updated trust store, edit the `setDomainEnv.sh` script in each of the domain home directories in the enterprise deployment.

1. Log in to `WCCHOST1` and open the following file with a text editor:

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

2. Replace reference to the existing `DemoTrust.jks` entry with the following entry:

Note:

All the values for `EXTRA_JAVA_PROPERTIES` must be on one line in the file, followed by the export command on a new line.

```
EXTRA_JAVA_PROPERTIES="-Djavax.net.ssl.trustStore=/u01/oracle/config/
keystores/appTrustKeyStore.jks ${EXTRA_JAVA_PROPERTIES} ....."
export EXTRA_JAVA_PROPERTIES
```

3. Make the same change to the `setDomainEnv.sh` file in the `MSERVER_HOME/bin` directory `WCCHOST1`, `WCCHOST2`.

Note:

The `setDomainEnv.sh` file cannot be copied between `ASERVER_HOME/bin` and `MSERVER_HOME/bin` as there are differences in the files for these two domain home locations. The `MSERVER_HOME/bin/setDomainEnv.sh` file can be copied between hosts.

WebLogic Server automatically overwrites the `setDomainEnv.sh` file after each domain extension. Some patches may also replace this file. Verify your customizations to `setDomainEnv.sh` after each of these types of maintenance operations.

Configuring Node Manager to Use the Custom Keystores

To configure the Node Manager to use the custom keystores, add the following lines to the end of the `nodemanager.properties` files located both in `ASERVER_HOME/nodemanager` and `MSERVER_HOME/nodemanager` directories in all nodes:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity KeyStore
CustomIdentityKeyStorePassPhrase=Identity KeyStore Passwd
CustomIdentityAlias=Identity Key Store Alias
CustomIdentityPrivateKeyPassPhrase=Private Key used when creating Certificate
```

Make sure to use the correct value for `CustomIdentityAlias` for Node Manager's listen address. For example, in the `WCCHOST1 MSERVER_HOME`, use the alias `WCCHOST1` and in the `ASERVER_HOME` on `WCCHOST1`, use the alias `ADMINVHN` according to the steps in [Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility](#).

```
Example for WCCHOST1:
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=KEYSTORE_HOME/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=password
CustomIdentityAlias=WCCHOST1
CustomIdentityPrivateKeyPassPhrase=password
```

The passphrase entries in the `nodemanager.properties` file are encrypted when you start Node Manager. For security reasons, minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, restart Node Manager as soon as possible so that the entries are encrypted.

 Note:

The CustomIdentityAlias value will need to be corrected every time the domain is extended after this configuration is performed. An unpack operation will replace the CustomIdentityAlias with the Administration Server's value when the domain configuration is written.

Configuring WebLogic Servers to Use the Custom Keystores

Configure the WebLogic Servers to use the custom keystores using the Oracle WebLogic Server Administration Console. Complete this procedure for the Administration Server and the Managed Servers that require access to the front end LBR on SSL.

To configure the identity and trust keystores:

1. Log in to the Administration Console, and click **Lock & Edit**.
2. In the left pane, expand **Environment**, and select **Servers**.
3. Click the name of the server for which you want to configure the identity and trust keystores.
4. Select **Configuration**, and then **Keystores**.
5. In the **Keystores** field, click **Change**, and select **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates, and click Save.
6. In the Identity section, define attributes for the identity keystore.
 - Custom Identity Keystore: Enter the fully qualified path to the identity keystore:
`KEYSTORE_HOME/appIdentityKeyStore.jks`
 - Custom Identity Keystore Type: Leave this field blank, it defaults to JKS.
 - Custom Identity Keystore Passphrase: Enter the password
Keystore_Password you provided in [Creating an Identity Keystore Using the utils.ImportPrivateKey Utility](#)

This attribute may be optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server reads only from the keystore, so whether or not you define this property depends on the requirements of the keystore.
7. In the Trust section, define properties for the trust keystore:
 - Custom Trust Keystore: Enter the fully qualified path to the trust keystore:
`KEYSTORE_HOME/appTrustKeyStore.jks`
 - Custom Trust Keystore Type: Leave this field blank, it defaults to JKS.
 - Custom Trust Keystore Passphrase: The password you provided as the New_Password value in [Creating a Trust Keystore Using the Keytool Utility](#).

As mentioned in the previous step, this attribute may be optional or required depending on the type of keystore.

8. Click **Save**.
9. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.
10. Click **Lock & Edit**.
11. Select **Configuration**, then **SSL**.
12. In the Private Key Alias field, enter the alias you used for the host name the managed server listens on.

In the Private Key Passphrase and the Confirm Private Key Passphrase fields, enter the password for the keystore that you created in [Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility](#)
13. Click **Save**.
14. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
15. Restart the Administration Server.
16. Restart the Managed Servers where the keystore has been updated.

 Note:

The fact that servers can be restarted using the Administration Console/ Node Manager is a good verification that the communication between Node Manager, Administration Server, and the managed servers is correct.

Testing Composites Using SSL Endpoints

Once SSL has been enabled, composites endpoints can be verified on SSL from Oracle Enterprise Manager FMW Control. To test an SSL endpoint, follow these steps:

1. Enter the following URL into a browser to display the Fusion Middleware Control login screen:

`http://ADMINVHN:7001/em`

In this example:
 - Replace ADMINVHN with the host name that is assigned to the ADMINVHN Virtual IP address in [Identifying and Obtaining Software Distributions for an Enterprise Deployment](#).
 - Port 7001 is the typical port used for the Administration Server console and Fusion Middleware Control. However, you should use the actual URL that was displayed at the end of the Configuration Wizard session when you created the domain.
2. Log in to Fusion Middleware Control by using the administrative user credentials.

3. From the tree on the left, expand SOA, then click **soa-infra** (WLS_SOA1).
4. Click the **Deployed Composites** navigation tab link.
5. Click **Composite** to open the composite's dashboard view.
6. Click the **Test** button and select one of the services from drop-down.
7. In the WSDL or WADL address, replace the base URL (<http://wccHost1:8001>) with the front-end load balancer base url (<https://wcc.example.com:443>) keeping the URI resource path and query string intact.
8. Click **Parse WSDL or WADL**.
9. Verify that the Endpoint URL shown is SSL, and no errors are returned.
10. Test the composite. If the response is as expected for the web service, the SSL communication between the Administration Server and the Load Balancer has been configured properly.

Configuring Roles for Administration of an Enterprise Deployment

In order to manage each product effectively within a single enterprise deployment domain, you must understand which products require specific administration roles or groups, and how to add a product-specific administration role to the Enterprise Deployment Administration group.

Each enterprise deployment consists of multiple products. Some of the products have specific administration users, roles, or groups that are used to control administration access to each product.

However, for an enterprise deployment, which consists of multiple products, you can use a single LDAP-based authorization provider and a single administration user and group to control access to all aspects of the deployment. See [Creating a New LDAP Authenticator and Provisioning a New Enterprise Deployment Administrator User and Group](#).

To be sure that you can manage each product effectively within the single enterprise deployment domain, you must understand which products require specific administration roles or groups, you must know how to add any specific product administration roles to the single, common enterprise deployment administration group, and if necessary, you must know how to add the enterprise deployment administration user to any required product-specific administration groups.

For more information, see the following topics.

- [Summary of Products with Specific Administration Roles](#)
- [Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group](#)

Summary of Products with Specific Administration Roles

The following table lists the Fusion Middleware products that have specific administration roles, which must be added to the enterprise deployment administration group (WCCAdministrators), which you defined in the LDAP Authorization Provider for the enterprise deployment.

Use the information in the following table and the instructions in [Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group](#) to add the required administration roles to the enterprise deployment Administration group.

Product	Application Stripe	Administration Role to be Assigned
SOA Infrastructure	soa-infra	SOAAdmin

Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group

For products that require a product-specific administration role, use the following procedure to add the role to the enterprise deployment administration group:

1. Sign-in to the Fusion Middleware Control by using the administrator's account (for example: weblogic_wcc), and navigate to the home page for your application.

These are the credentials that you created when you initially configured the domain and created the Oracle WebLogic Server Administration user name (typically, weblogic_wcc) and password.
2. From the **WebLogic Domain** menu, select **Security**, and then **Application Roles**.
3. For each production-specific application role, select the corresponding application stripe from the **Application Stripe** drop-down menu.
4. Click Search Application Roles icon  to display all the application roles available in the domain.
5. Select the row for the application role that you are adding to the enterprise deployment administration group.
6. Click the Edit icon  to edit the role.
7. Click the Add icon  on the Edit Application Role page.
8. In the Add Principal dialog box, select **Group** from the **Type** drop-down menu.
9. Search for the enterprise deployment administrators group, by entering the group name (for example, WCCAdministrators) in the **Principal Name Starts With** field and clicking the right arrow to start the search.
10. Select the administrator group in the search results and click **OK**.
11. Click **OK** on the Edit Application Role page.

Using Persistent Stores for TLOGs and JMS in an Enterprise Deployment

The persistent store provides a built-in, high-performance storage solution for WebLogic Server subsystems and services that require persistence.

For example, the JMS subsystem stores persistent JMS messages and durable subscribers, and the JTA Transaction Log (TLOG) stores information about the committed transactions that are coordinated by the server but may not have been completed. The persistent store supports persistence to a file-based store or to a JDBC-enabled database. Persistent stores' high availability is provided by server or service migration. Server or service migration requires that all members of a WebLogic cluster have access to the same transaction and JMS persistent stores (regardless of whether the persistent store is file-based or database-based).

For an enterprise deployment, Oracle recommends using JDBC persistent stores for transaction logs (TLOGs) and JMS.

This section analyzes the benefits of using JDBC versus File persistent stores and explains the procedure for configuring the persistent stores in a supported database. If you want to use File persistent stores instead of JDBC stores, the procedure for configuring them is also explained in this section.

- [Products and Components that use JMS Persistence Stores and TLOGs](#)
- [JDBC Persistent Stores vs. File Persistent Stores](#)
- [Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#)
- [Using File Persistent Stores for TLOGs and JMS in an Enterprise Deployment](#)

Products and Components that use JMS Persistence Stores and TLOGs

Determining which installed FMW products and components utilize persistent stores can be done through the WebLogic Server Console in the Domain Structure navigation under **DomainName** > **Services** > **Persistent Stores**. The list indicates the name of the store, the store type (FileStore and JDBC), and the target of the store. The stores listed that pertain to MDS are outside the scope of this chapter and should not be considered.

These components (as applicable) use stores by default:

Component/Product	JMS Stores	TLOG Stores
B2B	Yes	Yes
BAM	Yes	Yes
BPM	Yes	Yes
ESS	No	No
HC	Yes	Yes
Insight	Yes	Yes
MFT	Yes	Yes
OSB	Yes	Yes
SOA	Yes	Yes
WSM	No	No

Component/Product	JMS Stores	TLOG Stores
OAM	No	No

Component/Product	JMS Stores	TLOG Stores
OIM	Yes	Yes

JDBC Persistent Stores vs. File Persistent Stores

Oracle Fusion Middleware supports both database-based and file-based persistent stores for Oracle WebLogic Server transaction logs (TLOGs) and JMS. Before you decide on a persistent store strategy for your environment, consider the advantages and disadvantages of each approach.



Note:

Regardless of which storage method you choose, Oracle recommends that for transaction integrity and consistency, you use the same type of store for both JMS and TLOGs.

- [About JDBC Persistent Stores for JMS and TLOGs](#)
- [Performance Considerations for TLOGs and JMS Persistent Stores](#)

About JDBC Persistent Stores for JMS and TLOGs

When you store your TLOGs and JMS data in an Oracle database, you can take advantage of the replication and high availability features of the database. For example, you can use Oracle Data Guard to simplify cross-site synchronization. This is especially important if you are deploying Oracle Fusion Middleware in a disaster recovery configuration.

Storing TLOGs and JMS data in a database also means that you do not have to identify a specific shared storage location for this data. Note, however, that shared storage is still required for other aspects of an enterprise deployment. For example, it is necessary for Administration Server configuration (to support Administration Server failover), for deployment plans, and for adapter artifacts, such as the File and FTP Adapter control and processed files.

If you are storing TLOGs and JMS stores on a shared storage device, then you can protect this data by using the appropriate replication and backup strategy to guarantee zero data loss, and you potentially realize better system performance. However, the file system protection is always inferior to the protection provided by an Oracle Database.

For more information about the potential performance impact of using a database-based TLOGs and JMS store, see [Performance Considerations for TLOGs and JMS Persistent Stores](#).

Performance Considerations for TLOGs and JMS Persistent Stores

One of the primary considerations when you select a storage method for Transaction Logs and JMS persistent stores is the potential impact on performance. This topic

provides some guidelines and details to help you determine the performance impact of using JDBC persistent stores for TLOGs and JMS.

Performance Impact of Transaction Logs Versus JMS Stores

For transaction logs, the impact of using a JDBC store is relatively small, because the logs are very transient in nature. Typically, the effect is minimal when compared to other database operations in the system.

On the other hand, JMS database stores can have a higher impact on performance if the application is JMS intensive.

Factors that Affect Performance

There are multiple factors that can affect the performance of a system when it is using JMS DB stores for custom destinations. The main ones are:

- Custom destinations involved and their type
- Payloads being persisted
- Concurrency on the SOA system (producers on consumers for the destinations)

Depending on the effect of each one of the above, different settings can be configured in the following areas to improve performance:

- Type of data types used for the JMS table (using raw versus lob)
- Segment definition for the JMS table (partitions at index and table level)

Impact of JMS Topics

If your system uses Topics intensively, then as concurrency increases, the performance degradation with an Oracle RAC database will increase more than for Queues. In tests conducted by Oracle with JMS, the average performance degradation for different payload sizes and different concurrency was less than 30% for Queues. For topics, the impact was more than 40%. Consider the importance of these destinations from the recovery perspective when deciding whether to use database stores.

Impact of Data Type and Payload Size

When you choose to use the RAW or SecureFiles LOB data type for the payloads, consider the size of the payload being persisted. For example, when payload sizes range between 100b and 20k, then the amount of database time required by SecureFiles LOB is slightly higher than for the RAW data type.

More specifically, when the payload size reach around 4k, then SecureFiles tend to require more database time. This is because 4k is where writes move out-of-row. At around 20k payload size, SecureFiles data starts being more efficient. When payload sizes increase to more than 20k, then the database time becomes worse for payloads set to the RAW data type.

One additional advantage for SecureFiles is that the database time incurred stabilizes with payload increases starting at 500k. In other words, at that point it is not relevant (for SecureFiles) whether the data is storing 500k, 1MB or 2MB payloads, because the write is asynchronous, and the contention is the same in all cases.

The effect of concurrency (producers and consumers) on the queue's throughput is similar for both RAW and SecureFiles until the payload sizes reach 50K. For small

payloads, the effect on varying concurrency is practically the same, with slightly better scalability for RAW. Scalability is better for SecureFiles when the payloads are above 50k.

Impact of Concurrency, Worker Threads, and Database Partitioning

Concurrency and worker threads defined for the persistent store can cause contention in the RAC database at the index and global cache level. Using a reverse index when enabling multiple worker threads in one single server or using multiple Oracle WebLogic Server clusters can improve things. However, if the Oracle Database partitioning option is available, then global hash partition for indexes should be used instead. This reduces the contention on the index and the global cache buffer waits, which in turn improves the response time of the application. Partitioning works well in all cases, some of which will not see significant improvements with a reverse index.

Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment

This section explains the guidelines to use JDBC persistent stores for transaction logs (TLOGs) and JMS. It also explains the procedures to configure the persistent stores in a supported database.

- [Recommendations for TLOGs and JMS Datasource Consolidation](#)
To accomplish data source consolidation and connection usage reduction, use a single connection pool for both JMS and TLOGs persistent stores.
- [Roadmap for Configuring a JDBC Persistent Store for TLOGs](#)
The following topics describe how to configure a database-based persistent store for transaction logs.
- [Roadmap for Configuring a JDBC Persistent Store for JMS](#)
The following topics describe how to configure a database-based persistent store for JMS.
- [Creating a User and Tablespace for TLOGs](#)
Before you can create a database-based persistent store for transaction logs, you must create a user and tablespace in a supported database.
- [Creating a User and Tablespace for JMS](#)
Before you can create a database-based persistent store for JMS, you must create a user and tablespace in a supported database.
- [Creating GridLink Data Sources for TLOGs and JMS Stores](#)
Before you can configure database-based persistent stores for JMS and TLOGs, you must create two data sources: one for the TLOGs persistent store and one for the JMS persistent store.
- [Assigning the TLOGs JDBC Store to the Managed Servers](#)
After you create the tablespace and user in the database, and you have created the datasource, you can then assign the TLOGs persistence store to each of the required Managed Servers.
- [Creating a JDBC JMS Store](#)
After you create the JMS persistent store user and table space in the database, and after you create the data source for the JMS persistent store, you can then use the Administration Console to create the store.

- [Assigning the JMS JDBC store to the JMS Servers](#)
After you create the JMS tablespace and user in the database, create the JMS datasource, and create the JDBC store, then you can assign the JMS persistence store to each of the required JMS Servers.
- [Creating the Required Tables for the JMS JDBC Store](#)
The final step in using a JDBC persistent store for JMS is to create the required JDBC store tables. Perform this task before you restart the Managed Servers in the domain.

Recommendations for TLOGs and JMS Datasource Consolidation

To accomplish data source consolidation and connection usage reduction, use a single connection pool for both JMS and TLOGs persistent stores.

Oracle recommends you to reuse the WLSSchemaDataSource as is for TLOGs and JMS persistent stores under non-high workloads and consider increasing the WLSSchemaDataSource pool size. Reuse of datasource forces to use the same schema and tablespaces, and so the PREFIX_WLS_RUNTIME schema in the PREFIX_WLS tablespace is used for both TLOGs and JMS messages.

High stress (related with high JMS activity, for example) and contention in the datasource can cause stability and performance problems. For example:

- High contention in the DataSource can cause persistent stores to fail if no connections are available in the pool to persist JMS messages.
- High Contention in the DataSource can cause issues in transactions if no connections are available in the pool to update transaction logs.

For these cases, use a separate datasource for TLOGs and stores and a separate datasource for the different stores. You can still reuse the PREFIX_WLS_RUNTIME schema but configure separate custom datasources to the same schema to solve the contention issue.

Roadmap for Configuring a JDBC Persistent Store for TLOGs

The following topics describe how to configure a database-based persistent store for transaction logs.

1. [Creating a User and Tablespace for TLOGs](#)
2. [Creating GridLink Data Sources for TLOGs and JMS Stores](#)
3. [Assigning the TLOGs JDBC Store to the Managed Servers](#)

Note:

Steps 1 and 2 are optional. To accomplish data source consolidation and connection usage reduction, you can reuse PREFIX_WLS tablespace and WLSSchemaDataSource as described in [Recommendations for TLOGs and JMS Datasource Consolidation](#).

Roadmap for Configuring a JDBC Persistent Store for JMS

The following topics describe how to configure a database-based persistent store for JMS.

1. [Creating a User and Tablespace for JMS](#)
2. [Creating GridLink Data Sources for TLOGs and JMS Stores](#)
3. [Creating a JDBC JMS Store](#)
4. [Assigning the JMS JDBC store to the JMS Servers](#)
5. [Creating the Required Tables for the JMS JDBC Store](#)



Note:

Steps 1 and 2 are optional. To accomplish data source consolidation and connection usage reduction, you can reuse PREFIX_WLS tablespace and WLSSchemaDatasource as described in [Recommendations for TLOGs and JMS Datasource Consolidation](#).

Creating a User and Tablespace for TLOGs

Before you can create a database-based persistent store for transaction logs, you must create a user and tablespace in a supported database.

1. Create a tablespace called `tlogs`.

For example, log in to SQL*Plus as the `sysdba` user and run the following command:

```
SQL> create tablespace tlogs
      logging datafile 'path-to-data-file-or-+asmvolume'
      size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `TLOGS` and assign to it the `tlogs` tablespace.

For example:

```
SQL> create user TLOGS identified by password;

SQL> grant create table to TLOGS;

SQL> grant create session to TLOGS;

SQL> alter user TLOGS default tablespace tlogs;

SQL> alter user TLOGS quota unlimited on tlogs;
```

Creating a User and Tablespace for JMS

Before you can create a database-based persistent store for JMS, you must create a user and tablespace in a supported database.

1. Create a tablespace called `jms`.

For example, log in to SQL*Plus as the `sysdba` user and run the following command:

```
SQL> create tablespace jms
      logging datafile 'path-to-data-file-or-+asmvolume'
      size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `JMS` and assign to it the `jms` tablespace.

For example:

```
SQL> create user JMS identified by password;
```

```
SQL> grant create table to JMS;
```

```
SQL> grant create session to JMS;
```

```
SQL> alter user JMS default tablespace jms;
```

```
SQL> alter user JMS quota unlimited on jms;
```

Creating GridLink Data Sources for TLOGs and JMS Stores

Before you can configure database-based persistent stores for JMS and TLOGs, you must create two data sources: one for the TLOGs persistent store and one for the JMS persistent store.

For an enterprise deployment, you should use GridLink data sources for your TLOGs and JMS stores. To create a GridLink data source:

1. Sign in to the Oracle WebLogic Server Administration Console.
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:
 - Enter a logical name for the data source in the **Name** field.
For the TLOGs store, enter `TLOG`; for the JMS store, enter `JMS`.
 - Enter a name for **JNDI**.
For the TLOGs store, enter `jdbc/t logs`; for the JMS store, enter `jdbc/jms`.
 - For the Database Driver, select **Oracle's Driver (Thin) for GridLink Connections Versions: Any**.
 - Click **Next**.
5. In the Transaction Options page, clear the **Supports Global Transactions** check box, and then click **Next**.

☐ Supports Global Transactions

6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.

7. Enter the following connection properties:

- **Service Name:** Enter the service name of the database with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example:

wccedg.example.com

- **Host Name and Port:** Enter the SCAN address and port for the RAC database, separated by a colon. For example:

db-scan.example.com:1521

Click **Add** to add the host name and port to the list box below the field.

Figure 18-1 Adding Host Name and Port Details for the RAC Database

Enter host and port of each listener separated by colon and click the add button. In the case of a RAC DB listener, specify the SCAN address.

Host and Port:

Add

db-scan.example.com:1521

Remove

You can identify the SCAN address by querying the appropriate parameter in the database using the TCP Protocol:

```
SQL>show parameter remote_listener;
```

NAME	TYPE	VALUE
remote_listener	string	db-scan.example.com

 Note:

For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener, for example:

dbhost1-vip.example.com (port 1521)

and

dbhost2-vip.example.com (1521)

- **Database User Name:** Enter the following:
For the TLOGs store, enter TLOGS; for the JMS persistent store, enter JMS.
- **Password:** Enter the password that you used when you created the user in the database.

- **Confirm Password:** Enter the password again and click **Next**.
8. On the Test GridLink Database Connection page, review the connection parameters and click **Test All Listeners**.
- Here is an example of a successful connection notification:
- ```
Connection test
for jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=db-scan.example.com)
(PORT=1521))))(CONNECT_DATA=(SERVICE_NAME=wccedg.example.com))) succeeded.
```
- Click **Next**.
9. In the ONS Client Configuration page, do the following:
- Select **FAN Enabled** to subscribe to and process Oracle FAN events.
  - Enter the SCAN address: ONS remote port for the RAC database and the ONS remote port as reported by the database (see the following example) and click **Add**:
- ```
[orcl@db-scan1 ~]$ srvctl config nodeapps -s
```
- ONS exists: Local port 6100, remote port 6200, EM port 2016
- Click **Next**.



Note:

For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

```
custdbhost1.example.com (port 6200)
```

and

```
custdbhost2.example.com (6200)
```

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.
- Here is an example of a successful connection notification:
- ```
Connection test for db-scan.example.com:6200 succeeded.
```
- Click **Next**.
11. In the Select Targets page, select the cluster that is using the persistent store, and then select **All Servers in the cluster**.
12. Click **Finish**.
13. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.
14. Repeat step 4 through step 13 to create the GridLink Data Source for JMS File Stores.

## Assigning the TLOGs JDBC Store to the Managed Servers

After you create the tablespace and user in the database, and you have created the datasource, you can then assign the TLOGs persistence store to each of the required Managed Servers.

1. Login in to the Oracle WebLogic Server Administration Console.
2. In the **Change Center**, click **Lock and Edit**.
3. In the Domain Structure tree, expand **Environment**, then **Servers**.
4. Click the name of the Managed Server you want to use the TLOGs store.
5. Select the **Configuration > Services** tab.
6. Under **Transaction Log Store**, select **JDBC** from the **Type** menu.
7. From the **Data Source** menu, select the data source you created for the TLOGs persistence store.
8. In the **Prefix Name** field, specify a prefix name to form a unique JDBC TLOG store name for each configured JDBC TLOG store
9. Click **Save**.
10. Repeat steps 3 to 7 for each of the additional Managed Servers in the cluster.
11. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

## Creating a JDBC JMS Store

After you create the JMS persistent store user and table space in the database, and after you create the data source for the JMS persistent store, you can then use the Administration Console to create the store.

1. Log in to the Oracle WebLogic Server Administration Console.
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Persistent Store**.
4. Click **New**, and then click **JDBC Store**.
5. Enter a persistent store name that easily relates it to the pertaining JMS servers that will be using it.
6. Specify a unique prefix qualifying the installation and cluster and associate it with the data source you created for the JMS persistent store.
7. Target the store to the entity that will host the JTA services.
8. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.



## Assigning the JMS JDBC store to the JMS Servers

After you create the JMS tablespace and user in the database, create the JMS datasource, and create the JDBC store, then you can assign the JMS persistence store to each of the required JMS Servers.

To assign the JMS persistence store to the JMS servers:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the **Change Center**, click **Lock and Edit**.
3. In the Domain Structure tree, expand **Services**, then **Messaging**, and then **JMS Servers**.
4. Click the name of the JMS Server that you want to use the persistent store.
5. From the **Persistent Store** menu, select the JMS persistent store you created earlier.
6. Click **Save**.
7. Repeat steps 3 to 6 for each of the additional JMS Servers in the cluster.
8. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

## Creating the Required Tables for the JMS JDBC Store

The final step in using a JDBC persistent store for JMS is to create the required JDBC store tables. Perform this task before you restart the Managed Servers in the domain.

1. Review the information in [Performance Considerations for TLOGs and JMS Persistent Stores](#), and decide which table features are appropriate for your environment.

There are three Oracle DB schema definitions provided in this release and were extracted for review in the previous step. The basic definition includes the RAW data type without any partition for indexes. The second uses the blob data type, and the third uses the blob data type and secure files.

2. Create a domain-specific well-named folder structure for the custom DDL file on shared storage. The `ORACLE_RUNTIME` shared volume is recommended so it is available to all servers.

Example:

```
mkdir -p ORACLE_RUNTIME/domain_name/ddl
```

3. Create a `jms_custom.ddl` file in new shared ddl folder based on your requirements analysis.

For example, to implement an optimized schema definition that uses both secure files and hash partitioning, create the `jms_custom.ddl` file with the following content:

```
CREATE TABLE $TABLE (
 id int not null,
 type int not null,
 handle int not null,
```

```
record blob not null,
PRIMARY KEY (ID) USING INDEX GLOBAL PARTITION BY HASH (ID)
PARTITIONS 8)
LOB (RECORD) STORE AS SECUREFILE (ENABLE STORAGE IN ROW);
```

This example can be compared to the default schema definition for JMS stores, where the RAW data type is used without any partitions for indexes.

Note that the number of partitions should be a power of two. This ensures that each partition is of similar size. The recommended number of partitions varies depending on the expected table or index growth. You should have your database administrator (DBA) analyze the growth of the tables over time and adjust the tables accordingly. See Partitioning Concepts in *Database VLDB and Partitioning Guide*.

4. Use the Administration Console to edit the existing JDBC Store you created earlier; create the table that is used for the JMS data:
  - a. Login in to the Oracle WebLogic Server Administration Console.
  - b. In the **Change Center**, click **Lock and Edit**.
  - c. In the Domain Structure tree, expand **Services**, then **Persistent Stores**.
  - d. Click the persistent store you created earlier.
  - e. Under the **Advanced** options, enter `ORACLE_RUNTIME/domain_name/ddl/jms_custom.ddl` in the **Create Table from DDL File** field.
  - f. Click **Save**.
  - g. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.
5. Restart the Managed Servers.

## Using File Persistent Stores for TLOGs and JMS in an Enterprise Deployment

This section explains the procedures to configure TLOGs and JMS File persistent stores in a shared folder.

- [Configuring TLOGs File Persistent Store in a Shared Folder](#)
- [Configuring JMS File Persistent Store in a Shared Folder](#)

### Configuring TLOGs File Persistent Store in a Shared Folder

Oracle WebLogic Server uses the transaction logs to recover from system crashes or network failures.

- [Configuring TLOGs File Persistent Store in a Shared Folder with a Static Cluster](#)
- [Configuring TLOGs File Persistent Store in a Shared Folder with a Dynamic Cluster](#)
- [Validating the Location and Creation of the Transaction Logs](#)

## Configuring TLOGs File Persistent Store in a Shared Folder with a Static Cluster

To set the location for the default persistence stores for each managed server in a static cluster, complete the following steps:

1. Log into the Oracle WebLogic Server Administration console:

`ADMINVHN:7001/console`



### Note:

If you have already configured web tier, use `http://admin.example.com/console`.

2. In the Change Center section, click **Lock & Edit**.
3. For each of the Managed Servers in the cluster:
  - a. In the Domain Structure window, expand the **Environment** node, and then click the **Servers** node.  
The Summary of Servers page appears.
  - b. Click the name of the server (represented as a hyperlink) in the **Name** column of the table.  
The settings page for the selected server appears and defaults to the Configuration tab.
  - c. On the **Configuration** tab, click the **Services** tab.
  - d. In the Default Store section of the page, enter the path to the folder where the default persistent stores stores its data files.  
For the enterprise deployment, use the `ORACLE_RUNTIME` directory location. This subdirectory serves as the central, shared location for transaction logs for the cluster. See [File System and Directory Variables Used in This Guide](#).  
For example:  
`ORACLE_RUNTIME/domain_name/cluster_name/tlogs`  
In this example, replace `ORACLE_RUNTIME` with the value of the variable for your environment. Replace `domain_name` with the name you assigned to the domain. Replace `cluster_name` with the name of the cluster you just created.
  - e. Click **Save**.
4. Complete step 3 for all servers in the SOA\_Cluster.
5. Click **Activate Changes**.



### Note:

You validate the location and the creation of the transaction logs later in the configuration procedure.

## Configuring TLOGs File Persistent Store in a Shared Folder with a Dynamic Cluster

To set the location for the default persistence stores for a dynamic cluster, update the server template:

1. Log into the Oracle WebLogic Server Administration Console:

`ADMINVHN:7001/console`

### Note:

If you have already configured web tier, use `http://admin.example.com/console`.

2. In the Change Center section, click **Lock & Edit**.
3. Navigate to the server template for the cluster:
  - a. In the Domain Structure window, expand the **Environment and Clusters** nodes, and then click the **Server Templates** node.

The Summary of Server Templates page appears.
  - b. Click the name of the server template (represented as a hyperlink) in the **Name** column of the table.

The settings page for the selected server template appears and defaults to the **Configuration** tab.
  - c. On the **Configuration** tab, click the **Services** tab.
  - d. In the Default Store section of the page, enter the path to the folder where the default persistent stores stores its data files.

For the enterprise deployment, use the `ORACLE_RUNTIME` directory location. This subdirectory serves as the central, shared location for transaction logs for the cluster. See [File System and Directory Variables Used in This Guide](#).

For example:

```
ORACLE_RUNTIME/domain_name/cluster_name/tlogs
```

In this example, replace `ORACLE_RUNTIME` with the value of the variable for your environment. Replace `domain_name` with the name that you assigned to the domain. Replace `cluster_name` with the name of the cluster you just created.
  - e. Click **Save**.
4. Click **Activate Changes**.

### Note:

You validate the location and the creation of the transaction logs later in the configuration procedure.

## Validating the Location and Creation of the Transaction Logs

After the WLS\_SERVER\_TYPE1 and WLS\_SERVER\_TYPE2 managed Servers are up and running, verify that the transaction log directory and transaction logs are created as expected, based on the steps that you performed in [Configuring TLOGs File Persistent Store in a Shared Folder with a Static Cluster](#) and [Configuring TLOGs File Persistent Store in a Shared Folder with a Dynamic Cluster](#):

`ORACLE_RUNTIME/domain_name/OSB_Cluster/tlogs`

- `_WLS_WLS_SERVER_TYPE1000000.DAT`
- `_WLS_WLS_SERVER_TYPE2000000.DAT`

## Configuring JMS File Persistent Store in a Shared Folder

If you have already configured and extended your domain, the JMS Persistent Files are already configured in a shared location. If you need to change any other persistent store file to the shared folder, perform the following steps:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Navigate to **Domain > Services > Persistent Store** and click the name of the persistent store that you want to move to the shared folder.

The **Configuration: General** tab is displayed.

3. Change the directory to `ORACLE_RUNTIME/domain_name/WCC_cluster/jms`.
4. Click **Save**.
5. Click **Activate Changes**.

# Performing Backups and Recoveries for an Enterprise Deployment

It is recommended that you follow the below mentioned guidelines to make sure that you back up the necessary directories and configuration data for an Oracle WebCenter Content enterprise deployment.

### Note:

Some of the static and runtime artifacts listed in this section are hosted from Network Attached Storage (NAS). If possible, backup and recover these volumes from the NAS filer directly rather than from the application servers.

For general information about backing up and recovering Oracle Fusion Middleware products, see the following sections in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*:

- Backing Up Your Environment
- Recovering Your Environment

Table 18-1 lists the static artifacts to back up in a typical Oracle WebCenter Content enterprise deployment.

**Table 18-1 Static Artifacts to Back Up in the Oracle WebCenter Content Enterprise Deployment**

| Type                                 | Host                                  | Tier             |
|--------------------------------------|---------------------------------------|------------------|
| Database Oracle home                 | DBHOST1 and DBHOST2                   | Data Tier        |
| Oracle Fusion Middleware Oracle home | WEBHOST1 and WEBHOST2                 | Web Tier         |
| Oracle Fusion Middleware Oracle home | WCCHOST1 and WCCHOST2 (or NAS Filer)  | Application Tier |
| Installation-related files           | WEBHOST1, WEHOST2, and shared storage | N/A              |

Table 18-2 lists the runtime artifacts to back up in a typical Oracle WebCenter Content enterprise deployment.

**Table 18-2 Run-Time Artifacts to Back Up in the Oracle WebCenter Content Enterprise Deployment**

| Type                                             | Host                    | Tier             |
|--------------------------------------------------|-------------------------|------------------|
| Administration Server domain home (ASERVER_HOME) | WCCHOST1 (or NAS Filer) | Application Tier |
| Application home (APPLICATION_HOME)              | WCCHOST1 (or NAS Filer) | Application Tier |
| Oracle RAC databases                             | DBHOST1 and DBHOST2     | Data Tier        |
| Scripts and Customizations                       | Per host                | Application Tier |
| Deployment Plan home (DEPLOY_PLAN_HOME)          | WCCHOST1 (or NAS Filer) | Application Tier |
| OHS/OTD Configuration directory                  | WEBHOST1 and WEBHOST2   | Web Tier         |

## Modifying the Upload and Stage Directories to an Absolute Path in an Enterprise Deployment

After you configure the domain and unpack it to the Managed Server domain directories on all the hosts, verify and update the upload and stage directories for Managed Servers in the new clusters. Also, update the upload directory for the AdminServer to have the same absolute path instead of relative, otherwise deployment issues can occur. If you implement dynamic clusters, the configuration of the server template assigned to each newly added cluster should be verified and updated, otherwise, verify and update every statically-defined Managed Server for the newly added clusters.



### Note:

This option is applicable only for static clusters.

This step is necessary to avoid potential issues when you perform remote deployments and for deployments that require the stage mode.

To update the directory paths for the Deployment Stage and Upload locations, complete the following steps:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Navigate to and edit the appropriate objects for your cluster type.
  - a. For Static Clusters, navigate to **Servers** and click the name of the Managed Server you want to edit.
  - b. For Dynamic Clusters, navigate to **Clusters > Server Templates**, and click on the name of the server template to be edited.
5. For each new Managed Server or Server Template to be edited:
  - a. Click the **Configuration** tab, and then click the **Deployment** tab.
  - b. Verify that the **Staging Directory Name** is set to the following:

*MSERVER\_HOME/servers/server\_or\_template\_name/stage*

Replace *MSERVER\_HOME* with the full path for the *MSERVER\_HOME* directory.

If you use static clusters, update with the correct name of the Managed Server that you are editing.

If you use dynamic clusters, leave the template name intact.

For example: */u02/oracle/config/domains/wccedg\_domain/servers/XYZ-server-template/stage*

- c. Update the **Upload Directory Name** to the following value:
- ASERVER\_HOME/servers/AdminServer/upload*
- Replace *ASERVER\_HOME* with the directory path for the *ASERVER\_HOME* directory.
- d. Click **Save**.
    - e. Return to the Summary of Servers or Summary of Server Templates screen as applicable.
  6. Repeat the previous steps for each of the new managed servers or dynamic cluster server templates.
  7. Navigate to and update the Upload Directory Name value for the AdminServer:
    - a. Navigate to **Servers**, and select the AdminServer.
    - b. Click the **Configuration** tab, and then click the **Deployment** Tab.
    - c. Verify that the **Staging Directory Name** is set to the following absolute path:

*ASERVER\_HOME/servers/AdminServer/stage*

- d. Update the **Upload Directory Name** to the following absolute path:

*ASERVER\_HOME/servers/AdminServer/upload*

Replace *ASERVER\_HOME* with the directory path for the *ASERVER\_HOME* directory.

- e. Click **Save**.
8. When you have modified all the appropriate objects, click **Activate Changes**.
9. Restart all Managed Servers for the changes to take effect.



**Note:**

If you continue directly with further domain configurations, a restart to enable the stage and upload directory changes is not strictly necessary at this time.

## Starting and Stopping Servers in Dynamic Clusters

You can start and stop server instances in dynamic clusters by using the same methods you use to start and stop server instances in configured static clusters.

Methods to start and stop server instances in configured clusters:

- WebLogic Server Administration Console
- Fusion Middleware Control
- WLST start and shutdown commands
- Node Manager
- Start scripts

Depending on which startup method you choose and the tasks you have already performed, you may have to follow several other procedures before you can start server instances. See Starting and Stopping Servers section in *Oracle Fusion Middleware Administering Server Startup and Shutdown for Oracle WebLogic Server*.



**Note:**

Before you begin, ensure that WebLogic Server is installed on all hosts where you want to run your server instances. If you want to use Node Manager to start and stop your server instances, then you must also run Node Manager on these hosts.

## Expanding or Reducing Dynamic Clusters

When you create a dynamic cluster, WebLogic Server generates the number of dynamic servers you specify. Before you decide upon the number of server instances, ensure you have the performance capacity to handle the desired number.

The number of dynamic server instances available are based on the configured maximum specified in the server template for a given dynamic cluster. Transient changes in capacity requirements can be easily met by starting or stopping some of the available managed servers within the cluster, keeping in mind that a minimum of two or three are required to maintain high-availability.

If you need additional server capacity on top of the number of server instances you originally specified, you can increase the maximum number of dynamic servers in



the dynamic cluster configuration. To reduce the number of server instances in the dynamic cluster, decrease the value of the maximum number of dynamic servers attribute. Before lowering this value, shut down the server instances you plan to remove.

You can also use the WLST `scaleUp` and `scaleDown` commands to manage your dynamic cluster. To increase the number of dynamic servers in the dynamic cluster, use the `scaleUp` command and enable the `updateConfiguration` argument. WLST will increase the maximum size of the cluster by the specified number of servers and start the server instances.

The `scaleUp` command increases the number of running servers for the specified dynamic cluster. The non-running server instance with the lowest server ID starts first, followed by the next highest non-running server ID, until the specified number of server instances is started.

You can start one, all, or any number of server instances in the dynamic cluster by specifying the desired number with the `numServers` argument in the `scaleUp` command. If all available server instances are already running, the `scaleUp` command increases the size of the cluster to the minimum number of requested server instances before starting the specified number of servers.

To decrease the maximum size of the dynamic cluster, use the `scaleDown` command and enable the `updateConfiguration` argument. WLST will gracefully shut down the specified number of running server instances and remove them from the dynamic cluster. See `scaleUp` and `scaleDown` in *Oracle Fusion Middleware WLST Command Reference for WebLogic Server*. The `scaleDown` command gracefully shuts down the specified number of running servers. The server instance with the highest server ID shuts down first, followed by the next highest ID, until the specified number of server instances is shut down.

 **Note:**

You can only use the WLST `scaleUp` and `scaleDown` commands with dynamic server instances. In a mixed cluster, containing both manually configured and dynamic server instances, the `scaleUp` and `scaleDown` commands ignore the configured servers. You must manually start and stop configured server instances in a mixed cluster.

For example, a cluster contains two running dynamic servers and two non-running configured servers. If you use the `scaleUp` command, WLST adds one additional dynamic server instance to your cluster and starts the dynamic server.

The WLST `scaleUp` and `scaleDown` commands provide ways to manually scale your dynamic cluster. For automatic scaling, you can configure elasticity for your dynamic cluster. Elasticity enables a dynamic cluster to perform scaling and re-provisioning operations automatically in response to demand or on a calendar based schedule. WebLogic Server provides elasticity for dynamic clusters through the Policies and Actions system of the WebLogic Diagnostic Framework (WLDF). See *Configuring Elasticity in Dynamic Clusters for Oracle WebLogic Server*.

# Using Whole Server Migration and Service Migration in an Enterprise Deployment

The Oracle WebLogic Server migration framework supports Whole Server Migration and Service Migration. The following sections explain how these features can be used in an Oracle Fusion Middleware enterprise topology.

- [About Whole Server Migration and Automatic Service Migration in an Enterprise Deployment](#)  
Oracle WebLogic Server provides a migration framework that is an integral part of any highly available environment. The following sections provide more information about how this framework can be used effectively in an enterprise deployment.
- [Creating a GridLink Data Source for Leasing](#)  
Whole Server Migration and Automatic Service Migration require a data source for the leasing table, which is a tablespace created automatically as part of the Oracle WebLogic Server schemas by the Repository Creation Utility (RCU).
- [Configuring Whole Server Migration for an Enterprise Deployment](#)  
After you have prepared your domain for whole server migration or automatic service migration, you can configure Whole Server Migration for specific Managed Servers within a cluster.
- [Configuring Automatic Service Migration in an Enterprise Deployment](#)  
You may need to configure automatic service migration for specific services in an enterprise deployment.

## About Whole Server Migration and Automatic Service Migration in an Enterprise Deployment

Oracle WebLogic Server provides a migration framework that is an integral part of any highly available environment. The following sections provide more information about how this framework can be used effectively in an enterprise deployment.

- [Understanding the Difference between Whole Server and Service Migration](#)
- [Implications of Using Whole Server Migration or Service Migration in an Enterprise Deployment](#)
- [Understanding Which Products and Components Require Whole Server Migration and Service Migration](#)

## Understanding the Difference between Whole Server and Service Migration

The Oracle WebLogic Server migration framework supports two distinct types of automatic migration:

- **Whole Server Migration**, where the Managed Server instance is migrated to a different physical system upon failure.

Whole server migration provides for the automatic restart of a server instance, with all its services, on a different physical machine. When a failure occurs in a server that is part of a cluster which is configured with server migration, the server is restarted on any of the other machines that host members of the cluster.

For this to happen, the servers must use a floating IP as listen address and the required resources (transactions logs and JMS persistent stores) must be available on the candidate machines.

See Whole Server Migration in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

- **Service Migration**, where specific services are moved to a different Managed Server within the cluster.

To understand service migration, it's important to understand *pinned services*.

In a WebLogic Server cluster, most subsystem services are hosted homogeneously on all server instances in the cluster, enabling transparent failover from one server to another. In contrast, pinned services, such as JMS-related services, the JTA Transaction Recovery Service, and user-defined singleton services, are hosted on individual server instances within a cluster—for these services, the WebLogic Server migration framework supports failure recovery with service migration, as opposed to failover.

See Understanding the Service Migration Framework in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

## Implications of Using Whole Server Migration or Service Migration in an Enterprise Deployment

When a server or service is started in another system, the required resources (such as services data and logs) must be available to both the original system and to the failover system; otherwise, the service cannot resume the same operations successfully on the failover system.

For this reason, both whole server and service migration require that all members of the cluster have access to the same transaction and JMS persistent stores (whether the persistent store is file-based or database-based).

This is another reason why shared storage is important in an enterprise deployment. When you properly configure shared storage, you ensure that in the event of a manual failover (Administration Server failover) or an automatic failover (whole server migration or service migration), both the original machine and the failover machine can access the same file store with no change in service.

In the case of an automatic service migration, when a pinned service needs to be resumed, the JMS and JTA logs that it was using before failover need to be accessible.

In addition to shared storage, Whole Server Migration requires the procurement and assignment of a virtual IP address (VIP). When a Managed Server fails over to another machine, the VIP is automatically reassigned to the new machine.

Note that service migration does not require a VIP.

## Understanding Which Products and Components Require Whole Server Migration and Service Migration

Note that the table lists the recommended best practice. It does not preclude you from using Whole Server or Automatic Server Migration for those components that support it.

| Component                 | Whole Server Migration (WSM) | Automatic Service Migration (ASM) |
|---------------------------|------------------------------|-----------------------------------|
| Oracle WebCenter Content  | YES                          | YES (Recommended)                 |
| Oracle SOA Suite          | YES                          | YES (Recommended)                 |
| Oracle Enterprise Capture | YES                          | YES (Recommended)                 |

## Creating a GridLink Data Source for Leasing

Whole Server Migration and Automatic Service Migration require a data source for the leasing table, which is a tablespace created automatically as part of the Oracle WebLogic Server schemas by the Repository Creation Utility (RCU).

### Note:

To accomplish data source consolidation and connection usage reduction, you can reuse the WLSSchemaDataSource as is for database leasing. This datasource is already configured with the FMW1221\_WLS\_RUNTIME schema, where the leasing table is stored.

For an enterprise deployment, you should create a GridLink data source:

1. Log in to the Oracle WebLogic Server Administration Console.
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:
  - Enter a logical name for the data source in the **Name** field. For example, **Leasing**.
  - Enter a name for **JNDI**. For example, **jdbc/leasing**.
  - For the Database Driver, select **Oracle's Driver (Thin) for GridLink Connections Versions: Any**.
  - Click **Next**.
5. In the Transaction Options page, clear the **Supports Global Transactions** check box, and then click **Next**.

6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.

7. Enter the following connection properties:

- **Service Name:** Enter the service name of the database with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example:

wccedg.example.com

- **Host Name and Port:** Enter the SCAN address and port for the RAC database, separated by a colon. For example:

db-scan.example.com:1521

Click **Add** to add the host name and port to the list box below the field.

**Figure 19-1 Specifying SCAN Address for the RAC Database**

Enter host and port of each listener separated by colon and click the add button. In the case of a RAC DB listener, specify the SCAN address.

**Host and Port:**

Add

db-scan.example.com:1521

Remove

You can identify the SCAN address by querying the appropriate parameter in the database using the TCP Protocol:

```
SQL>show parameter remote_listener;
```

| NAME                                       | TYPE   | VALUE               |
|--------------------------------------------|--------|---------------------|
| <hr style="border-top: 1px dashed #000;"/> |        |                     |
| remote_listener                            | string | db-scan.example.com |

**Note:**

For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener, for example:

dbhost1-vip.mycompany.com (port 1521)

and

dbhost2-vip.mycompany.com (1521)

For Oracle Database 10g, use multi data sources to connect to an Oracle RAC database. For information about configuring multi data sources, see [Using Multi Data Sources with Oracle RAC](#).

- **Database User Name:** Enter the following:

FMW1221\_WLS\_RUNTIME

In this example, FMW1221 is the prefix you used when you created the schemas as you prepared to configure the initial enterprise manager domain.

Note that in previous versions of Oracle Fusion Middleware, you had to manually create a user and tablespace for the migration leasing table. In Fusion Middleware 12c (12.2.1), the leasing table is created automatically when you create the WLS schemas with the Repository Creation Utility (RCU).

- **Password:** Enter the password you used when you created the WLS schema in RCU.
  - **Confirm Password:** Enter the password again and click **Next**.
8. On the Test GridLink Database Connection page, review the connection parameters and click **Test All Listeners**.

Here is an example of a successful connection notification:

```
Connection test
for jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=db-scan.example.com)
(PORT=1521))))(CONNECT_DATA=(SERVICE_NAME=wccedg.example.com))) succeeded.
```

Click **Next**.

9. In the ONS Client Configuration page, do the following:
- Select **FAN Enabled** to subscribe to and process Oracle FAN events.
  - Enter the SCAN address in the **ONS Host and Port** field, and then click **Add**.

This value should be the ONS host and ONS remote port for the RAC database. To find the ONS remote port for the database, you can use the following command on the database host:

```
[orcl@db-scan1 ~]$ srvctl config nodeapps -s
```

```
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

- Click **Next**.



#### Note:

For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

```
custdbhost1.example.com (port 6200)
```

and

```
custdbhost2.example.com (6200)
```

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.

Here is an example of a successful connection notification:

```
Connection test for db-scan.example.com:6200 succeeded.
```

Click **Next**.

11. In the Select Targets page, select the cluster that you are configuring for Whole Server Migration or Automatic Service Migration, and then select **All Servers in the cluster**.
12. Click **Finish**.
13. Click **Activate Changes**.

## Configuring Whole Server Migration for an Enterprise Deployment

After you have prepared your domain for whole server migration or automatic service migration, you can configure Whole Server Migration for specific Managed Servers within a cluster.



### Note:

As mentioned earlier, for migration to work, servers must use a virtual hostname that matches a floating IP, as the listen address. You can specify the listen address directly in the Configuration Wizard or update it in the administration console.

- [Editing the Node Manager's Properties File to Enable Whole Server Migration](#)
- [Setting Environment and Superuser Privileges for the wlsifconfig.sh Script](#)
- [Configuring Server Migration Targets](#)
- [Testing Whole Server Migration](#)

## Editing the Node Manager's Properties File to Enable Whole Server Migration

Use the section to edit the Node Manager properties file on the two nodes where the servers are running.

1. Locate and open the following file with a text editor:

```
MSERVER_HOME/nodemanager/nodemanager.properties
```

2. If not done already, set the StartScriptEnabled property in the nodemanager.properties file to true.

This is required to enable Node Manager to start the managed servers.

3. Add the following properties to the nodemanager.properties file to enable server migration to work properly:

- Interface

```
Interface=eth0
```

This property specifies the interface name for the floating IP (eth0, for example).

 **Note:**

Do not specify the sub interface, such as `eth0:1` or `eth0:2`. This interface is to be used without the `:0`, or `:1`.

The Node Manager's scripts traverse the different `:X` enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, or, `eth2`, `eth3`, `ethn`, depending on the number of interfaces configured.

- `NetMask`

`NetMask=255.255.255.0`

This property specifies the net mask for the interface for the floating IP.

- `UseMACBroadcast`

`UseMACBroadcast=true`

This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the `-b` flag in the `arping` command.

4. Restart the Node Manager.
5. Verify in the output of Node Manager (the shell where the Node Manager is started) that these properties are in use. Otherwise, problems may occur during migration. The output should be similar to the following:

```
...
SecureListener=true
LogCount=1
eth0=*,NetMask=255.255.255.0
...
```

## Setting Environment and Superuser Privileges for the `wlsifconfig.sh` Script

Use this section to set the environment and superuser privileges for the `wlsifconfig.sh` script, which is used to transfer IP addresses from one machine to another during migration. It must be able to run `ifconfig`, which is generally only available to superusers.

For more information about the `wlsifconfig.sh` script, see *Configuring Automatic Whole Server Migration in Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

Refer to the following sections for instructions on preparing your system to run the `wlsifconfig.sh` script.

- [Setting the PATH Environment Variable for the `wlsifconfig.sh` Script](#)
- [Granting Privileges to the `wlsifconfig.sh` Script](#)



## Setting the PATH Environment Variable for the wlsifconfig.sh Script

Ensure that the commands listed in the following table are included in the PATH environment variable for each host computers.

| File                | Directory Location                |
|---------------------|-----------------------------------|
| wlsifconfig.sh      | MSERVER_HOME/bin/server_migration |
| wlscontrol.sh       | WL_HOME/common/bin                |
| nodemanager.domains | MSERVER_HOME/nodemanager          |

## Granting Privileges to the wlsifconfig.sh Script

Grant *sudo* privilege to the operating system user (for example, oracle) with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries.



### Note:

For security reasons, *sudo* should be restricted to the subset of commands required to run the wlsifconfig.sh script.

Ask the system administrator for the *sudo* and system rights as appropriate to perform this required configuration task.

The following is an example of an entry inside */etc/sudoers* granting *sudo* execution privilege for oracle to run ifconfig and arping:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

## Configuring Server Migration Targets

To configure migration in a cluster:

1. Sign in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock & Edit**.
6. Select **Database** as Migration Basis. From the drop-down list, select **Leasing** as Data Source For Automatic Migration.

7. Under **Candidate Machines For Migratable Server**, in the Available filed, select the Managed Servers in the cluster and click the right arrow to move them to **Chosen**.
8. Click **Save**.
9. Set the Candidate Machines for Server Migration. You must perform this task for all of the managed servers as follows:
  - a. In Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
  - b. Select the server for which you want to configure migration.
  - c. Click the **Migration** tab.
  - d. Select **Automatic Server Migration Enabled** and click **Save**.

This enables the Node Manager to start a failed server on the target node automatically.

For information on targeting applications and resources, see [Using Multi Data Sources with Oracle RAC](#).
  - e. In the **Available** field, located in the Migration Configuration section, select the machines to which to allow migration and click the right arrow.

In this step, you are identifying the host to which the Managed Server should failover if the current host is unavailable. For example, for the Managed Server on the HOST1, select HOST2; for the Managed Server on HOST2, select HOST1.
10. Click **Activate Changes**.
11. Restart the Administration Server and the servers for which server migration has been configured.

**Tip:**

Click **Customize this table** in the Summary of Servers page, move Current Machine from the Available Window to the Chosen window to view the machine on which the server is running. This is different from the configuration if the server is migrated automatically.

## Testing Whole Server Migration

Perform the steps in this section to verify that automatic whole server migration is working properly.

### To test from Node 1:

1. Stop the managed server process.

```
kill -9 pid
```

*pid* specifies the process ID of the managed server. You can identify the *pid* in the node by running this command:

```
ps -ef | grep WLS_WCC1
```

2. Watch the Node Manager console (the terminal window where you performed the kill command): you should see a message indicating that the managed server's floating IP has been disabled.
3. Wait for the Node Manager to try a second restart of the Managed Server. Node Manager waits for a period of 30 seconds before trying this restart.
4. After node manager restarts the server and before it reaches *Running* state, kill the associated process again.

Node Manager should log a message indicating that the server will not be restarted again locally.

 **Note:**

The number of restarts required is determined by the `RestartMax` parameter in the following configuration file:

`MSERVER_HOME/servers/WLS_WCC1/data/nodemanager/startup.properties`

The default value is `RestartMax=2`.

**To test from Node 2:**

1. Watch the local Node Manager console. After 30 seconds since the last try to restart the managed server on Node 1, Node Manager on Node 2 should prompt that the floating IP for the managed server is being brought up and that the server is being restarted in this node.
2. Access a product URL by using the same IP address. If the URL is successful, then the migration was successful.

**Verification From the Administration Console**

You can also verify migration using the Oracle WebLogic Server Administration Console:

1. Log in to the Administration Console.
2. Click **Domain** on the left console.
3. Click the **Monitoring** tab and then the **Migration** subtab.

The Migration Status table provides information on the status of the migration.

 **Note:**

After a server is migrated, to fail it back to its original machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager starts the managed server on the machine to which it was originally assigned.

# Configuring Automatic Service Migration in an Enterprise Deployment

You may need to configure automatic service migration for specific services in an enterprise deployment.

- [Setting the Leasing Mechanism and Data Source for an Enterprise Deployment Cluster](#)
- [Changing the Migration Settings for the Managed Servers in the Cluster](#)
- [About Selecting a Service Migration Policy](#)
- [Setting the Service Migration Policy for Each Managed Server in the Cluster](#)
- [Validating Automatic Service Migration in Static Clusters](#)
- [Failing Back Services After Automatic Service Migration](#)

## Setting the Leasing Mechanism and Data Source for an Enterprise Deployment Cluster

Before you can configure automatic service migration, you must verify the leasing mechanism and data source that is used by the automatic service migration feature. You must configure the leasing mechanism and datasource for both static and dynamic clusters.

### Note:

To accomplish data source consolidation and connection usage reduction, you can reuse the WLSSchemaDatasource datasource as is for database leasing. This datasource is already configured with the FMW1221\_WLS\_RUNTIME schema, where the leasing table is stored.

The following procedure assumes that you have configured the Leasing data source either by reusing the WLSSchemaDatasource or a custom datasource that you created as described in [Creating a GridLink Data Source for Leasing](#).

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. In the Domain Structure window, expand **Environment** and select **Clusters**.  
The Summary of Clusters page appears.
4. In the **Name** column of the table, click the cluster for which you want to configure migration.
5. Click the **Migration** tab.
6. Verify that **Database** is selected in the **Migration Basis** drop-down menu.

7. From the **Data Source for Automatic Migration** drop-down menu, select the Leasing data source that you created in [Creating a GridLink Data Source for Leasing](#). Select the WLSSchemaDataSource for data source consolidation.
8. Click **Save**.
9. Activate changes.
10. Restart the managed servers for the changes to be effective. If you are configuring other aspects of ASM in the same configuration change session, you can use a final unique restart to reduce downtime.

## Changing the Migration Settings for the Managed Servers in the Cluster

After you set the leasing mechanism and data source for the cluster, you can then enable automatic JTA migration for the Managed Servers that you want to configure for service migration. Note that this topic applies only if you are deploying JTA services as part of your enterprise deployment.

For example, this task is not required for Oracle WebCenter Content enterprise deployments.

To change the migration settings for the Managed Servers in each cluster:

1. If you haven't already, log in to the Administration Console, and click **Lock & Edit**.
2. In the Domain Structure pane, expand the **Environment** node and then click **Servers**.  
The Summary of Servers page appears.
3. Click the name of the server you want to modify in **Name** column of the table.  
The settings page for the selected server appears and defaults to the Configuration tab.
4. Click the **Migration** tab.
5. From the **JTA Migration Policy** drop-down menu, select **Failure Recovery**.
6. In the **JTA Candidate Servers** section of the page, select the Managed Servers in the **Available** list box, and then click the move button to move them into the **Chosen** list box.
7. In the **JMS Service Candidate Servers** section of the page, select the Managed Servers in the **Available** list box, and then click the move button to move them into the **Chosen** list box.
8. Click **Save**.
9. Restart the managed servers and the Administration Server for the changes to be effective. If you are configuring other aspects of ASM in the same configuration change session, you can use a final unique restart to reduce downtime.

## About Selecting a Service Migration Policy

When you configure Automatic Service Migration, you select a Service Migration Policy for each cluster. This topic provides guidelines and considerations when selecting the Service Migration Policy.

For example, products or components running singletons or using Path services can benefit from the **Auto-Migrate Exactly-Once** policy. With this policy, if at least one Managed Server in the candidate server list is running, the services hosted by this migratable target are active somewhere in the cluster if servers fail or are administratively shut down (either gracefully or forcibly). This can cause multiple homogenous services to end up in one server on startup.

When you use this policy, you should monitor the cluster startup to identify what servers are running on each server. You can then perform a manual fallback, if necessary, to place the system in a balanced configuration.

Other Fusion Middleware components are better suited for the **Auto-Migrate Failure-Recovery Services** policy.

Based on these guidelines, you should use **Auto-Migration Failure-Recovery Services** for the clusters in an Oracle WebCenter Content enterprise deployment.

See Policies for Manual and Automatic Service Migration in *Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

## Setting the Service Migration Policy for Each Managed Server in the Cluster

After you modify the migration settings for each server in the cluster, you can then identify the services and set the migration policy for each Managed Server in the cluster, using the WebLogic Administration Console:

1. If you have not already, log in to the Administration Console, and click **Lock & Edit**.
2. In the Domain Structure pane, expand **Environment**, then expand **Clusters**, then select **Migratable Targets**.
3. Click the name of the first Managed Server in the cluster.
4. Click the **Migration** tab.
5. From the **Service Migration Policy** drop-down menu, select the appropriate policy for the cluster.

See [About Selecting a Service Migration Policy](#).

6. In the Constrained Candidate Servers section of the page, select both Managed Servers in the **Available** list box and move them to the **Chosen** list box.
7. Click **Save**.
8. Repeat steps 2 through 7 for each of the additional Managed Servers in the cluster.
9. In the Domain Structure pane, select **Environment** > **Clusters** > *cluster\_name* > **Configuration** tab > **General** tab > **Advanced**.
10. In the Service Activation Request Response Timeout field, type 0.
11. Activate the changes.
12. Restart the managed servers for the changes to be effective. If you are configuring other aspects of ASM in the same configuration change session, you can use a final unique restart to reduce downtime.

## Validating Automatic Service Migration in Static Clusters

After you configure automatic service migration for your cluster and Managed Servers, validate the configuration, as follows:

1. If you have not already done so, log in to the Administration Console.
2. In the Domain Structure pane, expand **Environment**, and then expand **Clusters**.
3. Click **Migratable Targets**.
4. Click the **Control** tab.

The console displays a list of migratable targets and their current hosting server.

5. In the Migratable Targets table, select a row for the one of the migratable targets.
6. Note the value in the **Current Hosting Server** column.
7. Use the operating system command line to stop the first Managed Server.

Use the following command to end the Managed Server Process and simulate a crash scenario:

```
kill -9 pid
```

In this example, replace *pid* with the process ID (PID) of the Managed Server. You can identify the PID by running the following UNIX command:

```
ps -ef | grep managed_server_name
```

### Note:

After you kill the process, the Managed Server might be configured to start automatically. In this case, you must kill the second process using the `kill -9` command again.

8. Watch the terminal window (or console) where the Node Manager is running.  
You should see a message indicating that the selected Managed Server has failed. The message is similar to the following:  

```
<INFO> <domain_name> <server_name>
<The server 'server_name' with process id 4668 is no longer alive; waiting
for the process to die.>
<INFO> <domain_name> <server_name>
<Server failed during startup. It may be retried according to the auto
restart configuration.>
<INFO> <domain_name> <server_name>
<Server failed but will not be restarted because the maximum number of
restart attempts has been exceeded.>
```
9. Return to the Oracle WebLogic Server Administration Console and refresh the table of migratable targets; verify that the migratable targets are transferred to the remaining, running Managed Server in the cluster:
  - Verify that the Current Hosting Server for the process you killed is now updated to show that it has been migrated to a different host.
  - Verify that the value in the **Status of Last Migration** column for the process is *Succeeded*.

10. Open and review the log files for the Managed Servers that are now hosting the services; look for any JTA or JMS errors.

**Note:**

For JMS tests, it is a good practice to get message counts from destinations and make sure that there are no stuck messages in any of the migratable targets:

For example, for uniform distributed destinations (UDDs):

- a. Access the JMS Subdeployment module in the Administration Console:  
  
In the Domain Structure pane, select **Services**, then **Messaging**, and then **JMS Modules**.
- b. Click the JMS Module.
- c. In the Summary of Resources table, click **Destinations**, and then click the **Monitoring** tab.
- d. Review the **Messages Total** and **Messages Pending** values. Click **Customize table** to add these columns to the table, if these values do not appear in the table.

## Failing Back Services After Automatic Service Migration

When Automatic Service Migration occurs, Oracle WebLogic Server does not support failing back services to their original server when a server is back online and rejoins the cluster.

As a result, after the Automatic Service Migration migrates specific JMS services to a backup server during a fail-over, it does not migrate the services back to the original server after the original server is back online. Instead, you must migrate the services back to the original server manually.

To fail back a service to its original server, follow these steps:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the Domain Structure tree, expand **Environment**, expand **Clusters**, and then select **Migratable Targets**.
3. To migrate one or more migratable targets at once, on the Summary of Migratable Targets page:
  - a. Click the **Control** tab.
  - b. Use the check boxes to select one or more migratable targets to migrate.
  - c. Click **Migrate**.
  - d. Use the **New hosting server** drop-down to select the original Managed Server.
  - e. Click **OK**.



A request is submitted to migrate the JMS-related service. In the Migratable Targets table, the Status of Last Migration column indicates whether the requested migration has succeeded or failed.

- f. Release the edit lock after the migration is successful.

# Configuring Single Sign-On for an Enterprise Deployment

You need to configure the Oracle HTTP Server WebGate in order to enable single sign-on with Oracle Access Manager.

- [About Oracle HTTP Server Webgate](#)  
Oracle HTTP Server WebGate is a web server plug-in that intercepts HTTP requests and forwards them to an existing Oracle Access Manager instance for authentication and authorization.
- [General Prerequisites for Configuring Oracle HTTP Server WebGate](#)  
Before you can configure Oracle HTTP Server WebGate, you must have installed and configured a certified version of Oracle Access Manager.
- [Enterprise Deployment Prerequisites for Configuring OHS 12c Webgate](#)  
When you are configuring Oracle HTTP Server Webgate to enable single sign-on for an enterprise deployment, consider the prerequisites mentioned in this section.
- [Configuring Oracle HTTP Server 12c WebGate for an Enterprise Deployment](#)  
You need to perform the following steps in order to configure Oracle HTTP Server 12c WebGate for Oracle Access Manager on both WEBHOST1 and WEBHOST2.
- [Registering the Oracle HTTP Server WebGate with Oracle Access Manager](#)  
You can register the WebGate agent with Oracle Access Manager using the Oracle Access Manager Administration console.
- [Setting Up the WebLogic Server Authentication Providers](#)  
To set up the WebLogic Server authentication providers, back up the configuration files, set up the Oracle Access Manager Identity Assertion Provider and set the order of providers.
- [Configuring Oracle ADF and OPSS Security with Oracle Access Manager](#)  
Some Oracle Fusion Middleware management consoles use Oracle Application Development Framework (Oracle ADF) security, which can integrate with Oracle Access Manager Single Sign On (SSO). These applications can take advantage of Oracle Platform Security Services (OPSS) SSO for user authentication, but you must first configure the domain-level `jps-config.xml` file to enable these capabilities.

## About Oracle HTTP Server Webgate

Oracle HTTP Server WebGate is a web server plug-in that intercepts HTTP requests and forwards them to an existing Oracle Access Manager instance for authentication and authorization.

For Oracle Fusion Middleware 12c, the Oracle WebGate software is installed as part of the Oracle HTTP Server 12c software installation. See *Registering and Managing OAM 11g Agents in Administrator's Guide for Oracle Access Management*.

## General Prerequisites for Configuring Oracle HTTP Server WebGate

Before you can configure Oracle HTTP Server WebGate, you must have installed and configured a certified version of Oracle Access Manager.

For the most up-to-date information, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page.

For WebGate certification matrix, click and open <http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/oam-webgates-2147084.html>, then click the *Certification Matrix for 12c Access Management WebGates* link to download the certification matrix spreadsheet.



### Note:

For production environments, it is highly recommended that you install Oracle Access Manager in its own environment and not on the machines that are hosting the enterprise deployment.

For more information about Oracle Access Manager, see the latest Oracle Identity and Access Management documentation, which you can find in the **Middleware** documentation on the [Oracle Help Center](#).

## Enterprise Deployment Prerequisites for Configuring OHS 12c Webgate

When you are configuring Oracle HTTP Server Webgate to enable single sign-on for an enterprise deployment, consider the prerequisites mentioned in this section.

- Oracle recommends that you deploy Oracle Access Manager as part of a highly available, secure, production environment. For more information about deploying Oracle Access Manager in an enterprise environment, see the Enterprise Deployment Guide for your version of Oracle Identity and Access Management.
- To enable single sign-on for the WebLogic Server Administration Console and the Oracle Enterprise Manager Fusion Middleware Control, you must add a central LDAP-provisioned administration user to the directory service that Oracle Access Manager is using (for example, Oracle Internet Directory or Oracle Unified Directory). For more information about the required user and groups to add to the LDAP directory, follow the instructions in [Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group](#).



### Note:

It is recommended that you use the WebGate version that is certified with your Oracle Access Manager deployment.

## Configuring Oracle HTTP Server 12c WebGate for an Enterprise Deployment

You need to perform the following steps in order to configure Oracle HTTP Server 12c WebGate for Oracle Access Manager on both WEBHOST1 and WEBHOST2.

In the following procedure, replace the directory variables, such as `WEB_ORACLE_HOME` and `WEB_CONFIG_DIR`, with the values, as defined in [File System and Directory Variables Used in This Guide](#).

1. Perform a complete backup of the web tier domain.
2. Change directory to the following location in the Oracle HTTP Server Oracle home:

```
cd WEB_ORACLE_HOME/webgate/ohs/tools/deployWebGate/
```

3. Run the following command to create the WebGate Instance directory and enable WebGate logging on OHS Instance:

```
./deployWebGateInstance.sh -w WEB_CONFIG_DIR -oh WEB_ORACLE_HOME
```

4. Verify that a webgate directory and subdirectories was created by the `deployWebGateInstance` command:

```
ls -lat WEB_CONFIG_DIR/webgate/
total 16
drwxr-x---+ 8 orcl oinstall 20 Oct 2 07:14 ..
drwxr-xr-x+ 4 orcl oinstall 4 Oct 2 07:14 .
drwxr-xr-x+ 3 orcl oinstall 3 Oct 2 07:14 tools
drwxr-xr-x+ 3 orcl oinstall 4 Oct 2 07:14 config
```

5. Run the following command to ensure that the `LD_LIBRARY_PATH` environment variable contains `WEB_ORACLE_HOME/lib` directory path:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:WEB_ORACLE_HOME/lib
```

6. Change directory to the following directory

```
WEB_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools
```

7. Run the following command from the `InstallTools` directory.

```
./EditHttpConf -w WEB_CONFIG_DIR -oh WEB_ORACLE_HOME -o
output_file_name
```



### Note:

The `-oh WEB_ORACLE_HOME` and `-o output_file_name` parameters are optional.

This command:

- Copies the `apache_webgate.template` file from the Oracle HTTP Server Oracle home to a new `webgate.conf` file in the Oracle HTTP Server configuration directory.
- Updates the `httpd.conf` file to add one line, so it includes the `webgate.conf`.
- Generates a WebGate configuration file. The default name of the file is `webgate.conf`, but you can use a custom name by using the `-o output_file_name` argument to the command.

## Registering the Oracle HTTP Server WebGate with Oracle Access Manager

You can register the WebGate agent with Oracle Access Manager using the Oracle Access Manager Administration console.

See Registering an OAM Agent Using the Console in *Administrator's Guide for Oracle Access Management*.

- [Locating and Preparing the RREG Tool](#)
- [About RREG In-Band and Out-of-Band Mode](#)
- [Updating the Standard Properties in the OAM11gRequest.xml File](#)
- [Updating the Protected, Public, and Excluded Resources for an Enterprise Deployment](#)
- [Running the RREG Tool](#)
- [Files and Artifacts Generated by RREG](#)
- [Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location](#)
- [Insert OHS SimpleCA Certificate into the Wallet Artifact](#)
- [Enable MD5 Certificate Signatures for the Oracle HTTP Server Instances](#)
- [Restarting the Oracle HTTP Server Instance](#)

### Locating and Preparing the RREG Tool

To set up the RREG tool, complete the following steps:

1. Sign in to one of the Oracle Access Manager hosts in the Application tier.
2. Change to the following directory in the Oracle Access Manager Oracle home:  
`OAM_ORACLE_HOME/oam/server/rreg/client`

 **Note:**

The location is required only for the out-of-band mode.

In this example, `OAM_ORACLE_HOME` refers to the Oracle home on the system where the Oracle Access Manager software was installed.

**Note:**

If the Oracle Enterprise Deployment Guide for IDM was used, `OAM_ORACLE_HOME` may be `/u01/oracle/products/access/iam`.

**Note:**

If you do not have privileges or access to the Oracle Access Manager server, then you can use out-of-band mode to generate the required files and register the WebGate with Oracle Access Manager. See [About RREG In-Band and Out-of-Band Mode](#).

3. Decompress the `RREG.tar.gz` file to the required directory.
4. From the unzipped directory, open the `oamreg.sh` file and set the following environment variables in the file, as follows:
  - Set `OAM_REG_HOME` to the absolute path to the directory in which you extracted the contents of RREG archive.

Set `JAVA_HOME` to the absolute path of the directory in which a supported JDK is installed on your machine.

## About RREG In-Band and Out-of-Band Mode

You can run the RREG Tool in one of the two modes: in-band and out-of-band.

Use **in-band** mode when you have the privileges to access the Oracle Access Manager server and run the RREG tool yourself from the Oracle Access Manager Oracle home. You can then copy the generated artifacts and files to the web server configuration directory after you run the RREG Tool.

Use **out-of-band** mode if you do *not* have privileges or access to the Oracle Access Manager server. For example, in some organizations, only the Oracle Access Manager server administrators have privileges to access the server directories and perform administration tasks on the server. In out-of-band mode, the process can work as follows:

1. The Oracle Access Manager server administrator provides you with a copy of the RREG archive file (`RREG.tar.gz`).

The server administrator can find it in the location described in [Locating and Preparing the RREG Tool](#).

2. Untar the `RREG.tar.gz` file that was provided to you by the server administrator.

For example:

```
gunzip RREG.tar.gz
tar -xvf RREG.tar
```

After you unpack the RREG archive, you can find the tool for registering the agent in the following location:

```
RREG_HOME/bin/oamreg.sh
```

In this example, *RREG\_Home* is the directory in which you extracted the contents of RREG archive.

3. Use the instructions in [Updating the Standard Properties in the OAM11gRequest.xml File](#) to update the `OAM11gRequest.xml` file, and send the completed `OAM11gRequest.xml` file to the Oracle Access Manager server administrator.
4. The Oracle Access Manager server administrator then uses the instructions in [Running the RREG Tool in Out-Of-Band Mode](#) to run the RREG Tool and generate the `AgentID_response.xml` file.
5. The Oracle Access Manager server administrator sends the `AgentID_response.xml` file to you.
6. Use the instructions in [Running the RREG Tool in Out-Of-Band Mode](#) to run the RREG Tool with the `AgentID_response.xml` file and generate the required artifacts and files on the client system.

## Updating the Standard Properties in the OAM11gRequest.xml File

Before you can register the Webgate agent with Oracle Access Manager, you must update some required properties in the `OAM11gRequest.xml` file.

### Note:

- If you plan to use the default values for most of the parameters in the provided XML file, then you can use the shorter version (`OAM11gRequest_short.xml`), in which all non-listed fields take a default value.
- In the primary server list, the default names are mentioned as `OAM_SERVER1` and `OAM_SERVER2` for OAM servers. Rename these names in the list if the server names are changed in your environment.

To perform this task:

1. If you are using in-band mode, then change directory to the following location on one of the OAM Servers:

```
OAM_ORACLE_HOME/oam/server/rreg/input
```

If you are using out-of-band mode, then change directory to the location where you unpacked the RREG archive on the WEBHOST1 server.

2. Make a copy of the `OAM11gRequest.xml` file template with an environment-specific name.

```
cp OAM11gRequest.xml OAM11gRequest_edg.xml
```

3. Review the properties listed in the file, and then update your copy of the `OAM11gRequest.xml` file to make sure that the properties reference the host names and other values specific to your environment.

Table 20-1 Fields in the OAM11GRequest.xml file.

| OAM11gRequest.xml Property | Set to...                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| serverAddress              | The host and the port of the Administration Server for the Oracle Access Manager domain.                                                            |
| agentName                  | Any custom name for the agent. Typically, you use a name that identifies the Fusion Middleware product that you are configuring for single sign-on. |
| applicationDomain          | A value that identifies the web tier host and the FMW component you are configuring for single sign-on.                                             |
| security                   | Must be set to the security mode configured on the Oracle Access Management server. This is one of the three modes: open, simple, or certificate.   |

 **Note:**  
For an enterprise deployment, Oracle recommends simple mode, unless additional requirements exist to implement custom security certificates for the encryption of authentication and authorization traffic. In most cases, avoid using open mode, because in open mode, traffic to and from the Oracle Access Manager server is not encrypted.

For more information using certificate mode or about Oracle Access Manager supported security modes in general, see Securing Communication Between OAM Servers and WebGates in *Administrator's Guide for Oracle Access Management*.

|                    |         |
|--------------------|---------|
| cachePragmaHeader  | private |
| cacheControlHeader | private |



Table 20-1 (Cont.) Fields in the OAM11GRequest.xml file.

| OAM11gRequest.xml Property | Set to...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipValidation               | <p>0</p> <pre>&lt;ipValidation&gt;0&lt;/ipValidation&gt;</pre> <p>If ipValidation is set to '1', the IP address stored in the cookie must match the client's IP address, otherwise, the SSO cookie is rejected and the user must reauthenticate. This can cause problems with certain Web applications. For example, Web applications managed by a proxy server typically change the user's IP address, substituting the IP address of the proxy. Setting to '0' Disables IP validation.</p>        |
| ipValidationExceptions     | <p>Can be empty when ipValidation is '0'.</p> <p>If IP Validation is true, the IP address is compared to the IP Validation Exceptions list. If the address is found on the exceptions list, it does not need to match the IP address stored in the cookie. You can add as many IP addresses as needed. For example, the IP address of the front end load balancer:</p> <pre>&lt;ipValidationExceptions&gt;   &lt;ipAddress&gt;130.35.165.42&lt;/ipAddress&gt; &lt;/ipValidationExceptions&gt;</pre> |
| agentBaseUrl               | <p>Fully-qualified URL with the host and the port of the front-end Load Balancer VIP in front of the WEBHOST<sub>n</sub> machines on which Oracle HTTP 12c WebGates are installed.</p> <p>For example:</p> <pre>&lt;agentBaseUrl&gt;   https://wcc.example.com:443 &lt;/agentBaseUrl&gt;</pre>                                                                                                                                                                                                      |
| virtualHost                | <p>Set to <b>true</b> when protecting more than the agentBaseUrl, such as SSO protection for the administrative VIP.</p>                                                                                                                                                                                                                                                                                                                                                                            |

**Table 20-1 (Cont.) Fields in the OAM11GRequest.xml file.**

| OAM11gRequest.xml Property | Set to...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hostPortVariationsList     | <p>Add hostPortVariation host and port elements for each of the load-balancer URLs that are protected by the WebGates.</p> <p>For example:</p> <pre> &lt;hostPortVariationsList&gt;   &lt;hostPortVariations&gt;     &lt;host&gt;wccinternal.example.com&lt;/host&gt;   &lt;/hostPortVariations&gt;   &lt;hostPortVariations&gt;     &lt;host&gt;admin.example.com&lt;/host&gt;     &lt;port&gt;80&lt;/port&gt;   &lt;/hostPortVariations&gt;   &lt;hostPortVariations&gt;     &lt;host&gt;osb.example.com&lt;/host&gt;     &lt;port&gt;443&lt;/port&gt;   &lt;/hostPortVariations&gt; &lt;/hostPortVariationsList&gt; </pre> |
| logoutUrls                 | <p>Leave it empty.</p> <p>The Logout URL triggers the logout handler, which removes the cookie and requires the user to re-authenticate the next time the user accesses a resource protected by Access Manager. If Logout URL is not configured, the request URL is checked for <i>logout.</i> and, if found (except <i>logout.gif</i> and <i>logout.jpg</i>), also triggers the logout handler. If a value is set to this property, all used logout URLs must be added.</p>                                                                                                                                                  |
| primaryServerList          | <p>Verify that the host and the port of the OAM Managed Servers matches with this list. Example:</p> <pre> &lt;primaryServerList&gt;   &lt;Server&gt;     &lt;host&gt;wls_oam1&lt;/host&gt;     &lt;port&gt;14100&lt;/port&gt;     &lt;numOfConnections&gt;1&lt;/numOfConnections&gt;   &lt;/Server&gt;   &lt;Server&gt;     &lt;host&gt;wls_oam2&lt;/host&gt;     &lt;port&gt;14100&lt;/port&gt;     &lt;numOfConnections&gt;2&lt;/numOfConnections&gt;   &lt;/Server&gt; &lt;/primaryServerList&gt; </pre>                                                                                                                  |

## Updating the Protected, Public, and Excluded Resources for an Enterprise Deployment

When you set up an Oracle Fusion Middleware environment for single sign-on, you identify a set of URLs that you want Oracle Access Manager to protect with single sign-on. You identify these using specific sections of the `OAM11gRequest.xml` file. To identify the URLs:

1. If you have not already opened the copied `OAM11gRequest_edg.xml` file for editing, locate, and open the file in a text editor.

See [Locating and Preparing the RREG Tool](#)

See [Updating the Standard Properties in the OAM11gRequest.xml File](#)

2. Remove the sample entries from the file, and then enter the list of protected, public, and excluded resources in the appropriate sections of the file, as shown in the following example.

### Note:

If you are using Oracle Access Manager 11g Release 2 (11.1.2.2) or later, then note that the entries with the wildcard syntax (“`.../*`”) are included in this example for backward compatibility with previous versions of Oracle Access Manager.

```
<protectedResourcesList>
 <resource>/adfAuthentication</resource>
 <resource>/ibr/adfAuthentication</resource>
 <resource>/imaging/faces</resource>
 <resource>/em</resource>
 <resource>/console</resource>
 <resource>/DefaultToDoTaskFlow</resource>
 <resource>/sdpmessaging/userprefs-ui</resource>
 <resource>/integration/worklistapp</resource>
 <resource>/workflow/sdpmessaging-sca-ui-worklist</resource>
 <resource>/soa/composer</resource>
 <resource>/soa-infra/deployer</resource>
 <resource>/soa-infra/events/edn-db-log</resource>
 <resource>/soa-infra/cluster/info</resource>
 <resource>/soa-infra</resource>
 <resource>/dc-console/adfAuthentication</resource>
 <resource>/dc-client/adfAuthentication</resource>
 <resource>/wcc/adfAuthentication</resource>
</protectedResourcesList>
<publicResourcesList>
 <resource>/cs</resource>
 <resource>/_ocsh</resource>
 <resource>/_dav</resource>
 <resource>/imaging</resource>
 <resource>/soa-infra/directWSDL</resource>
 <resource>/dc-console</resource>
```

```

 <resource>/wcc</resource>
 </publicResourcesList>
 <excludedResourcesList>
 <resource>/imaging/jnlp</resource>
 <resource>/wsm-pm</resource>
 <resource>/soa-infra/services</resource>
 <resource>/ucs/messaging/webservice</resource>
 <resource>/imaging/ws</resource>
 <resource>/idcnativews</resource>
 <resource>/imaging/lib</resource>
 <resource>/cs/common/idcapplet.jar</resource>
 <resource>/cs/common/checkoutandopen*.jar </resource>
 <resource>/cs/images</resource>
 <resource>/dc-client</resource>
 <resource>/axf-ws</resource>
 </excludedResourcesList>

```

3. Save and close the OAM11GRequest\_edg.xml file.

#### Note:

For 11g Webgate, a user-defined parameter `filterOAMAuthnCookie` (default set to true) can be used to prevent the `OAMAuthnCookie` from being passed to downstream applications for security consideration. Some products such as IPM require to set the `filterOAMAuthnCookie` parameter to false.

## Running the RREG Tool

The following topics provide information about running the RREG tool to register your Oracle HTTP Server Webgate with Oracle Access Manager.

- [Running the RREG Tool in In-Band Mode](#)
- [Running the RREG Tool in Out-Of-Band Mode](#)

## Running the RREG Tool in In-Band Mode

To run the RREG Tool in in-band mode:

1. Change to the RREG home directory.

If you are using in-band mode, the RREG directory is inside the Oracle Access Manager Oracle home:

```
OAM_ORACLE_HOME/oam/server/rreg
```

If you are using out-of-band mode, then the RREG home directory is the location where you unpacked the RREG archive.

2. Change to the following directory:

- (UNIX) `RREG_HOME/bin`
- (Windows) `RREG_HOME\bin`

```
cd RREG_HOME/bin/
```

3. Set the permissions of the `oamreg.sh` command so that you can execute the file:

```
chmod +x oamreg.sh
```

4. Enter the following command:

```
./oamreg.sh inband RREG_HOME/input/OAM11GRequest_edg.xml
```

In this example:

- It is assumed that the edited `OAM11GRequest.xml` file is located in the `RREG_HOME/input` directory.
- The output from this command is saved to the following directory:

```
RREG_HOME/output/
```

The following example shows a sample RREG session:

```
Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
Mode: inband
Filename: /u01/oracle/products/fmw/iam_home/oam/server/rreg/client/rreg/
input/OAM11GRequest_edg.xml
Enter admin username:weblogic_idm
Username: weblogic_iam
Enter admin password:
Do you want to enter a Webgate password?(y/n):
n
Do you want to import an URIs file?(y/n):
n
```

```

Request summary:
OAM11G Agent Name:SOA12213_EDG_AGENT
Base URL: https://soa.example.com:443
URL String:null
Registering in Mode:inband
Your registration request is being sent to the Admin server at: http://
host1.example.com:7001

```

```
Jul 08, 2015 7:18:13 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Jul 08, 2015 7:18:14 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Inband registration process completed successfully! Output artifacts
are created in the output folder.
```

## Running the RREG Tool in Out-Of-Band Mode

To run the RREG Tool in out-of-band mode on the WEBHOST server, the administrator uses the following command:

```
RREG_HOME/bin/oamreg.sh outofband input/OAM11GRequest.xml
```

In this example:

- Replace *RREG\_HOME* with the location where the RREG archive file was unpacked on the server.
- The edited *OAM11GRequest.xml* file is located in the *RREG\_HOME/input* directory.
- The RREG Tool saves the output from this command (the *AgentID\_response.xml* file) to the following directory:

*RREG\_HOME/output/*

The Oracle Access Manager server administrator can then send the *AgentID\_response.xml* to the user who provided the *OAM11GRequest.xml* file.

To run the RREG Tool in out-of-band mode on the web server client machine, use the following command:

```
RREG_HOME/bin/oamreg.sh outofband input/AgentID_response.xml
```

In this example:

- Replace *RREG\_HOME* with the location where you unpacked the RREG archive file on the client system.
- The *AgentID\_response.xml* file, which was provided by the Oracle Access Manager server administrator, is located in the *RREG\_HOME/input* directory.
- The RREG Tool saves the output from this command (the artifacts and files required to register the Webgate software) to the following directory on the client machine:

*RREG\_HOME/output/*

## Files and Artifacts Generated by RREG

The files that get generated by the RREG Tool vary, depending on the security level you are using for communications between the WebGate and the Oracle Access Manager server. See *Securing Communication Between OAM Servers and WebGates* in *Administrator's Guide for Oracle Access Management*.

Note that in this topic any references to *RREG\_HOME* should be replaced with the path to the directory where you ran the RREG tool. This is typically the following directory on the Oracle Access Manager server, or (if you are using out-of-band mode) the directory where you unpacked the RREG archive:

*OAM\_ORACLE\_HOME/oam/server/rreg/client*

The following table lists the artifacts that are always generated by the RREG Tool, regardless of the Oracle Access Manager security level.

| File                      | Location                                                                                                                                                                                                         |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cwallet.sso</i>        | <ul style="list-style-type: none"> <li>• <i>RREG_HOME/output/Agent_ID/</i> - For WebGate 11g (11.1.2.3).</li> <li>• <i>RREG_HOME/output/Agent_ID/wallet</i> - For WebGate 11g (11.1.2.2) and OHS 12c.</li> </ul> |
| <i>ObAccessClient.xml</i> | <i>RREG_HOME/output/Agent_ID/</i>                                                                                                                                                                                |

The following table lists the additional files that are created if you are using the SIMPLE or CERT security level for Oracle Access Manager:

| File         | Location                   |
|--------------|----------------------------|
| aaa_key.pem  | RREG_HOME/output/Agent_ID/ |
| aaa_cert.pem | RREG_HOME/output/Agent_ID/ |
| password.xml | RREG_HOME/output/Agent_ID/ |

Note that the password.xml file contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be different than the passphrase used on the server.

You can use the files generated by RREG to generate a certificate request and get it signed by a third-party Certification Authority. To install an existing certificate, you must use the existing aaa\_cert.pem and aaa\_chain.pem files along with password.xml and aaa\_key.pem.

## Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location

After the RREG Tool generates the required artifacts, manually copy the artifacts from the *RREG\_Home/output/agent\_ID* directory to the Oracle HTTP Server configuration directory on the web tier host.

The location of the files in the Oracle HTTP Server configuration directory depends upon the Oracle Access Manager security mode setting (OPEN, SIMPLE, or CERT).

The following table lists the required location of each generated artifact in the Oracle HTTP Server configuration directory, based on the security mode setting for Oracle Access Manager. In some cases, you might have to create the directories if they do not exist already. For example, the wallet directory might not exist in the configuration directory.

### Note:

For an enterprise deployment, Oracle recommends simple mode, unless additional requirements exist to implement custom security certificates for the encryption of authentication and authorization traffic. The information about using open or certification mode is provided here as a convenience.

Avoid using open mode, because in open mode, traffic to and from the Oracle Access Manager server is not encrypted.

For more information about using certificate mode or about Oracle Access Manager supported security modes in general, see *Securing Communication Between OAM Servers and WebGates* in *Administrator's Guide for Oracle Access Management*.

Table 20-2 Web Tier Host Location to Copy the Generated Artifacts

| File                            | Location When Using OPEN Mode        | Location When Using SIMPLE Mode                                                                                                                        | Location When Using CERT Mode         |
|---------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| wallet/cwallet.sso <sup>1</sup> | WEB_CONFIG_DIR/webgate/config/wallet | WEB_CONFIG_DIR/webgate/config/wallet/<br>By default the wallet folder is not available. Create the wallet folder under WEB_CONFIG_DIR/webgate/config/. | WEB_CONFIG_DIR/webgate/config/wallet/ |
| ObAccessClient.xml              | WEB_CONFIG_DIR/webgate/config        | WEB_CONFIG_DIR/webgate/config/                                                                                                                         | WEB_CONFIG_DIR/webgate/config/        |
| password.xml                    | N/A                                  | WEB_CONFIG_DIR/webgate/config/                                                                                                                         | WEB_CONFIG_DIR/webgate/config/        |
| aaa_key.pem                     | N/A                                  | WEB_CONFIG_DIR/webgate/config/simple/                                                                                                                  | WEB_CONFIG_DIR/webgate/config/        |
| aaa_cert.pem                    | N/A                                  | WEB_CONFIG_DIR/webgate/config/simple/                                                                                                                  | WEB_CONFIG_DIR/webgate/config/        |

<sup>1</sup> Copy cwallet.sso from the wallet folder and not from the output folder. Even though there are 2 files with the same name they are different. The one in the wallet sub directory is the correct one.

 **Note:**

If you need to redeploy the ObAccessClient.xml to WEBHOST1 and WEBHOST2, delete the cached copy of ObAccessClient.xml and its lock file, ObAccessClient.xml.lck from the servers. The cache location on WEBHOST1 is:

WEB\_DOMAIN\_HOME/servers/ohs1/cache/

And you must perform the similar step for the second Oracle HTTP Server instance on WEBHOST2:

WEB\_DOMAIN\_HOME/servers/ohs2/cache/

## Insert OHS SimpleCA Certificate into the Wallet Artifact

If the OHS servers have been configured with an 11g or earlier version of the OAM server, there is a need to insert the OHS SimpleCA certificate into the wallet file artifact that was deployed in [Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location](#).

Complete the following steps:

1. On WEBHOST1, go to the following directory:

WEB\_CONFIG\_DIR/webgate/config/wallet



2. Run the following command to insert the SimpleCA certificate into the wallet file:

```
WEB_ORACLE_HOME/oracle_common/bin/orapki wallet add -wallet ./
-trusted_cert -cert WEB_ORACLE_HOME/webgate/ohs/tools/openssl/
simpleCA/cacert.pem -auto_login_only
```

The following output is displayed:

```
simpleCA/cacert.pem -auto_login_only
Oracle PKI Tool : Version 12.2.1.3.0
Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights
reserved.
```

```
Operation is successfully completed.
```

3. Validate the certificate insertion with the following command:

```
WEB_ORACLE_HOME/oracle_common/bin/orapki wallet display -wallet ./
```

The following output is displayed:

```
Oracle PKI Tool : Version 12.2.1.3.0
Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights
reserved.
```

```
Requested Certificates:
User Certificates:
Oracle Secret Store entries: OAMAgent@#3#@wcedgRwse01Env1Ps3_Key
Trusted Certificates:
Subject: CN=NetPoint Simple Security CA - Not for General
Use,OU=NetPoint,O=Obliv\, Inc.,L=Cupertino,ST=California,C=US
```

4. Repeat steps 1 through 3 on WEBHOST2.

## Enable MD5 Certificate Signatures for the Oracle HTTP Server Instances

Some releases of Oracle Access Management Server implement simple mode security certificates by using MD5 signatures unless upgraded or patched appropriately. Oracle Recommends that, if possible, the OAM certificates are upgraded to SHA-2 certificates. This might not be possible for customers who have several versions of Oracle HTTP server to contend with.

If upgrading the certificates is not possible, support for MD5 signatures must be enabled manually to make Oracle HTTP server 12.2.1.x work with Oracle Access Manager 11g's MD5 certificates when you use a webgate in simple security mode.

To enable MD5 certificate signatures on each OHS instance, complete the following steps:

1. On WEBHOST1, change to the following directory:

```
WEB_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1
```

2. Open the `ohs.plugins.nodemanager.properties` file, add the following line, and save the file.

```
environment.ORACLE_SSL_ALLOW_MD5_CERT_SIGNATURES = 1
```

3. Repeat steps 1 and 2 for all other instances on the `WEBHOST $n$`  servers.  
For example, the `ohs2` instance on `WEBHOST2`



#### Note:

The change takes effect when the instances are restarted in the next topic.

## Restarting the Oracle HTTP Server Instance

For information about restarting the Oracle HTTP Server instance, see *Restarting Oracle HTTP Server Instances by Using WLST in Oracle Fusion Middleware Administering Oracle HTTP Server*.

If you have configured Oracle HTTP Server in a WebLogic Server domain, you can also use Oracle Fusion Middleware Control to restart the Oracle HTTP Server instances. See *Restarting Oracle HTTP Server Instances by Using Fusion Middleware Control in Oracle Fusion Middleware Administering Oracle HTTP Server*.

## Setting Up the WebLogic Server Authentication Providers

To set up the WebLogic Server authentication providers, back up the configuration files, set up the Oracle Access Manager Identity Assertion Provider and set the order of providers.

The following topics assumes that you have already configured the LDAP authenticator by following the steps in [Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group](#). If you have not already created the LDAP authenticator, then do so before you continue with this section.

- [Backing Up Configuration Files](#)
- [Setting Up the Oracle Access Manager Identity Assertion Provider](#)
- [Updating the Default Authenticator and Setting the Order of Providers](#)

## Backing Up Configuration Files

To be safe, you should first back up the relevant configuration files:

```
ASERVER_HOME/config/config.xml
ASERVER_HOME/config/fmwconfig/jps-config.xml
ASERVER_HOME/config/fmwconfig/system-jazn-data.xml
```

Also back up the `boot.properties` file for the Administration Server:

```
ASERVER_HOME/servers/AdminServer/security/boot.properties
```

## Setting Up the Oracle Access Manager Identity Assertion Provider

Set up an Oracle Access Manager identity assertion provider in the Oracle WebLogic Server Administration Console.

To set up the Oracle Access Manager identity assertion provider:

1. Log in to the WebLogic Server Administration Console, if not already logged in.
2. Click **Lock & Edit**.
3. Click **Security Realms** in the left navigation bar.
4. Click the **myrealm** default realm entry.
5. Click the **Providers** tab.
6. Click **New**, and select the asserter type **OAMIdentityAsserter** from the drop-down menu.
7. Name the asserter (for example, *OAM ID Asserter*), and click **OK**.
8. Click the newly added asserter to see the configuration screen for the Oracle Access Manager identity assertion provider.
9. Set the control flag to *REQUIRED*.
10. Under Chosen types, select both the **ObSSOCookie** and **OAM\_REMOTE\_USER** options, if they are not selected by default.
11. Click **Save** to save the settings.
12. Click **Activate Changes** to propagate the changes.

## Updating the Default Authenticator and Setting the Order of Providers

Set the order of identity assertion and authentication providers in the WebLogic Server Administration console.

To update the default authenticator and set the order of the providers:

1. Log in to the WebLogic Server Administration Console, if not already logged in.
2. Click **Lock & Edit**.
3. From the left navigation, select **Security Realms**.
4. Click the **myrealm** default realm entry.
5. Click the **Providers** tab.
6. From the table of providers, click the **DefaultAuthenticator**.
7. Set the Control Flag to *SUFFICIENT*.
8. Click **Save** to save the settings.
9. From the navigation breadcrumbs, click **Providers** to return to the list of providers.
10. Click **Reorder**.
11. Sort the providers to ensure that the OAM Identity Assertion provider is first and the DefaultAuthenticator provider is last.

Table 20-3 Sort order

| Sort Order | Provider                        | Control Flag |
|------------|---------------------------------|--------------|
| 1          | OAMIdentityAsserter             | REQUIRED     |
| 2          | LDAP Authentication Provider    | SUFFICIENT   |
| 3          | DefaultAuthenticator            | SUFFICIENT   |
| 4          | Trust Service Identity Asserter | N/A          |
| 5          | DefaultIdentityAsserter         | N/A          |

12. Click **OK**.
13. Click **Activate Changes** to propagate the changes.
14. Shut down the Administration Server, Managed Servers, and any system components, as applicable.
15. Restart the Administration Server.
16. If you are going to configure ADF consoles with SSO, you can keep the managed servers down and restart them later. If not, you need to restart managed servers now.

## Configuring Oracle ADF and OPSS Security with Oracle Access Manager

Some Oracle Fusion Middleware management consoles use Oracle Application Development Framework (Oracle ADF) security, which can integrate with Oracle Access Manager Single Sign On (SSO). These applications can take advantage of Oracle Platform Security Services (OPSS) SSO for user authentication, but you must first configure the domain-level `jps-config.xml` file to enable these capabilities.

The domain-level `jps-config.xml` file is located in the following location after you create an Oracle Fusion Middleware domain:

`ASERVER_HOME/config/fmwconfig/jps-config.xml`

### Note:

The domain-level `jps-config.xml` should not be confused with the `jps-config.xml` that is deployed with custom applications.

To update the OPSS configuration to delegate SSO actions in Oracle Access Manager, complete the following steps:

1. Change to the following directory:  
`ORACLE_COMMON_HOME/common/bin`
2. Start the WebLogic Server Scripting Tool (WLST):  
`./wlst.sh`

3. Connect to the Administration Server, by using the following WLST command:

```
connect('admin_user','admin_password','admin_url')
```

For example:

```
connect('weblogic_wcc','mypassword','t3://ADMINVHN:7001')
```

4. Run the addOAMSSOProvider command, as shown:

```
addOAMSSOProvider(loginuri="/${app.context}/
adfAuthentication", logouturi="/oamssso/logout.html")
```

The following table defines the expected value for each argument in the addOAMSSOProvider command.

**Table 20-4 Expected Values for the Argument in the addOAMSSOProvider command**

| Argument        | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>loginuri</i> | Specifies the URI of the login page <div data-bbox="808 827 850 865"></div> <div data-bbox="850 827 938 863"><b>Note:</b></div> <div data-bbox="850 884 1343 976">For ADF security enabled applications, <i>"/context-root/adfAuthentication"</i> should be provided for the 'loginuri' parameter.</div> <p>For example:</p> <pre>/\${app.context}/adfAuthentication</pre> <div data-bbox="808 1180 850 1218"></div> <div data-bbox="850 1180 938 1215"><b>Note:</b></div> <div data-bbox="850 1236 1278 1331"><i>\${app.context}</i> must be entered as shown. At runtime, the application replaces the variable appropriately.</div> <p>Here is the flow:</p> <ol style="list-style-type: none"> <li>a. User accesses a resource that has been protected by authorization policies in OPSS, for example.</li> <li>b. If the user is not yet authenticated, ADF redirects the user to the URI configured in <i>loginuri</i>.</li> <li>c. Access Manager, should have a policy to protect the value in <i>loginuri</i>: for example, <i>"/context-root/adfAuthentication"</i>.</li> <li>d. When ADF redirects to this URI, Access Manager displays a Login Page (depending on the authentication scheme configured in Access Manager for this URI).</li> </ol> |

**Table 20-4 (Cont.) Expected Values for the Argument in the addOAMSSOProvider command**

| Argument            | Definition                                                                                                  |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| <i>logouturi</i>    | Specifies the URI of the logout page. The value of the <i>loginurl</i> is usually <i>/oam/logout.html</i> . |
| <i>autologinuri</i> | Specifies the URI of the autologin page. This is an optional parameter.                                     |

5. Disconnect from the Administration Server by entering the following command:  
`disconnect()`
6. Restart the Administration Server and the managed servers.

# A

## Using Multi Data Sources with Oracle RAC

Oracle recommends that you use GridLink data sources when you develop new Oracle RAC applications. However, if you are using legacy applications and databases that do not support GridLink data sources, refer to the information in this appendix.

This appendix provides information about multi data sources and Oracle RAC and procedure for configuring multi data sources for an Enterprise Deployment.

- [About Multi Data Sources and Oracle RAC](#)  
A multi data source provides an ordered list of data sources to use to satisfy connection requests.
- [Typical Procedure for Configuring Multi Data Sources for an Enterprise Deployment](#)  
You need to configure data sources when you configure a domain. If you want to use Multi Data Sources instead of GridLink data sources, replace the GridLink instructions with the instructions provided in this section.

### About Multi Data Sources and Oracle RAC

A multi data source provides an ordered list of data sources to use to satisfy connection requests.

Normally, every connection request to this kind of multi data source is served by the first data source in the list. If a database connection test fails and the connection cannot be replaced, or if the data source is suspended, a connection is sought sequentially from the next data source on the list.

For more information about configuring Multi Data Sources with Oracle RAC, see Using Multi Data Sources with Oracle RAC in *Oracle Fusion Middleware Administering JDBC Data Sources for Oracle WebLogic Server*.

### Typical Procedure for Configuring Multi Data Sources for an Enterprise Deployment

You need to configure data sources when you configure a domain. If you want to use Multi Data Sources instead of GridLink data sources, replace the GridLink instructions with the instructions provided in this section.

For example, when you are configuring the initial Administration domain for an Enterprise Deployment reference topology, you use the configuration wizard to define the characteristics of the domain, as well as the data sources.

The procedures for configuring the topologies in this Enterprise Deployment Guide include specific instructions for defining GridLink data sources with Oracle RAC. If you want to use Multi Data Sources instead of GridLink data sources, replace the GridLink instructions with the following:

1. In the Configure JDBC Component Schema screen:

- a. Select the appropriate schemas.
  - b. For the RAC configuration for component schemas, **Convert to RAC multi data source**.
  - c. Ensure that the following data source appears on the screen with the schema prefix when you ran the Repository Creation Utility.
  - d. Click **Next**.
2. The Configure RAC Multi Data Sources Component Schema screen appears (Figure A-1).

**Figure A-1 Configure RAC Multi Data Source Component Schema Screen**

**Fusion Middleware Configuration Wizard**

**Configure RAC Multi Data Source Component Schema**

**Note:** Change only the input fields below that you wish to modify and values will be applied to all selected rows.

Driver: \*Oracle's Driver (Thin) for RAC Service-Instance c[...]

Service Name: imedg.mycompany.com

Username: soaedg\_mds

Password: \*\*\*\*\*

| Host Name              | Instance Name | Port |
|------------------------|---------------|------|
| infradbhost1-vip.mycom | imedg1        | 1521 |
| infradbhost2-vip.mycom | imedg2        | 1521 |

Add Delete

| Multi Data Source Schema                            | Service Name        | Schema Owner | Schema Password |
|-----------------------------------------------------|---------------------|--------------|-----------------|
| <input checked="" type="checkbox"/> OWSM MDS Schema | imedg.mycompany.com | soaedg_mds   | *****           |

Exit Help Previous Next

In this screen, do the following:

- a. Enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU.
  - **Driver:** Select **Oracle driver (Thin) for RAC Service-Instance connections, Versions:10, 11**.
  - **Service Name:** Enter the service name of the database.
  - **Username:** Enter the complete user name (including the prefix) for the schemas.
  - **Password:** Enter the password to use to access the schemas.
- b. Enter the host name, instance name, and port.



- c. Click **Add**.
  - d. Repeat this for each Oracle RAC instance.
  - e. Click **Next**.
- 3. In the Test JDBC Data Sources screen, the connections are tested automatically. The **Status** column displays the results. Ensure that all connections were successful. If not, click **Previous** to return to the previous screen and correct your entries.

Click **Next** when all the connections are successful.

# Oracle® Fusion Middleware

## Installing and Configuring Oracle WebCenter Content



12c (12.2.1.4.0)

E95183-06

August 2022

ORACLE®

Copyright © 2019, 2022, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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 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" or "commercial computer software documentation" 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, and MySQL 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

## Preface

---

|                             |      |
|-----------------------------|------|
| Audience                    | viii |
| Documentation Accessibility | viii |
| Diversity and Inclusion     | viii |
| Related Documents           | ix   |
| Conventions                 | ix   |

## 1 About the Oracle WebCenter Content Installation

---

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| Using the Standard Installation Topology as a Starting Point      | 1-1 |
| About the WebCenter Content Standard Installation Topology        | 1-1 |
| About Elements in the Standard Installation Topology Illustration | 1-3 |
| About Installing Oracle User Messaging Service                    | 1-4 |
| About Oracle WebCenter Content Scale Up                           | 1-4 |
| Using This Document to Extend an Existing Domain                  | 1-4 |

## 2 Preparing to Install and Configure Oracle WebCenter Content

---

|                                                                                                |      |
|------------------------------------------------------------------------------------------------|------|
| Mandatory Steps for Installing WebCenter Content on Windows Operating Systems                  | 2-1  |
| Disabling the 8.3 File Naming Convention on a Windows Operating System                         | 2-2  |
| Downloading Visual C++ Libraries                                                               | 2-2  |
| Downloading Microsoft .Net Framework 4.x                                                       | 2-3  |
| Roadmap for Installing and Configuring the Standard Installation Topologies                    | 2-3  |
| Roadmap for Verifying Your System Environment                                                  | 2-4  |
| Verifying Certification, System, and Interoperability Requirements                             | 2-5  |
| Selecting an Installation User                                                                 | 2-6  |
| About User Permissions                                                                         | 2-6  |
| Understanding Non-Default User Permissions on UNIX Operating Systems                           | 2-8  |
| Verifying that the Installation User has Administrator Privileges on Windows Operating Systems | 2-8  |
| Understanding Directories for Installation and Configuration                                   | 2-9  |
| Understanding the Recommended Directory Structure                                              | 2-9  |
| About the Oracle Home Directory                                                                | 2-10 |

|                                                                             |      |
|-----------------------------------------------------------------------------|------|
| About the Domain Home Directory                                             | 2-11 |
| About the Application Home Directory                                        | 2-12 |
| Installing Multiple Products in the Same Domain                             | 2-12 |
| Preparing for Shared Storage                                                | 2-13 |
| Understanding JDK Requirements for an Oracle Fusion Middleware Installation | 2-13 |
| About Database Requirements for an Oracle Fusion Middleware Installation    | 2-14 |
| Obtaining the Product Distribution                                          | 2-14 |
| About Product Distributions                                                 | 2-14 |

### 3 Installing the Oracle WebCenter Content Software

---

|                                         |     |
|-----------------------------------------|-----|
| Verifying the Installation Checklist    | 3-1 |
| Starting the Installation Program       | 3-2 |
| Navigating the Installation Screens     | 3-3 |
| Verifying the Installation              | 3-4 |
| Reviewing the Installation Log Files    | 3-4 |
| Checking the Directory Structure        | 3-5 |
| Viewing the Contents of the Oracle Home | 3-5 |

### 4 Configuring WebCenter Content Domain

---

|                                                                                |      |
|--------------------------------------------------------------------------------|------|
| Creating the Database Schemas                                                  | 4-1  |
| Installing and Configuring a Certified Database                                | 4-2  |
| Starting the Repository Creation Utility                                       | 4-2  |
| Navigating the Repository Creation Utility Screens to Create Schemas           | 4-2  |
| Introducing the RCU                                                            | 4-3  |
| Selecting a Method of Schema Creation                                          | 4-3  |
| Providing Database Connection Details                                          | 4-4  |
| Specifying a Custom Prefix and Selecting Schemas                               | 4-5  |
| Specifying Schema Passwords                                                    | 4-7  |
| Completing Schema Creation                                                     | 4-7  |
| Configuring the Domain                                                         | 4-7  |
| Starting the Configuration Wizard                                              | 4-8  |
| Navigating the Configuration Wizard Screens to Create and Configure the Domain | 4-8  |
| Selecting the Domain Type and Domain Home Location                             | 4-10 |
| Selecting Configuration Templates for Oracle WebCenter Content                 | 4-10 |
| Configuring High Availability Options                                          | 4-11 |
| Selecting the Application Home Location                                        | 4-12 |
| Configuring the Administrator Account                                          | 4-12 |
| Specifying the Domain Mode and JDK                                             | 4-13 |
| Specifying JDBC Data Sources                                                   | 4-13 |

|                                                                             |      |
|-----------------------------------------------------------------------------|------|
| Testing the JDBC Data Source                                                | 4-14 |
| Specifying the Database Configuration Type                                  | 4-14 |
| Specifying JDBC Component Schema Information                                | 4-16 |
| Testing the JDBC Connections                                                | 4-16 |
| Entering Credentials                                                        | 4-17 |
| Selecting Advanced Configuration                                            | 4-17 |
| Configuring the Administration Server Listen Address                        | 4-17 |
| Configuring Node Manager                                                    | 4-18 |
| Configuring Managed Servers for Oracle WebCenter Content                    | 4-18 |
| Configuring a Cluster for WebCenter Content                                 | 4-19 |
| Defining Server Templates                                                   | 4-19 |
| Configuring Dynamic Servers                                                 | 4-19 |
| Assigning WebCenter Content Managed Servers to the Cluster                  | 4-20 |
| Configuring Coherence Clusters                                              | 4-20 |
| Creating a New WebCenter Content Machine                                    | 4-21 |
| Assigning Servers to WebCenter Content Machines                             | 4-21 |
| Virtual Targets                                                             | 4-22 |
| Partitions                                                                  | 4-22 |
| Reviewing Your Configuration Specifications and Configuring the Domain      | 4-22 |
| Writing Down Your Domain Home and Administration Server URL                 | 4-22 |
| Starting the Servers                                                        | 4-23 |
| Starting Node Manager                                                       | 4-23 |
| Starting the Administration Server                                          | 4-24 |
| Starting the Managed Servers                                                | 4-24 |
| Oracle WebCenter Content Managed Server Locations (URLs)                    | 4-25 |
| Verifying the Configuration                                                 | 4-25 |
| Configuring Inbound Refinery Settings (Single Node)                         | 4-25 |
| Inbound Refinery Configuration Page                                         | 4-26 |
| Configuring WebCenter Content Settings                                      | 4-28 |
| WebCenter Content Configuration Page                                        | 4-29 |
| Completing the Imaging Configuration                                        | 4-31 |
| Completing the Initial Imaging Configuration                                | 4-32 |
| Configuring the Full-Text Features in the WebCenter Content Repository      | 4-39 |
| Setting Imaging System Security                                             | 4-39 |
| Configuring the Imaging Viewer Cache                                        | 4-40 |
| Installing and Configuring AXF BPM and AXF for BPEL                         | 4-42 |
| Configuring Capture                                                         | 4-54 |
| About Completing the Oracle WebCenter Enterprise Capture Configuration      | 4-54 |
| Completing the Initial Configuration of Oracle WebCenter Enterprise Capture | 4-55 |

## 5 Next Steps After Configuring the Domain

---

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Performing Basic Administrative Tasks                            | 5-1 |
| Performing Additional Domain Configuration Tasks                 | 5-2 |
| Preparing Your Environment for High Availability                 | 5-3 |
| Configuring WebCenter Content User Interface on Additional Nodes | 5-4 |
| Setting the WebCenter Content User Interface Server Socket Port  | 5-5 |
| Configuring WebCenter Content User Interface Settings            | 5-5 |
| Setting Connection Attributes with WLST                          | 5-5 |
| Setting Connection Attributes with Fusion Middleware Control     | 5-6 |
| Setting Configuration Attributes with WLST                       | 5-6 |
| Setting Configuration Attributes with Fusion Middleware Control  | 5-7 |

## 6 Uninstalling or Reinstalling Oracle WebCenter Content

---

|                                                             |     |
|-------------------------------------------------------------|-----|
| About Product Uninstallation                                | 6-1 |
| Stopping Oracle Fusion Middleware                           | 6-2 |
| Removing Your Database Schemas                              | 6-2 |
| Uninstalling the Software                                   | 6-3 |
| Starting the Uninstall Wizard                               | 6-3 |
| Selecting the Product to Uninstall                          | 6-3 |
| Navigating the Uninstall Wizard Screens                     | 6-3 |
| Removing the Oracle Home Directory Manually                 | 6-4 |
| Removing the Program Shortcuts on Windows Operating Systems | 6-4 |
| Removing the Domain and Application Data                    | 6-5 |
| Reinstalling the Software                                   | 6-5 |

## A Configuring Content Server

---

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| Configuring Records Management in Content Server                                         | A-1 |
| About Configuring Oracle iPlanet Web Server as a Web Tier and Configuring Shared Folders | A-3 |
| Configuring the Content Server for Desktop                                               | A-3 |
| About Installing and Configuring the Desktop on a Client Workstation                     | A-5 |
| Opening Files from Microsoft Office 2010 Over a Non-SSL Connection                       | A-5 |

## B Inbound Refinery Standalone Topology

---

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| Roadmap for Installing and Configuring the Inbound Refinery Standalone Topology | B-1 |
|---------------------------------------------------------------------------------|-----|

## C Installing Libraries and Setting Environment Variables

---

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Installing Libraries on UNIX Platforms                           | C-1 |
| Setting Library Paths in Environment Variables on UNIX Platforms | C-3 |

## D Additional Configuration Steps

---

|                                                                                 |      |
|---------------------------------------------------------------------------------|------|
| Converting Vector Graphics and Spreadsheet Text in UNIX                         | D-1  |
| Setting up Fonts on a UNIX System                                               | D-2  |
| Setting Up TrueType Fonts on a UNIX System                                      | D-2  |
| Installing Fonts for National Language Support on a UNIX System                 | D-3  |
| Reassociating the Identity Store with an External LDAP Authentication Provider  | D-3  |
| Reassociating the Identity Store with Oracle Internet Directory                 | D-4  |
| Configuring OracleTextSearch for Content Server                                 | D-8  |
| Creating a Search Schema and Configuring an External Data Source                | D-9  |
| Configuring OracleTextSearch for Content Server in a Configuration File         | D-10 |
| Extracting and Running the Installation File for Desktop Client Software        | D-11 |
| Using Command-Line Parameters for Automation                                    | D-12 |
| Disabling Integrations                                                          | D-12 |
| Performing Silent Roll-Outs                                                     | D-12 |
| Configuring Content Server Connections Through the Registry on a Windows System | D-13 |
| Creating a Hash Partition to Improve Database Performance                       | D-14 |

## E Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product

---

|                                                                                      |     |
|--------------------------------------------------------------------------------------|-----|
| About Updating the JDK Location After Installing an Oracle Fusion Middleware Product | E-1 |
| Updating the JDK Location in an Existing Oracle Home                                 | E-2 |
| Updating the JDK Location in an Existing Domain Home                                 | E-3 |



# Preface

This document describes how to install and configure Oracle WebCenter Content.

- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Documents](#)
- [Conventions](#)

Learn about the conventions used in this document.

## Audience

This guide is intended for system administrators or application developers who are installing and configuring Oracle WebCenter Content. It is assumed that readers are familiar with web technologies and have a general understanding of Windows and UNIX platforms.

## Documentation Accessibility

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

### **Access to Oracle Support**

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

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## Related Documents

Refer to the Oracle Fusion Middleware Library for additional information.

- For Oracle WebCenter Content information, see [Oracle WebCenter Content Documentation](#).
- For installation information, see Fusion Middleware Installation Documentation.
- For upgrade information, see Fusion Middleware Upgrade Documentation.
- For administration-related information, see Fusion Middleware Administration Documentation.
- For release-related information, see Fusion Middleware Release Notes.

## Conventions

Learn about the conventions used in this document.

This document uses the following text conventions:

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

# 1

## About the Oracle WebCenter Content Installation

The standard installation for Oracle WebCenter Content described in this guide creates the standard topology, which represents a sample starting topology for this product.

- [Using the Standard Installation Topology as a Starting Point](#)  
The standard installation topology is a flexible topology that you can use as a starting point in production environments.
- [Using This Document to Extend an Existing Domain](#)  
The procedures in this guide describe how to create a new domain. The assumption is that no other Oracle Fusion Middleware products are installed on your system.

### Using the Standard Installation Topology as a Starting Point

The standard installation topology is a flexible topology that you can use as a starting point in production environments.

The information in this guide helps you to create a standard installation topology for Oracle WebCenter Content. If required, you can later extend the standard installation topology to create a secure and highly available production environment, see [Next Steps After Configuring the Domain](#).

The standard installation topology represents a sample topology for this product. It is not the only topology that this product supports. See *About the Standard Installation Topology in Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware*.

- [About the WebCenter Content Standard Installation Topology](#)  
This topology represents a standard WebLogic Server domain that contains an Administration Server and a cluster that contains two Managed Servers.
- [About Elements in the Standard Installation Topology Illustration](#)  
The standard installation topology typically includes common elements.
- [About Installing Oracle User Messaging Service](#)  
Oracle User Messaging Service (UMS) is a software technology that enables two-way communication between users and deployed applications.
- [About Oracle WebCenter Content Scale Up](#)  
Oracle WebCenter Content supports only one Inbound Refinery Managed Server per node per domain, and one WebCenter Content Managed Server per node, per domain.

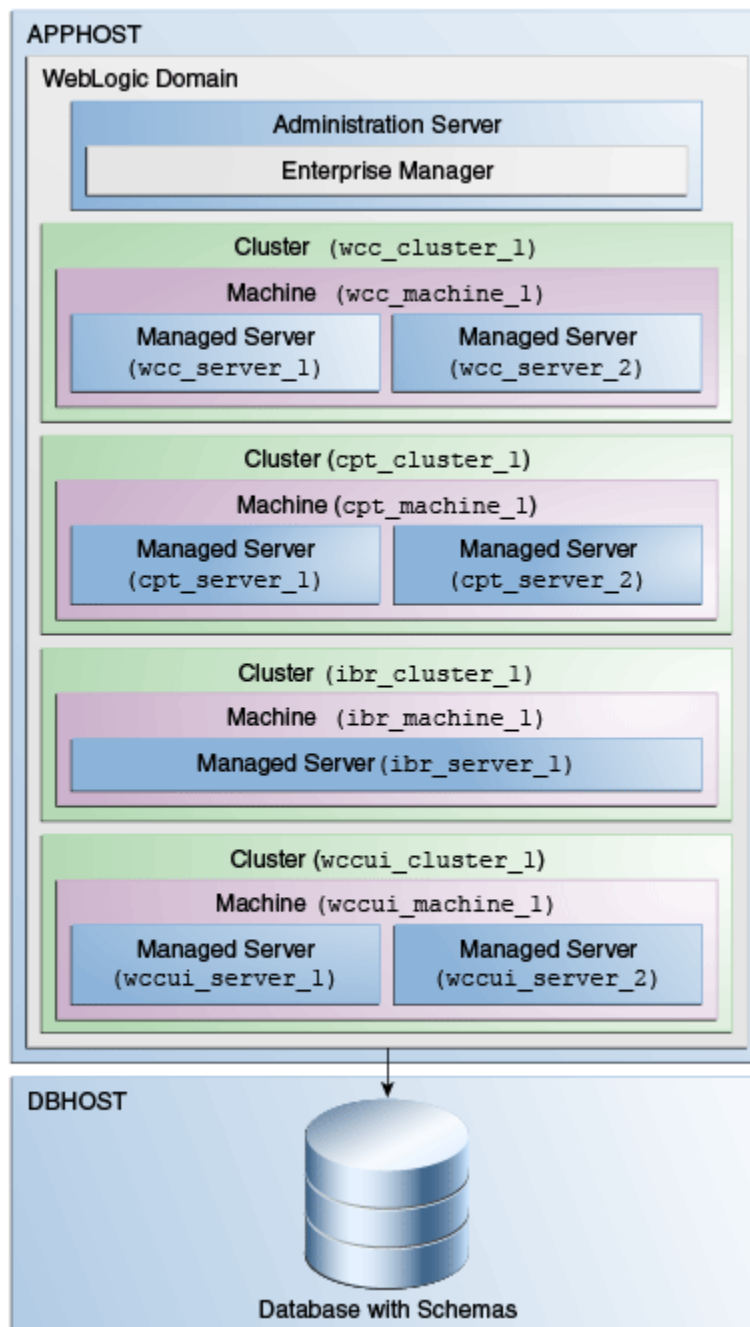
### About the WebCenter Content Standard Installation Topology

This topology represents a standard WebLogic Server domain that contains an Administration Server and a cluster that contains two Managed Servers.

The following figure shows the standard installation topology for WebCenter Content.

See [Table 1-1](#) for information on the elements for this topology.

Figure 1-1 WebCenter Content Standard Installation Topology



**Note:**

If you have enabled IPM server, it will be represented as a separate managed server.

## About Elements in the Standard Installation Topology Illustration

The standard installation topology typically includes common elements.

The following table describes all elements of the topology illustration:

**Table 1-1 Description of Elements in Standard Installation Topologies**

| Element               | Description and Links to Related Documentation                                                                                                                                                                                                                                                                |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPHOST               | A standard term used in Oracle documentation to refer to the machine that hosts the application tier.                                                                                                                                                                                                         |
| DBHOST                | A standard term used in Oracle documentation to refer to the machine that hosts the database.                                                                                                                                                                                                                 |
| WebLogic Domain       | A logically related group of Java components (in this case, the Administration Server, Managed Servers, and other related software components).<br>See <i>What Is an Oracle WebLogic Server Domain?</i> in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                           |
| Administration Server | Central control entity of a WebLogic domain. It maintains configuration objects for that domain and distributes configuration changes to Managed Servers.<br>See <i>What Is the Administration Server?</i> in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                        |
| Enterprise Manager    | The Oracle Enterprise Manager Fusion Middleware Control is a primary tool used to manage a domain.<br>See <i>Oracle Enterprise Manager Fusion Middleware Control</i> in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                                                              |
| Cluster               | A collection of multiple WebLogic Server instances running simultaneously and working together.<br>See <i>Overview of Managed Servers and Managed Server Clusters</i> in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                                                             |
| Machine               | A logical representation of the computer that hosts one or more WebLogic Server instances (servers). Machines are also the logical glue between the Managed Servers and the Node Manager. In order to start or stop the Managed Servers using the Node Manager, associate the Managed Servers with a machine. |
| Managed Server        | A host for your applications, application components, web services, and their associated resources.<br>See <i>Overview of Managed Servers and Managed Server Clusters</i> in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                                                         |

**Table 1-1 (Cont.) Description of Elements in Standard Installation Topologies**

| Element        | Description and Links to Related Documentation                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Infrastructure | <p>A collection of services that include the following:</p> <ul style="list-style-type: none"> <li>• Metadata repository (MDS) contains the metadata for Oracle Fusion Middleware components, such as the Oracle Application Developer Framework. See <i>What Is the Metadata Repository?</i> in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i>.</li> <li>• Oracle Application Developer Framework (Oracle ADF).</li> <li>• Oracle Web Services Manager (OWSM).</li> </ul> |

## About Installing Oracle User Messaging Service

Oracle User Messaging Service (UMS) is a software technology that enables two-way communication between users and deployed applications.

See Introduction to Oracle User Messaging Service in *Oracle Fusion Middleware Administering Oracle User Messaging Service*.

UMS is included in the Oracle Fusion Middleware Infrastructure distribution. It installs as part of the Oracle Fusion Middleware Infrastructure standard installation topology, as described in About Installing Oracle User Messaging Service (UMS) in *Oracle Fusion Middleware Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

UMS runtime components consist of an Oracle Fusion Middleware Configuration Wizard template and an Oracle Fusion Middleware schema, which is installed into a supported database by using the Repository Creation Utility (RCU).

For development, you can install and use Oracle JDeveloper 12c to develop applications that can take advantage of UMS features. See Introducing Oracle JDeveloper in *Oracle Fusion Middleware Installing Oracle JDeveloper*.

## About Oracle WebCenter Content Scale Up

Oracle WebCenter Content supports only one Inbound Refinery Managed Server per node per domain, and one WebCenter Content Managed Server per node, per domain.

You cannot scale up Inbound Refinery or WebCenter Content. To add Managed Servers in a cluster, see Scaling Out a Topology (Machine Scale Out) in the *Oracle Fusion Middleware High Availability Guide* to add a Managed Server to a new node.

## Using This Document to Extend an Existing Domain

The procedures in this guide describe how to create a new domain. The assumption is that no other Oracle Fusion Middleware products are installed on your system.

If you have installed and configured other Oracle Fusion Middleware products on your system (for example, Fusion Middleware Infrastructure, with a domain that is up and

running) and wish to extend the same domain to include Oracle WebCenter Content, see [Installing Multiple Products in the Same Domain](#).

# 2

## Preparing to Install and Configure Oracle WebCenter Content

To prepare for your Oracle WebCenter Content installation, verify that your system meets the basic requirements, then obtain the correct installation software.

- [Mandatory Steps for Installing WebCenter Content on Windows Operating Systems](#)  
There are three mandatory procedures that you must run before you install Oracle WebCenter Content.
- [Roadmap for Installing and Configuring the Standard Installation Topologies](#)  
Installing and configuration standard installation topology requires certain steps.
- [Roadmap for Verifying Your System Environment](#)  
Before you begin the installation and configuration process, you must verify your system environment.
- [Obtaining the Product Distribution](#)  
You can obtain the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content distribution on the Oracle Technology Network (OTN).
- [About Product Distributions](#)  
You create the initial Oracle WebCenter Content domain using the Oracle Fusion Middleware Infrastructure distribution, which contains both Oracle WebLogic Server software and Oracle Java Required Files (JRF) software.

### Mandatory Steps for Installing WebCenter Content on Windows Operating Systems

There are three mandatory procedures that you must run before you install Oracle WebCenter Content.

- [Disabling the 8.3 File Naming Convention on a Windows Operating System](#)  
Before you install Oracle WebCenter Content on a Windows Operating System, you must disable the 8.3 file naming convention (maximum 8-character file name and 3-character extension).
- [Downloading Visual C++ Libraries](#)  
WebCenter Content and Inbound Refinery require the Visual C++ libraries included in Microsoft's Visual C++ Redistributable Package.
- [Downloading Microsoft .Net Framework 4.x](#)  
The WinNativeConverter uses vb.Net code, so it requires Microsoft .NET Framework 4.x.



## Disabling the 8.3 File Naming Convention on a Windows Operating System

Before you install Oracle WebCenter Content on a Windows Operating System, you must disable the 8.3 file naming convention (maximum 8-character file name and 3-character extension).

If the WebCenter Content `weblayout` directory is on a file system with 8.3 semantics, the legacy 16-bit 8.3 file names conflict with revision labels, causing file loss.

To disable the 8.3 file naming convention on a Windows Operating System:

1. Open the Windows Registry Editor (`regedit`), and go to the following key:  
`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/FileSystem`
2. Set the value of the `NtfsDisable8dot3NameCreation` key to **1**.
3. Restart the Windows Operating System to make the change take effect.

## Downloading Visual C++ Libraries

WebCenter Content and Inbound Refinery require the Visual C++ libraries included in Microsoft's Visual C++ Redistributable Package.

You must download Microsoft Visual C++ 2013 that contain the libraries.

To download the package:

1. Go to the Microsoft Download Center at <http://www.microsoft.com/downloads>
2. Search for **Microsoft Visual C++ 2013 SP1 Redistributable Package (x64)**.
3. Download the `vc_redist_x64.exe` file.
4. Search for **Microsoft Visual C++ 2013 SP1 Redistributable Package (x86)**
5. Download the `vc_redist_x86.exe` file.

It is important to install the correct binary as per the system you are installing on. On a 32 bit machine, only the `vc_redist_x86.exe` is required. On a 64 bit machine, you need to install both `vc_redist_x86.exe` and `vc_redist_x64.exe`.



### Note:

For a list of platforms that support PDF Searchable Document Output Format, go to the Oracle Fusion Middleware Supported System Configurations page. In the table, on the row **Oracle Fusion Middleware 12c certifications**, select the **System Requirements and Supported Platforms for WebLogic Server 12c (12.2.1.4.0)** (.xls) file.

## Downloading Microsoft .Net Framework 4.x

The WinNativeConverter uses vb.Net code, so it requires Microsoft .NET Framework 4.x.

Download Microsoft .NET Framework 4.x at <http://www.microsoft.com/downloads>

## Roadmap for Installing and Configuring the Standard Installation Topologies

Installing and configuration standard installation topology requires certain steps.

This document has all steps required to install and configure standard installation topologies. The guide also refers to additional information that you can use if you want to create a modified version of this topology.

The following table shows the steps required to install and configure the topology.

**Table 2-1 Standard Installation Roadmap**

| Task                                                                                   | Description                                                                                                                                                                                    | Documentation                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verify your system environment                                                         | Before beginning the installation, verify that the minimum system and network requirements are met.                                                                                            | See <a href="#">Roadmap for Verifying Your System Environment</a> .                                                                                                                                                                                       |
| Check for any mandatory patches that will be required before or after the installation | Review the Oracle Fusion Middleware Infrastructure release notes to see if there are any mandatory patches required for the software products you are installing.                              | See Install and Configure in <i>Release Notes for Oracle Fusion Middleware Infrastructure</i> .                                                                                                                                                           |
| Obtain the appropriate distributions                                                   | Install Oracle Fusion Middleware Infrastructure to create the Oracle Home for Oracle WebCenter Content                                                                                         | See <a href="#">About Product Distributions</a> .                                                                                                                                                                                                         |
| Determine your installation directories                                                | Verify that the installer can access or create the installer directories that it must access or create. Also, verify that the directories exist on systems that meet the minimum requirements. | See What are the Key Oracle Fusion Middleware Directories? in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                                                                                                                    |
| Install prerequisite software                                                          | Install Oracle Fusion Middleware Infrastructure to create the Oracle home directory.                                                                                                           | For Oracle Fusion Middleware Infrastructure , see <i>Installing and Configuring the Oracle Fusion Middleware Infrastructure</i> . You only need to perform the installation for Infrastructure. You do not need to configure a domain for Infrastructure. |
| Install the software                                                                   | Run the Oracle Universal Installer to install Oracle WebCenter Content.<br><br>Installing the software transfers the software to your system and creates the Oracle home directory.            | See <a href="#">Installing the Oracle WebCenter Content Software</a> .                                                                                                                                                                                    |

**Table 2-1 (Cont.) Standard Installation Roadmap**

| Task                                                                | Description                                                                                                                                                           | Documentation                                                                                             |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Select a database profile and review any required custom variables. | Before you install required schemas in the database, review the information about any custom variables you will need to set for the Oracle WebCenter Content schemas. | See <a href="#">About Database Requirements for an Oracle Fusion Middleware Installation</a> .            |
| Create the schemas                                                  | Run the Repository Creation Utility to create the schemas required for configuration.                                                                                 | See <a href="#">Creating the Database Schemas</a> .                                                       |
| Create a WebLogic domain                                            | Use the Configuration Wizard to create and configure the WebLogic domain.                                                                                             | See <a href="#">Configuring the Domain</a> if you are creating the topology for Oracle WebCenter Content. |
| Administer and prepare your domain for high availability            | Discover additional tools and resources to administer your domain and configure your domain to be highly available.                                                   | See <a href="#">Next Steps After Configuring the Domain</a> .                                             |

## Roadmap for Verifying Your System Environment

Before you begin the installation and configuration process, you must verify your system environment.

[Table 2-2](#) identifies important tasks and checks to perform to ensure that your environment is prepared to install and configure Oracle WebCenter Content.

**Table 2-2 Roadmap for Verifying Your System Environment**

| Task                                                                  | Description                                                                                                                                              | Documentation                                                                                     |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Verify certification and system requirements.                         | Verify that your operating system is certified and configured for installation and configuration.                                                        | See <a href="#">Verifying Certification, System, and Interoperability Requirements</a> .          |
| Identify a proper installation user.                                  | Verify that the installation user has the required permissions to install and configure the software.                                                    | See <a href="#">Selecting an Installation User</a> .                                              |
| Select the installation and configuration directories on your system. | Verify that you can create the necessary directories to install and configure the software, according to the recommended directory structure.            | See <a href="#">Understanding Directories for Installation and Configuration</a> .                |
| Install a certified JDK.                                              | The installation program for the distribution requires a certified JDK present on your system.                                                           | See <a href="#">Understanding JDK Requirements for an Oracle Fusion Middleware Installation</a> . |
| Install and configure a database for mid-tier schemas.                | To configure your WebLogic domain, you must have access to a certified database that is configured for the schemas required by Oracle WebCenter Content. | See <a href="#">About Database Requirements for an Oracle Fusion Middleware Installation</a> .    |

- [Verifying Certification, System, and Interoperability Requirements](#)  
Oracle recommends that you use the certification matrix and system requirements documents with each other to verify that your environment meets the requirements for installation.
- [Selecting an Installation User](#)  
The user who installs and configures your system must have the required permissions and privileges.
- [Understanding Directories for Installation and Configuration](#)  
During the installation and domain configuration process, you must plan on providing the locations for these directories: Oracle home, Domain home, and the Application home.
- [Understanding JDK Requirements for an Oracle Fusion Middleware Installation](#)  
Most Fusion Middleware products are in `.jar` file format. These distributions do *not* include a JDK. To run a `.jar` distribution installer, you must have a certified JDK already installed on your system.
- [About Database Requirements for an Oracle Fusion Middleware Installation](#)  
Many Oracle Fusion Middleware products require database schemas prior to configuration. If you do not already have a database where you can install these schemas, you must install and configure a certified database.

## Verifying Certification, System, and Interoperability Requirements

Oracle recommends that you use the certification matrix and system requirements documents with each other to verify that your environment meets the requirements for installation.

### 1. Verifying that your environment meets certification requirements:

Make sure that you install your product on a supported hardware and software configuration. See the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page.

Oracle has tested and verified the performance of your product on all certified systems and environments. Whenever new certifications are released, they are added to the certification document right away. New certifications can be released at any time. Therefore, the certification documents are kept outside the documentation libraries and are available on Oracle Technology Network.

### 2. Using the system requirements document to verify certification:

Oracle recommends that you use the *Oracle Fusion Middleware System Requirements and Specifications* document to verify that the certification requirements are met. For example, if the certification document indicates that your product is certified for installation on 64-Bit Oracle Linux 6.5, use this document to verify that your system meets the required minimum specifications. These include disk space, available memory, specific platform packages and patches, and other operating system-specific requirements. System requirements can change in the future. Therefore, the system requirement documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

### 3. Verifying interoperability among multiple products:

To learn how to install and run multiple Fusion Middleware products from the same release or mixed releases with each other, see *Oracle Fusion Middleware 12c Interoperability and Compatibility* in *Oracle Fusion Middleware Understanding Interoperability and Compatibility*.

## Selecting an Installation User

The user who installs and configures your system must have the required permissions and privileges.

- [About User Permissions](#)  
The user who installs a Fusion Middleware product owns the files and has certain permissions on the files.
- [Understanding Non-Default User Permissions on UNIX Operating Systems](#)  
Changing the default permissions setting reduces the security of the installation and possibly your system. Oracle does not recommend changing default permission settings.
- [Verifying that the Installation User has Administrator Privileges on Windows Operating Systems](#)  
To update the Windows Registry, you must have administrator privileges.

## About User Permissions

The user who installs a Fusion Middleware product owns the files and has certain permissions on the files.

- Read and write permissions on all non-executable files (for example, `.jar`, `.properties`, or `.xml`). All other users in the same group as the file owner have read permissions only.
- Read, write, and execute permissions on all executable files (for example, `.exe`, `.sh`, or `.cmd`). All other users in the same group as the file owner have read and execute permissions only.

This means that someone other than the person who installs the software can use the installed binaries in the Oracle home directory to configure a domain or set of Fusion Middleware products.

During configuration, the files generated by the configuration process are owned by the user who ran the Configuration Wizard. This user has the same permissions as described above for the installation user. However, security-sensitive files are not created with group permissions. Only the user that created the domain has read and write permissions and can administer the domain.

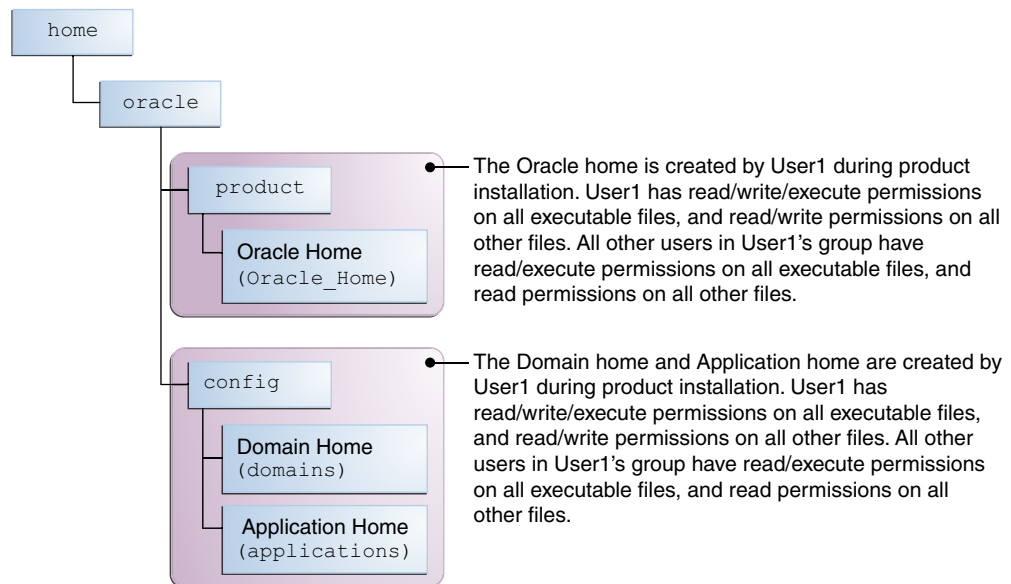
Consider the following examples:

- **Example 1: A Single User Installs the Software and Configures the Domain**

This example explains the file permissions where the same user installs the software and configures the domain.

To ensure proper permissions and privileges for all files, Oracle recommends that the same owner perform both tasks: install the Oracle Fusion Middleware product and configure the WebLogic Server domain by using the Configuration Wizard.

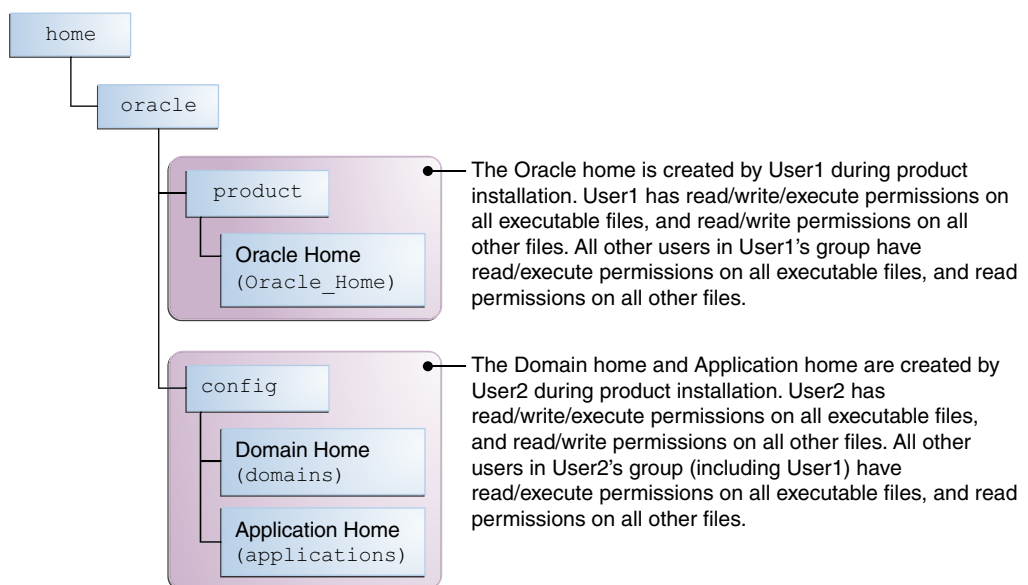
**Figure 2-1 Directory Structure when a Single User Installs the Software and Configures the Domain**



If the user who creates the domain is different than the user who installed the software, then both users must have the same privileges, as shown in the next example.

- **Example 2: The Oracle Home Directory and Domain are Created by Different Users**  
This example explains the file permissions where one user creates the Oracle home and another user configures the domain.

**Figure 2-2 Directory Structure when Different Users Install the Software and Configure the Domain**





**Note:**

Certain domain files do not have group permissions. For example, `cwallet.sso`.

Consider the following points before you run the installer:

- On UNIX operating systems, Oracle recommends that you set `umask` to `027` on your system before you install the software. This ensures that the file permissions are set properly during installation. Use the following command:  

```
umask 027
```

You must enter this command in the same terminal window from which you plan to run the product installer.
- On UNIX operating systems, do not run the installation program as a `root` user. If you run the installer as a root user, the startup validation may fail and you cannot continue the installation.
- When you manage a product installation (for example, applying patches or starting managed Servers), use the same user ID that you used to install the product.
- On Windows operating systems, you must have administrative privileges to install the product. See [Verifying the Installation User has Administrator Privileges on Windows Operating Systems](#).

## Understanding Non-Default User Permissions on UNIX Operating Systems

Changing the default permissions setting reduces the security of the installation and possibly your system. Oracle does not recommend changing default permission settings.

If other users require access to particular files or executable, consider using the UNIX `sudo` command (or other similar command) in lieu of changing file permissions.

Refer to your UNIX operating system Administrator's Guide or contact your operating system vendor if you need further assistance.

## Verifying that the Installation User has Administrator Privileges on Windows Operating Systems

To update the Windows Registry, you must have administrator privileges.

By default, users with the administrator privilege sign in to the system with regular privileges, but can request elevated permissions to perform administrative tasks.

To perform a task with elevated privileges:

1. Find the Command Prompt icon, either from the Start menu or the Windows icon in the lower-left corner.
2. Right-click **Command Prompt** and select **Run as administrator**.

This opens a new command prompt window, and all actions performed in this window are done with administrator privileges.

 **Note:**

If you have User Access Control enabled on your system, you may see an additional window asking you to confirm this action. Confirm and continue with this procedure.

3. Perform the desired task.

For example, to start the product installer:

For a jar file, enter:

```
java -jar distribution_name.jar
```

For an executable (.exe, .bin, or .sh file), enter:

```
distribution_name.exe
```

## Understanding Directories for Installation and Configuration

During the installation and domain configuration process, you must plan on providing the locations for these directories: Oracle home, Domain home, and the Application home.

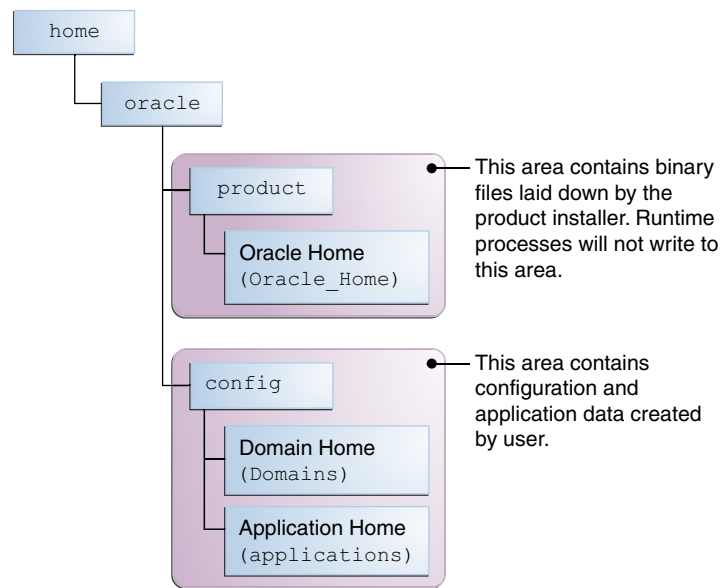
- [Understanding the Recommended Directory Structure](#)  
Oracle recommends specific locations for the Oracle Home, Domain Home, and Application Home.
- [About the Oracle Home Directory](#)  
When you install any Oracle Fusion Middleware product, you must use an Oracle home directory.
- [About the Domain Home Directory](#)  
The Domain home is the directory where domains that you configure are created.
- [About the Application Home Directory](#)  
The Application home is the directory where applications for domains you configure are created.
- [Installing Multiple Products in the Same Domain](#)  
There are two methods to install and configure multiple products in one domain. This is also known as *extending* a domain.
- [Preparing for Shared Storage](#)  
Oracle Fusion Middleware allows you to configure multiple WebLogic Server domains from a single Oracle home. This allows you to install the Oracle home in a single location on a shared volume and reuse the Oracle home for multiple host installations.

## Understanding the Recommended Directory Structure

Oracle recommends specific locations for the Oracle Home, Domain Home, and Application Home.

Oracle recommends a directory structure similar to the one shown in [Figure 2-3](#).



**Figure 2-3 Recommended Oracle Fusion Middleware Directory Structure**

A base location (Oracle base) should be established on your system (for example, `/home/oracle`) and from there, two separate branches should be created. The `product` directory should contain the product binary files and all of the Oracle home directories. The `config` directory should contain your domain and application data.

Oracle recommends that you do not keep your configuration data anywhere underneath the Oracle home; if you upgrade your product to another major release, you will be required to create a new Oracle home for binaries. You must also make sure that your configuration data exist in a location to which the binaries in the Oracle home have access.

The `/home/oracle/product` (for the Oracle home) and `/home/oracle/config` (for the application and configuration data) directories are used in examples throughout the documentation; be sure to replace these directories with the actual directories on your system.

## About the Oracle Home Directory

When you install any Oracle Fusion Middleware product, you must use an Oracle home directory.

This directory is a repository for common files that are used by multiple Fusion Middleware products installed on the same machine. These files ensure that Fusion Middleware operates correctly on your system. They facilitate checking of cross-product dependencies during installation. For this reason, you can consider the Oracle home directory a *central support directory* for all Oracle Fusion Middleware products installed on your system.

Fusion Middleware documentation refers to the Oracle home directory as `ORACLE_HOME`.

### Oracle Home Considerations

Keep the following in mind when you create the Oracle home directory and install Fusion Middleware products:

- Do not include spaces in the name of your Oracle home directory; the installer displays an error message if your Oracle home directory path contains spaces.
- You can install only one instance of each Oracle Fusion Middleware product in a single Oracle home directory. If you need to maintain separate versions of a product on the same machine, each version must be in its own Oracle home directory.

Although you can have several different products in a single Oracle home, only one version of each product can be in the Oracle home.

### Multiple Home Directories

Although in most situations, a single Oracle home directory is sufficient, it is possible to create more than one Oracle home directory. For example, you need to maintain multiple Oracle home directories in the following situations:

- You prefer to maintain separate development and production environments, with a separate product stack for each. With two directories, you can update your development environment without modifying the production environment until you are ready to do so.
- You want to maintain two different versions of a Fusion Middleware product at the same time. For example, you want to install a new version of a product while keeping your existing version intact. In this case, you must install each product version in its own Oracle home directory.
- You need to install multiple products that are not compatible with each other. See Oracle Fusion Middleware 12c (12.2.1.4.0) Interoperability and Compatibility in *Oracle Fusion Middleware Understanding Interoperability and Compatibility*.



#### Note:

If you create more than one Oracle home directory, you must provide non-overlapping port ranges during the configuration phase for each product.

## About the Domain Home Directory

The Domain home is the directory where domains that you configure are created.

The default Domain home location is `ORACLE_HOME/user_projects/domains/domain_name`. However, Oracle strongly recommends that you do not use this default location. Put your Domain home *outside* of the Oracle home directory, for example, in `/home/oracle/config/domains`. The `config` directory should contain domain and application data. Oracle recommends a separate domain directory so that new installs, patches, and other operations update the `ORACLE_HOME` only, *not* the domain configuration.

See [Understanding the Recommended Directory Structure](#) for more on the recommended directory structure and locating your Domain home.

Fusion Middleware documentation refers to the Domain home directory as `DOMAIN_HOME` and includes all folders up to and including the domain name. For example, if you name your domain `exampledomain` and locate your domain data in the `/home/oracle/config/domains` directory, the documentation would use `DOMAIN_HOME` to refer to `/home/oracle/config/domains/exampledomain`.

## About the Application Home Directory

The Application home is the directory where applications for domains you configure are created.

The default Application home location is `ORACLE_HOME/user_projects/applications/domain_name`. However, Oracle strongly recommends that you locate your Application home *outside* of the Oracle home directory; if you upgrade your product to another major release, you must create a new Oracle home for binaries.

See [Understanding the Recommended Directory Structure](#) for more on the recommended directory structure and locating your Application home..

Fusion Middleware documentation refers to the Application home directory as `APPLICATION_HOME` and includes all folders up to and including the domain name. For example, if you name your domain `exampledomain` and you locate your application data in the `/home/oracle/config/applications` directory, the documentation uses `APPLICATION_HOME` to refer to `/home/oracle/config/applications/exampledomain`.

## Installing Multiple Products in the Same Domain

There are two methods to install and configure multiple products in one domain. This is also known as *extending* a domain.

- **Method 1.**

Install and configure Product A, including creating the schemas and starting all servers in the domain to verify a successful domain configuration.

This is the method used in all installation guides in the Fusion Middleware library. You can repeat this process for as many products as necessary. It allows you to validate one product at a time and add more products incrementally.

To install Product B in the same domain as Product A:

1. Stop all servers to prevent any updates to the domain while you add the new product.

See *Starting and Stopping Oracle Fusion Middleware in Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

2. Follow the instructions in the installation guide for Product B, including creating the necessary schemas.
3. Run the Configuration Wizard to configure the domain.

During configuration, the Configuration Wizard automatically detects the components that have been installed and offers you the option to extend the existing Product A domain to include Product B.

- **Method 2.**

Install all of the required products, then create the schemas for all of the products. After you create the schemas, configure the domain by using the necessary product templates, then start all the servers.

This method of creating a multi-product domain may be slightly faster than Method 1; however, the installation guides in the Fusion Middleware library do not provide specific instructions for this method of domain creation.

 **See Also:**

- To update WebLogic domains, see *Updating WebLogic Domains in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.
- For important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products, see Oracle Fusion Middleware 12c (12.2.1.4.0) Interoperability and Compatibility in *Oracle Fusion Middleware Understanding Interoperability and Compatibility*.

## Preparing for Shared Storage

Oracle Fusion Middleware allows you to configure multiple WebLogic Server domains from a single Oracle home. This allows you to install the Oracle home in a single location on a shared volume and reuse the Oracle home for multiple host installations.

If you plan to use shared storage in your environment, see *Using Shared Storage in Oracle Fusion Middleware High Availability Guide* for more information.

## Understanding JDK Requirements for an Oracle Fusion Middleware Installation

Most Fusion Middleware products are in `.jar` file format. These distributions do *not* include a JDK. To run a `.jar` distribution installer, you must have a certified JDK already installed on your system.

Make sure that the JDK is installed *outside* of the Oracle home. If you install the JDK under the Oracle home, you will encounter problems when you try to perform tasks in the future. Oracle Universal Installer validates that the Oracle home directory is empty; the install will not progress until you specify an empty directory. Oracle recommends that you locate your JDK installation in the `/home/oracle/products/jdk` directory.

Some products (such as Oracle HTTP Server and Oracle JDeveloper) are available as **platform-specific distributions**. Platform-specific distributions have a `.bin` (for UNIX operating systems) or `.exe` (for Windows operating systems) installer; in these cases, a platform-specific JDK is in the distribution and you do not need to install a JDK separately. However, you may need to upgrade this JDK to a more recent version, depending on the JDK versions that are certified.

Always verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page. For 12c (12.2.1.4.0), the certified JDK is 1.8.0\_211 and later.

To download the required JDK, navigate to the following URL and download the Java SE JDK:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

## About Database Requirements for an Oracle Fusion Middleware Installation

Many Oracle Fusion Middleware products require database schemas prior to configuration. If you do not already have a database where you can install these schemas, you must install and configure a certified database.

To find a certified database for your operating system, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page on the Oracle Technology Network (OTN).

To make sure that your database is properly configured for schema creation, see *Repository Creation Utility Requirements* in the *Oracle Fusion Middleware System Requirements and Specifications* document.

After your database is properly configured, you use the Repository Creation Utility (RCU) to create product schemas in your database. This tool is available in the Oracle home for your Oracle Fusion Middleware product. See About the Repository Creation Utility in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

## Obtaining the Product Distribution

You can obtain the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content distribution on the Oracle Technology Network (OTN).

To prepare to install Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content:

1. Enter `java -version` on the command line to verify that a certified JDK is installed on your system. For 12c (12.2.1.4.0), the certified JDK is 1.8.0\_211 and later.

See [Understanding JDK Requirements for an Oracle Fusion Middleware Installation](#).

2. Locate and download the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content software.

See Obtaining Product Distributions in *Oracle Fusion Middleware Planning an Installation of Oracle Fusion Middleware*.

## About Product Distributions

You create the initial Oracle WebCenter Content domain using the Oracle Fusion Middleware Infrastructure distribution, which contains both Oracle WebLogic Server software and Oracle Java Required Files (JRF) software.

Oracle JRF software consists of:

- Oracle Web Services Manager
- Oracle Application Development Framework (Oracle ADF)
- Oracle Enterprise Manager Fusion Middleware Control
- Repository Creation Utility (RCU)

- Other libraries and technologies required to support Oracle Fusion Middleware products
- Installing Oracle Fusion Middleware Infrastructure is a prerequisite to installing Oracle WebCenter Content.

# 3

## Installing the Oracle WebCenter Content Software

Follow the steps in this section to install the Oracle WebCenter Content software. Before beginning the installation, ensure that you have verified the prerequisites and completed all steps covered in [Preparing to Install and Configure Oracle WebCenter Content](#).

- [Verifying the Installation Checklist](#)  
The installation process requires specific information.
- [Starting the Installation Program](#)  
Before running the installation program, you must verify the JDK and prerequisite software is installed.
- [Navigating the Installation Screens](#)  
The installer shows a series of screens where you verify or enter information.
- [Verifying the Installation](#)  
After you complete the installation, verify whether it was successful by completing a series of tasks.

### Verifying the Installation Checklist

The installation process requires specific information.

[Table 3-1](#) lists important items that you must know before, or decide during, Oracle WebCenter Content installation.

**Table 3-1 Installation Checklist**

| Information           | Example Value                      | Description                                                                                            |
|-----------------------|------------------------------------|--------------------------------------------------------------------------------------------------------|
| JAVA_HOME             | /home/Oracle/Java/<br>jdk1.8.0_211 | Environment variable that points to the Java JDK home directory.                                       |
| Database host         | examplehost.exampledomain          | Name and domain of the host where the database is running.                                             |
| Database port         | 1521                               | Port number that the database listens on. The default Oracle database listen port is 1521.             |
| Database service name | orcl.exampledomain                 | Oracle databases require a unique service name. The default service name is orcl.                      |
| DBA username          | SYS                                | Name of user with database administration privileges. The default DBA user on Oracle databases is SYS. |

**Table 3-1 (Cont.) Installation Checklist**

| Information                                      | Example Value                                    | Description                                                                                                                                                            |
|--------------------------------------------------|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DBA password                                     | myDBApw957                                       | Password of the user with database administration privileges.                                                                                                          |
| <i>ORACLE_HOME</i>                               | /home/Oracle/product/<br>ORACLE_HOME             | Directory in which you will install your software.<br><br>This directory will include Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content, as needed. |
| WebLogic Server hostname                         | examplehost.exampledomain                        | Host name for Oracle WebLogic Server and Oracle WebCenter Content consoles.                                                                                            |
| Console port                                     | 7001                                             | Port for Oracle WebLogic Server and Oracle WebCenter Content consoles.                                                                                                 |
| <i>DOMAIN_HOME</i>                               | /home/Oracle/config/<br>domains/wcc_domain       | Location in which your domain data is stored.                                                                                                                          |
| <i>APPLICATION_HOME</i>                          | /home/Oracle/config/<br>applications/wcc_domain  | Location in which your application data is stored.                                                                                                                     |
| Administrator user name for your WebLogic domain | weblogic                                         | Name of the user with Oracle WebLogic Server administration privileges. The default administrator user is weblogic.                                                    |
| Administrator user password                      | myADMpw902                                       | Password of the user with Oracle WebLogic Server administration privileges.                                                                                            |
| RCU                                              | <i>ORACLE_HOME</i> /<br>oracle_common/bin        | Path to the Repository Creation Utility (RCU).                                                                                                                         |
| RCU schema prefix                                | SHORT PRODUCT NAME                               | Prefix for names of database schemas used by Oracle WebCenter Content.                                                                                                 |
| RCU schema password                              | myRCUpw674                                       | Password for the database schemas used by Oracle WebCenter Content.                                                                                                    |
| Configuration utility                            | <i>ORACLE_HOME</i> /<br>oracle_common/common/bin | Path to the Configuration Wizard for domain creation and configuration.                                                                                                |

## Starting the Installation Program

Before running the installation program, you must verify the JDK and prerequisite software is installed.

To start the installation program:

1. Sign in to the host system.



2. If you have not already done so, verify that a certified JDK is installed on your system: enter `java -version` on the command line. For 12c (12.2.1.4.0), the certified JDK is 1.8.0\_211 and later.  
  
For more information about JDK requirements, see [Understanding JDK Requirements for an Oracle Fusion Middleware Installation](#).
3. Verify that you have installed all prerequisite software, such as Oracle Fusion Middleware Infrastructure.
4. Go to the directory where you downloaded the installation program.
5. Start the installation program by running the `java` executable from the JDK directory. For example:
  - (UNIX) `/home/Oracle/Java/jdk1.8.0_211/bin/java -jar fmw_12.2.1.4.0_wccontent.jar`
  - (Windows) `C:\home\Oracle\Java\jdk1.8.0_211\bin\java -jar fmw_12.2.1.4.0_wccontent.jar`

**Note:**

You can also start the installer in silent mode using a saved response file instead of launching the installer screens. For more about silent or command line installation, see *Using the Oracle Universal Installer in Silent Mode* in *Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

When the installation program appears, you are ready to begin the installation.

## Navigating the Installation Screens

The installer shows a series of screens where you verify or enter information.

The following table lists the order in which installer screens appear. If you need additional help with an installation screen, click **Help**.

**Table 3-2 Oracle WebCenter Content Install Screens**

| Screen                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installation Inventory Setup | On UNIX operating systems, this screen opens if this is the first time you are installing any Oracle product on this host. 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.<br><br>See <i>About the Oracle Central Inventory</i> in <i>Oracle Fusion Middleware Installing Software with the Oracle Universal Installer</i> .<br><br>This screen does not appear on Windows operating systems. |
| Welcome                      | Review the information to make sure that you have met all the prerequisites, then click <b>Next</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Auto Updates                 | Select to skip automatic updates, select patches, or search for the latest software updates, including important security updates, through your My Oracle Support account.                                                                                                                                                                                                                                                                                                                                                                          |

**Table 3-2 (Cont.) Oracle WebCenter Content Install Screens**

| Screen                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installation Location | Specify your Oracle home directory location.<br>You can click <b>View</b> to verify and ensure that you are installing Oracle WebCenter Content in the correct Oracle home.                                                                                                                                                                                                                                                                                                             |
| Installation Type     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Prerequisite Checks   | This screen verifies that your system meets the minimum necessary requirements.<br>To view the list of tasks that gets verified, select <b>View Successful Tasks</b> . To view log details, select <b>View Log</b> . If any prerequisite check fails, then an error message appears at the bottom of the screen. Fix the error and click <b>Rerun</b> to try again. To ignore the error or the warning message and continue with the installation, click <b>Skip</b> (not recommended). |
| Installation Progress | This screen shows the installation progress.<br>When the progress bar reaches 100% complete, click <b>Finish</b> to dismiss the installer, or click <b>Next</b> to see a summary.                                                                                                                                                                                                                                                                                                       |
| Installation Complete | This screen displays the Installation Location and the Feature Sets that are installed.<br>Review this information and click <b>Finish</b> to close the installer.                                                                                                                                                                                                                                                                                                                      |

## Verifying the Installation

After you complete the installation, verify whether it was successful by completing a series of tasks.

- [Reviewing the Installation Log Files](#)  
Review the contents of the installation log files to make sure that the installer did not encounter any problems.
- [Checking the Directory Structure](#)  
The contents of your installation vary based on the options that you selected during the installation.
- [Viewing the Contents of the Oracle Home](#)  
You can view the contents of the Oracle home directory by using the `viewInventory` script.

## Reviewing the Installation Log Files

Review the contents of the installation log files to make sure that the installer did not encounter any problems.

By default, the installer writes logs files to the `Oracle_Inventory_Location/logs` (on UNIX operating systems) or `Oracle_Inventory_Location\logs` (on Windows operating systems) directory.

For a description of the log files and where to find them, see *Installation Log Files in Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

## Checking the Directory Structure

The contents of your installation vary based on the options that you selected during the installation.

See *What Are the Key Oracle Fusion Middleware Directories?* in *Oracle Fusion Middleware Understanding Oracle Fusion Middleware*.

## Viewing the Contents of the Oracle Home

You can view the contents of the Oracle home directory by using the `viewInventory` script.

See *Viewing the Contents of an Oracle Home* in *Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

# 4

## Configuring WebCenter Content Domain

After you have installed WebCenter Content, you can configure the domain, which you can also extend for high availability.

The configuration steps presented here assume that you have completed the installation steps covered in:

- [Preparing to Install and Configure Oracle WebCenter Content](#)
- [Installing the Oracle WebCenter Content Software](#)

Refer to the following sections to create the database schemas, configure a WebLogic domain, and verify the configuration:

- [Creating the Database Schemas](#)  
Before you can configure an Oracle WebCenter Content domain, you must install required schemas on a certified database for use with this release of Oracle Fusion Middleware.
- [Configuring the Domain](#)  
Use the Configuration Wizard to create and configure a domain.
- [Starting the Servers](#)  
After configuration is complete, start Node Manager, then the WebLogic Administration Server and Managed Servers.
- [Verifying the Configuration](#)  
After completing all configuration steps, you can perform additional steps to verify that your domain is properly configured.
- [Configuring Inbound Refinery Settings \(Single Node\)](#)  
After you start the Inbound Refinery Managed Servers, configure the settings on the post-installation configuration screen. In most cases, you can accept the default settings.
- [Configuring WebCenter Content Settings](#)  
You must complete the WebCenter Content configuration on the post-installation configuration page in Content Server.

### Creating the Database Schemas

Before you can configure an Oracle WebCenter Content domain, you must install required schemas on a certified database for use with this release of Oracle Fusion Middleware.

- [Installing and Configuring a Certified Database](#)  
Before you create the database schemas, you must install and configure a certified database, and verify that the database is up and running.
- [Starting the Repository Creation Utility](#)  
Start the Repository Creation Utility (RCU) after you verify that a certified JDK is installed on your system.
- [Navigating the Repository Creation Utility Screens to Create Schemas](#)  
Enter required information in the RCU screens to create the database schemas.

## Installing and Configuring a Certified Database

Before you create the database schemas, you must install and configure a certified database, and verify that the database is up and running.



### Note:

For an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), you must modify the wallet settings and set the environment variables, and apply patches on `ORACLE_HOME`. For more information, see [Settings to connect to Autonomous Transaction Processing Database and Applying Patches on ORACLE HOME](#).

See [About Database Requirements for an Oracle Fusion Middleware Installation](#).

## Starting the Repository Creation Utility

Start the Repository Creation Utility (RCU) after you verify that a certified JDK is installed on your system.

To start the RCU:

1. Verify that a certified JDK already exists on your system by running `java -version` from the command line. For 12c (12.2.1.4.0), the certified JDK is 1.8.0\_211 and later.

See [Understanding JDK Requirements for an Oracle Fusion Middleware Installation](#).

2. Ensure that the `JAVA_HOME` environment variable is set to the location of the certified JDK. For example:

- (UNIX) `setenv JAVA_HOME /home/Oracle/Java/jdk1.8.0_211`
- (Windows) `set JAVA_HOME=C:\home\Oracle\Java\jdk1.8.0_211`

3. Change to the following directory:

- (UNIX) `ORACLE_HOME/oracle_common/bin`
- (Windows) `ORACLE_HOME\oracle_common\bin`

4. Enter the following command:

- (UNIX) `./rcu`
- (Windows) `rcu.bat`

## Navigating the Repository Creation Utility Screens to Create Schemas

Enter required information in the RCU screens to create the database schemas.

- [Introducing the RCU](#)  
The Welcome screen is the first screen that appears when you start the RCU.
- [Selecting a Method of Schema Creation](#)  
Use the Create Repository screen to select a method to create and load component schemas into the database.
- [Providing Database Connection Details](#)  
On the Database Connection Details screen, provide the database connection details for the RCU to connect to your database.
- [Specifying a Custom Prefix and Selecting Schemas](#)  
You must enter a custom prefix to group schemas together, then select schemas you need. You can select the required schema on the Select Components screen.
- [Specifying Schema Passwords](#)  
On the Schema Passwords screen, specify how you want to set the schema passwords on your database, then enter and confirm your passwords.
- [Completing Schema Creation](#)  
Navigate through the remaining RCU screens to complete schema creation.

## Introducing the RCU

The Welcome screen is the first screen that appears when you start the RCU.

Click **Next**.

## Selecting a Method of Schema Creation

Use the Create Repository screen to select a method to create and load component schemas into the database.

On the Create Repository screen:

- If you have the necessary permissions and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have SYSDBA privileges.
- If you do *not* have the necessary permissions or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option generates a SQL script that you can give to your database administrator. See *About System Load and Product Load in Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.
- If the DBA has already run the SQL script for System Load, select **Perform Product Load**.

### Note:

For an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), you must create schemas as a `Normal` user, and though, you do not have full SYS or SYSDBA privileges on the database, you must select **System Load and Product Load**.

## Providing Database Connection Details

On the Database Connection Details screen, provide the database connection details for the RCU to connect to your database.

### Note:

If you are unsure of the database service name, you can obtain it from the `SERVICE_NAMES` parameter in the initialization parameter file of the database. If the initialization parameter file does not contain the `SERVICE_NAMES` parameter, then the service name is the same as the global database name, which is specified in the `DB_NAME` and `DB_DOMAIN` parameters.

For an Oracle Autonomous Transaction Processing-Shared (ATP-S) database, use the database service name, `<databasename>_tpurgent` or `<databasename>_tp`, specified in `tnsnames.ora`. For service name details, see Database Service Names for Autonomous Transaction Processing and Autonomous JSON Database in *Using Oracle Autonomous Database on Shared Exadata Infrastructure*.

To create schemas on an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), you can specify the connection credentials using only the **Connection String** option. In this screen, a warning message is displayed. You can ignore the warning and continue with the schema creation. For more information, see SYS DBA Privileges Warning After Applying Patches.

To provide the database connection details:

1. On the Database Connection Details screen, provide the database connection details.  
For example:

```
Database Type: Oracle Database
Connection String Format: Connection Parameters or Connection
String
Connection String:
examplehost.exampledomain.com:1521:Orcl.exampledomain.com
Host Name: examplehost.exampledomain.com
Port: 1521
Service Name: Orcl.exampledomain.com
User Name: sys
Password: *****
Role: SYSDBA
```

For an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), enter connect string in the following format:

```
jdbc:oracle:thin:@TNS_alias?TNS_ADMIN=<path of the wallet files,
ojdbc.properties, and tnsnames.ora>
```

In the connect string, you must pass `TNS_alias` as the database name found in `tnsnames.ora`, and `TNS_ADMIN` property to the location of the wallet files, `ojdbc.properties`, and `tnsnames.ora`.

 **Note:**

For an Oracle Autonomous Transaction Processing-Shared (ATP-S) database, you must use only one of the database service names, `<dbname>_tpurgent` or `<dbname>_tp`, specified in `tnsnames.ora`. For database service name details, see Database Service Names for Autonomous Transaction Processing and Autonomous JSON Database in *Using Oracle Autonomous Database on Shared Exadata Infrastructure*.

Example connect string for Oracle Autonomous Transaction Processing-Dedicated (ATP-D) database::

```
jdbc:oracle:thin:@dbname_medium?TNS_ADMIN=/users/test/wallet_dbname/
```

Example connect string for Oracle Autonomous Transaction Processing-Shared (ATP-S) database:

```
jdbc:oracle:thin:@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/
```

2. Click **Next** to proceed, then click **OK** in the dialog window that confirms a successful database connection.

## Specifying a Custom Prefix and Selecting Schemas

You must enter a custom prefix to group schemas together, then select schemas you need. You can select the required schema on the Select Components screen.

Select **Create new prefix**, specify a custom prefix, then select the **WebCenter Content** schema. This action automatically selects the following schemas as dependencies:

- Oracle WebCenter Content Server - Complete
- Oracle WebCenter Enterprise Capture
- Oracle WebCenter Content Server - Search Only
- Oracle WebCenter Content: Imaging

The following schemas are selected by default:

- Metadata Services
- Oracle Platform Security Services
- Audit Services
- Audit Services Append
- Audit Services Viewer





**Tip:**

You must make a note of the custom prefix you choose to enter here; you will need this later on during the domain creation process.



**Note:**

If you install WebCenter Content only and select the **Oracle WebCenter Content Server - Complete** schema (but no other schemas), you must select the **Metadata Services** schema. You must select **Metadata Services** because WebCenter Content User Interface requires it.

To create schemas for Imaging, select **Oracle WebCenter Content: Imaging**, and also select **Oracle WebCenter Content Server - Complete** to use WebCenter Content as the Imaging repository.

For Oracle Web Services Manager (Oracle WSM) Policy Manager, or for using Imaging with Oracle SOA Suite, expand AS Common Schemas and select Metadata Services.

The schema Common Infrastructure Services is also created automatically. It enables you to retrieve information from RCU during domain configuration. This schema is grayed out; you cannot select or deselect it. For more details, see Understanding the Service Table Schema in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

The custom prefix logically groups these schemas together for use in this domain only; you must create a unique set of schemas for each domain because schema sharing across domains is not supported.



**Tip:**

For more details about custom prefixes, see Understanding Custom Prefixes in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

To organize your schemas in a multi-domain environment, see Planning Your Schema Creation in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, then click **OK** on the dialog window confirming that prerequisite checking for schema creation was successful.

## Specifying Schema Passwords

On the Schema Passwords screen, specify how you want to set the schema passwords on your database, then enter and confirm your passwords.



### Note:

For an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), the schema password must be minimum 12 characters, and must contain at least one uppercase, one lower case, and one number.

You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

Click **Next**.

## Completing Schema Creation

Navigate through the remaining RCU screens to complete schema creation.

On the Map Tablespaces screen, the Encrypt Tablespace check box appears *only* if you enabled Transparent Data Encryption (TDE) in the database (Oracle or Oracle EBR) when you start the RCU.

To complete schema creation:

1. On the Map Tablespaces screen, select **Encrypt Tablespace** if you want to encrypt all new tablespaces that the RCU creates.
2. In the Completion Summary screen, click **Close** to dismiss the RCU.

For an Oracle Autonomous Transaction Processing-Shared (ATP-S) database, in the **Map Tablespaces** screen you must override the default tablespaces and the temporary tablespaces, and also override the additional tablespaces, if applicable. See Map Tablespaces.

If you encounter any issues when you create schemas on an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), see Troubleshooting Tips for Schema Creation on an Autonomous Transaction Processing Database in *Creating Schemas with the Repository Creation Utility* and Issues Related to Product Installation and Configuration on an Autonomous Database in *Release Notes for Oracle Fusion Middleware Infrastructure*.

## Configuring the Domain

Use the Configuration Wizard to create and configure a domain.

For information on other methods to create domains, see Additional Tools for Creating, Extending, and Managing WebLogic Domains in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

- [Starting the Configuration Wizard](#)  
Start the Configuration Wizard to begin configuring a domain.
- [Navigating the Configuration Wizard Screens to Create and Configure the Domain](#)  
Enter required information in the Configuration Wizard screens to create and configure the domain for the topology.

## Starting the Configuration Wizard

Start the Configuration Wizard to begin configuring a domain.

To start the Configuration Wizard:

1. Change to the following directory:  
(UNIX) `ORACLE_HOME/oracle_common/common/bin`  
(Windows) `ORACLE_HOME\oracle_common\common\bin`  
where `ORACLE_HOME` is your 12c (12.2.1.4.0) Oracle home.
2. Enter the following command:  
(UNIX) `./config.sh`  
(Windows) `config.cmd`

## Navigating the Configuration Wizard Screens to Create and Configure the Domain

Enter required information in the Configuration Wizard screens to create and configure the domain for the topology.



### Note:

You can use this procedure to extend an existing domain. If your needs do not match the instructions in the procedure, be sure to make your selections accordingly, or see the supporting documentation for more details.

- [Selecting the Domain Type and Domain Home Location](#)  
Use the Configuration Type screen to select a Domain home directory location, optimally outside the Oracle home directory.
- [Selecting Configuration Templates for Oracle WebCenter Content](#)
- [Configuring High Availability Options](#)  
Use this screen to configure service migration and persistence settings that affect high availability. This screen appears for the first time when you create a cluster that uses automatic service migration, persistent stores, or both, and all subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.
- [Selecting the Application Home Location](#)  
Use the Application Location screen to select the location to store applications associated with your domain, also known as the *Application home* directory.

- [Configuring the Administrator Account](#)  
Use the Administrator Account screen to specify the user name and password for the default WebLogic Administrator account for the domain.
- [Specifying the Domain Mode and JDK](#)  
Use the Domain Mode and JDK screen to specify the domain mode and Java Development Kit (JDK).
- [Specifying JDBC Data Sources](#)  
Use this screen to specify JDBC Data Sources.
- [Testing the JDBC Data Source](#)  
Use this screen to test the data source connections you configured in the previous screens.
- [Specifying the Database Configuration Type](#)  
Use the Database Configuration type screen to specify details about the database and database schema.
- [Specifying JDBC Component Schema Information](#)  
Use the JDBC Component Schema screen to verify or specify details about the database schemas.
- [Testing the JDBC Connections](#)  
Use the JDBC Component Schema Test screen to test the data source connections.
- [Entering Credentials](#)  
Use the Credentials screen to set credentials for each key in the domain.
- [Selecting Advanced Configuration](#)  
Use the Advanced Configuration screen to complete the domain configuration.
- [Configuring the Administration Server Listen Address](#)  
Use the Administration Server screen to select the IP address of the host.
- [Configuring Node Manager](#)  
Use the Node Manager screen to select the type of Node Manager you want to configure, along with the Node Manager credentials.
- [Configuring Managed Servers for Oracle WebCenter Content](#)  
You create and configure new Managed Servers on the Managed Servers Screen.
- [Configuring a Cluster for WebCenter Content](#)  
Use the Clusters screen to create a new cluster.
- [Defining Server Templates](#)  
If you are creating dynamic clusters for a high availability setup, use the Server Templates screen to define one or more server templates for domain.
- [Configuring Dynamic Servers](#)  
If you are creating dynamic clusters for a high availability setup, use the Dynamic Servers screen to configure the dynamic servers.
- [Assigning WebCenter Content Managed Servers to the Cluster](#)  
Use the Assign Servers to Clusters screen to assign Managed Servers to a new *configured cluster*. A configured cluster is a cluster you configure manually. You do not use this screen if you are configuring a *dynamic cluster*, a cluster that contains one or more generated server instances that are based on a server template.
- [Configuring Coherence Clusters](#)  
Use the Coherence Clusters screen to configure the Coherence cluster.

- [Creating a New WebCenter Content Machine](#)  
Use the Machines screen to create new machines in the domain. A machine is required so that Node Manager can start and stop servers.
- [Assigning Servers to WebCenter Content Machines](#)  
Use the Assign Servers to Machines screen to assign the Administration Server and Managed Servers to the new machine you just created.
- [Virtual Targets](#)  
If you have a WebLogic Server Multitenant (MT) environment, you use the Virtual Targets screen to add or delete virtual targets. For this installation (not a WebLogic Server MT environment), you do not enter any values; just select **Next**.
- [Partitions](#)  
The Partitions screen is used to configure partitions for virtual targets in WebLogic Server Multitenant (MT) environments. Select **Next** without selecting any options.
- [Reviewing Your Configuration Specifications and Configuring the Domain](#)  
The Configuration Summary screen shows detailed configuration information for the domain you are about to create.
- [Writing Down Your Domain Home and Administration Server URL](#)  
The End of Configuration screen shows information about the domain you just configured.

## Selecting the Domain Type and Domain Home Location

Use the Configuration Type screen to select a Domain home directory location, optimally outside the Oracle home directory.

Oracle recommends that you locate your Domain home in accordance with the directory structure in *What Are the Key Oracle Fusion Middleware Directories?* in *Oracle Fusion Middleware Understanding Oracle Fusion Middleware*, where the Domain home is located outside the Oracle home directory. This directory structure helps avoid issues when you need to upgrade or reinstall software.

To specify the Domain type and Domain home directory:

1. On the Configuration Type screen, select **Create a new domain**.
2. In the Domain Location field, specify your Domain home directory.

For more details about this screen, see Configuration Type in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Selecting Configuration Templates for Oracle WebCenter Content

On the Templates screen, make sure **Create Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Inbound Refinery - 12.2.1.4.0[wcccontent]**
- **Oracle Universal Content Management - Content Server - 12.2.1.4.0 [wcccontent]**

Selecting this template automatically selects the following as dependencies:

- Oracle Enterprise Manager - 12.2.1.4.0 [em]
- Oracle JRF - 12.2.1.4.0 [oracle\_common]

- WebLogic Coherence Cluster Extension - 12.2.1.4.0 [wlserver]
- **Oracle WebCenter Enterprise Capture - 12.2.1.4.0 [wccapture]**
- **Oracle WebCenter Content - Web UI - 12.2.1.4.0 [wccontent]**
- Oracle WebCenter Content: Imaging

**Tip:**

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

## Configuring High Availability Options

Use this screen to configure service migration and persistence settings that affect high availability. This screen appears for the first time when you create a cluster that uses automatic service migration, persistent stores, or both, and all subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.

### Enable Automatic Service Migration

Select **Enable Automatic Service Migration** to enable pinned services to migrate automatically to a healthy Managed Server for failover. It configures migratable target definitions that are required for automatic service migration and the cluster leasing. Choose one of these cluster leasing options:

- **Database Leasing** - Managed Servers use a table on a valid JDBC System Resource for leasing. Requires that the Automatic Migration data source have a valid JDBC System Resource. If you select this option, the Migration Basis is configured to Database and the Data Source for Automatic Migration is also automatically configured by the Configuration Wizard. If you have a high availability database, such as Oracle RAC, to manage leasing information, configure the database for server migration according to steps in [High-availability Database Leasing](#).
- **Consensus Leasing** - Managed Servers maintain leasing information in-memory. You use Node Manager to control Managed Servers in a cluster. (All servers that are migratable, or which could host a migratable target, must have a Node Manager associated with them.) If you select this option, the Migration Basis is configured to Consensus by the Configuration Wizard.

See Leasing for more information on leasing.

See Service Migration for more information on Automatic Service Migration.

### JTA Transaction Log Persistence

This section has two options: **Default Persistent Store** and **JDBC TLog Store**.

- **Default Persistent Store** - Configures the JTA Transaction Log store of the servers in the default file store.
- **JDBC TLog Store** - Configures the JTA Transaction Log store of the servers in JDBC stores.

Oracle recommends that you select **JDBC TLog Store**. When you complete the configuration, you have a cluster where JDBC persistent stores are set up for Transaction logs.

For more details on persistent and TLOG stores, see the following topics in *Oracle Fusion Middleware Developing JTA Applications for Oracle WebLogic Server*:

- Using the Default Persistent Store
- Using a JDBC TLOG Store

### JMS Service Persistence

A persistent **JMS store** is a physical repository for storing persistent message data and durable subscribers. It can be either a disk-based **file store** or a JDBC-accessible database. You can use a **JMS file store** for paging of messages to disk when memory is exhausted.

- JMS File Store - Configures a component to use JMS File Stores. If you select this option, you can choose the **File Store** option in the Advanced Configuration Screen to change the settings, if required. In the File Stores screen, you can set file store names, directories, and synchronous write policies.
- JMS JDBC Store - Configures a component to use JDBC stores for all its JMS servers. When you complete the configuration, you have a cluster and JDBC persistent stores are configured for the JMS servers.

## Selecting the Application Home Location

Use the Application Location screen to select the location to store applications associated with your domain, also known as the *Application home* directory.

Oracle recommends that you locate your Application home in accordance with the directory structure in What Are the Key Oracle Fusion Middleware Directories? in *Oracle Fusion Middleware Understanding Oracle Fusion Middleware*, where the Application home is located outside the Oracle home directory. This directory structure helps avoid issues when you need to upgrade or re-install your software.

For more about the Application home directory, see [About the Application Home Directory](#).

For more information about this screen, see Application Location in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Configuring the Administrator Account

Use the Administrator Account screen to specify the user name and password for the default WebLogic Administrator account for the domain.

Oracle recommends that you make a note of the user name and password that you enter on this screen; you need these credentials later to boot and connect to the domain's Administration Server.

## Specifying the Domain Mode and JDK

Use the Domain Mode and JDK screen to specify the domain mode and Java Development Kit (JDK).

On the Domain Mode and JDK screen:

- Select **Production** in the **Domain Mode** field.
- Select the **Oracle HotSpot JDK** in the **JDK** field.

For more information about this screen, see Domain Mode and JDK in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Specifying JDBC Data Sources

Use this screen to specify JDBC Data Sources.

If you use a DB2 database, you must check system requirements before you select a DB2 driver. See the document *Oracle Fusion Middleware System Requirements and Specifications*.

1. Select the default Data Source, mds-WCCUIMDSREPO.
2. Enter values for DBMS/Service, Host Name, Port and Password and Username.

### Note:

For an Autonomous Transaction Processing database, (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), specify the connection credentials using only the **Connection URL String** option, and enter the connect string in the following format:

```
jdbc:oracle:thin:@TNS_alias?TNS_ADMIN=<path of the wallet files,
ojdbc.properties, and tnsnames.ora>
```

In the connect string, you must pass **TNS\_alias** as the database name found in **tnsnames.ora**, and **TNS\_ADMIN** property to the location of the wallet files, **ojdbc.properties**, and **tnsnames.ora**.

Example connect string for Oracle Autonomous Transaction Processing-Dedicated (ATP-D) database:

```
jdbc:oracle:thin:@dbname_medium?TNS_ADMIN=/users/test/wallet_dbname/
```

Example connect string for Oracle Autonomous Transaction Processing-Shared (ATP-S) database:

```
jdbc:oracle:thin:@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/
```

3. Click **Next**.



## Testing the JDBC Data Source

Use this screen to test the data source connections you configured in the previous screens.



### Note:

To test database connections, the database you are connecting to must be running. If you don't want to test the connections at this time, do not select any data sources and click **Next** to continue.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

To test the data source:

1. Select the check box next to the data source you want to test.
2. Select **Test Selected Connections**.
3. If the test is successful, then click **Next**. If it fails, click **Back**, correct the details and retest it.

## Specifying the Database Configuration Type

Use the Database Configuration type screen to specify details about the database and database schema.

On the Database Configuration type screen, select **RCU Data**. This option instructs the Configuration Wizard to connect to the database and Service Table (STB) schema to automatically retrieve schema information for schemas needed to configure the domain.



### Note:

If you select **Manual Configuration** on this screen, you must manually fill in parameters for your schema on the next screen.

For an Autonomous Transaction Processing database, (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), you must select only the **RCU Data** option.

After selecting **RCU Data**, specify details in the following fields:

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DBMS/Service                    | Enter the database DBMS name, or service name if you selected a service type driver.<br>Example: orcl.exampledomain.com                                                                                                                                                                                                                                                                        |
| Host Name                       | Enter the name of the server hosting the database.<br>Example: examplehost.exampledomain.com                                                                                                                                                                                                                                                                                                   |
| Port                            | Enter the port number on which the database listens.<br>Example: 1521                                                                                                                                                                                                                                                                                                                          |
| Schema Owner<br>Schema Password | Enter the username and password for connecting to the database's Service Table schema. This is the schema username and password entered for the Service Table component on the Schema Passwords screen in the RCU (see <a href="#">Specifying Schema Passwords</a> ).<br><br>The default username is <i>prefix_STB</i> , where <i>prefix</i> is the custom prefix that you defined in the RCU. |

For an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), specify the connection credentials using only the **Connection URL String** option, and enter the connect string in the following format:

```
jdbc:oracle:thin:@TNS_alias?TNS_ADMIN=<path of the wallet files,
ojdbc.properties, and tnsnames.ora>
```

In the connect string, you must pass *TNS\_alias* as the database name found in *tnsnames.ora*, and *TNS\_ADMIN* property to the location of the wallet files, *ojdbc.properties*, and *tnsnames.ora*.

Example connect string for Oracle Autonomous Transaction Processing-Dedicated (ATP-D) database:

```
jdbc:oracle:thin:@dbname_medium?TNS_ADMIN=/users/test/wallet_dbname/
```

Example connect string for Oracle Autonomous Transaction Processing-Shared (ATP-S) database:

```
jdbc:oracle:thin:@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/
```

Click **Get RCU Configuration** when you finish specifying the database connection information. The following output in the Connection Result Log indicates that the operation succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK
```

Successfully Done.

For more information about the schema installed when the RCU is run, see *About the Service Table Schema* in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

See *Database Configuration Type* in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Specifying JDBC Component Schema Information

Use the JDBC Component Schema screen to verify or specify details about the database schemas.

Verify that the values populated on the JDBC Component Schema screen are correct for all schemas. If you selected **RCU Data** on the previous screen, the schema table should already be populated appropriately.

For an Autonomous Transaction Processing database (both Oracle Autonomous Transaction Processing-Dedicated (ATP-D) and Oracle Autonomous Transaction Processing-Shared (ATP-S)), specify the connection credentials using only the **Connection URL String** option, and enter the connect string in the following format:

```
jdbc:oracle:thin:@TNS_alias?TNS_ADMIN=<path of the wallet files,
ojdbc.properties, and tnsnames.ora>
```

In the connect string, you must pass `TNS_alias` as the database service name found in `tnsnames.ora`, and `TNS_ADMIN` property to the location of the wallet files, `ojdbc.properties`, and `tnsnames.ora`.

Example connect string for Oracle Autonomous Transaction Processing-Dedicated (ATP-D) database:

```
jdbc:oracle:thin:@dbname_medium?TNS_ADMIN=/users/test/wallet_dbname/
```

Example connect string for Oracle Autonomous Transaction Processing-Shared (ATP-S) database:

```
jdbc:oracle:thin:@dbname_medium?TNS_ADMIN=/users/test/wallet_dbname/
```

For high availability environments, see the following sections in *Oracle Fusion Middleware High Availability Guide* for additional information on configuring data sources for Oracle RAC databases:

- Configuring Active GridLink Data Sources with Oracle RAC
- Configuring Multi Data Sources

See JDBC Component Schema in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard* for more details about this screen.

## Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

By default, the schema password for each schema component is the password you specified while creating your schemas. If you want different passwords for different schema components, manually edit them in the previous screen (JDBC Component Schema) by entering the password you want in the **Schema Password** column, against each row. After specifying the passwords, select the check box corresponding to the schemas that you changed the password in and test the connection again.

For more information about this screen, see JDBC Component Schema Test in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Entering Credentials

Use the Credentials screen to set credentials for each key in the domain.

The Store Name column shows the credential store associated with each key.

(Optional) You can click **Add** to enter additional key credentials.

1. Enter the User Name to use for the key.
2. Enter the Password to use for the key.
3. Select **Next**.

## Selecting Advanced Configuration

Use the Advanced Configuration screen to complete the domain configuration.

On the Advanced Configuration screen, select:

- Administration Server  
Required to properly configure the listen address of the Administration Server.
- Node Manager  
Required to configure Node Manager.
- Topology  
Required to configure the WebCenter Content Managed Server.

Optionally, select other available options as required for your desired installation environment. The steps in this guide describe a standard installation topology, but you may choose to follow a different path. If your installation requirements extend to additional options outside the scope of this guide, you may be presented with additional screens to configure those options. For information about all Configuration Wizard screens, see Configuration Wizard Screens in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Configuring the Administration Server Listen Address

Use the Administration Server screen to select the IP address of the host.

Select the drop-down list next to **Listen Address** and select the IP address of the host where the Administration Server will reside, or use the system name or DNS name that maps to a single IP address. Do *not* use All Local Addresses.

Do *not* specify any server groups for the Administration Server.



### Note:

Use the Mozilla Firefox browser to access Internet Protocol Version 6 (IPv6) URLs. You must enter the Global IPv6 address to create a domain and access URLs. (You should not use the local IPv6 address.)

## Configuring Node Manager

Use the Node Manager screen to select the type of Node Manager you want to configure, along with the Node Manager credentials.

Select **Per Domain Default Location** as the Node Manager type, then specify Node Manager credentials.

For more information about this screen, see Node Manager in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

For more about Node Manager types, see Node Manager Overview in *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

## Configuring Managed Servers for Oracle WebCenter Content

You create and configure new Managed Servers on the Managed Servers Screen.

You create two Managed Servers for each component, with the exception of Inbound Refinery.

1. In the Listen Address drop-down list, select the IP address of the host on that the Managed Servers will reside on or use the system name or DNS name that maps to a single IP address. Do not use **All Local Addresses**.
2. Select **Enable SSL** to enable an SSL (https) connection for WebCenter Content and WebCenter Content User Interface. Revise the **SSL Listen Port** value as needed.
3. Leave the Server Groups settings as they appear; the Configuration Wizard assigns the correct server group automatically. A server group ensures that the correct services target Managed Servers you are creating.

**Server groups** target Fusion Middleware applications and services to one or more servers by mapping defined application service groups to each defined server group. You can map a given application service group to multiple server groups if needed. Any application services that map to a certain server group are automatically targeted to all servers assigned to that group. For more information about server groups, see Application Service Groups, Server Groups, and Application Service Mappings in *Oracle Fusion Middleware Domain Template Reference*.

4. Click **Add** and repeat this process to create a second Managed Server for each component except for Inbound Refinery. For example, `cpt_server_2`.

You must configure a second Managed Server to configure the standard topology for high availability. If you are not creating a highly available environment, then this step is optional.

For more about the high availability standard topology, see Understanding the Fusion Middleware Standard HA Topology in *Oracle Fusion Middleware High Availability Guide*.

For more information about the next steps to prepare for high availability after your domain is configured, see [Preparing Your Environment for High Availability](#).

Examples and procedures in the rest of this document refer to these server names; if you choose different names be sure to replace them as needed.

**Tip:**

For more about options on this screen, see *Managed Servers in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Configuring a Cluster for WebCenter Content

Use the Clusters screen to create a new cluster.

On the Clusters screen:

1. Click **Add**.
2. Specify `wcc_cluster_1` in the Cluster Name field.
3. Leave the Cluster Address field blank.

Repeat the preceding steps to create three more clusters: `cpt_cluster_1`, `ibr_cluster_1`, and `wccui_cluster_1`.

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, see *Considerations for Choosing Unicast or Multicast in Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server*.

You can also create clusters using Fusion Middleware Control. In this case, you can configure cluster communication (unicast or multicast) when you create the new cluster. See *Create and configure clusters in Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

For more information about this screen, see *Clusters in Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Defining Server Templates

If you are creating dynamic clusters for a high availability setup, use the Server Templates screen to define one or more server templates for domain.

To continue configuring the domain, click **Next**.

For steps to create a dynamic cluster for a high availability setup, see *Using Dynamic Clusters in Oracle Fusion Middleware High Availability Guide*.

## Configuring Dynamic Servers

If you are creating dynamic clusters for a high availability setup, use the Dynamic Servers screen to configure the dynamic servers.

If you are *not* configuring a dynamic cluster, click **Next** to continue configuring the domain.

**Note:**

When you create dynamic clusters, keep in mind that after you assign the **Machine Name Match Expression**, you do not need to create machines for your dynamic cluster.

To create a dynamic cluster for a high availability setup, see Using Dynamic Clusters in *Oracle Fusion Middleware High Availability Guide*.

## Assigning WebCenter Content Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign Managed Servers to a new *configured cluster*. A configured cluster is a cluster you configure manually. You do not use this screen if you are configuring a *dynamic cluster*, a cluster that contains one or more generated server instances that are based on a server template.

For more on configured cluster and dynamic cluster terms, see About Dynamic Clusters in *Oracle Fusion Middleware Understanding Oracle WebLogic Server*.

On the Assign Servers to Clusters screen:

1. In the Clusters pane, select the cluster to which you want to assign the Managed Servers; in this case, `wcc_cluster_1`.
2. In the Servers pane, assign `wcc_server_1` to `wcc_cluster_1` by doing one of the following:
  - Click once on `wcc_server_1` to select it, then click the right arrow to move it beneath the selected cluster (`wcc_cluster_1`) in the Clusters pane.
  - Double-click on `wcc_server_1` to move it beneath the selected cluster (`wcc_cluster_1`) in the Clusters pane.
3. Repeat to assign `wcc_server_2` to `wcc_cluster_1`.

The following image shows a generic example of the Clusters pane after Managed Servers are assigned to clusters.

For more information about this screen, see Assign Servers to Clusters in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster.

Leave the default port number as the Coherence cluster listen port. After configuration, the Coherence cluster is automatically added to the domain.

**Note:**

Setting the unicast listen port to 0 creates an offset for the Managed Server port numbers. The offset is 5000, meaning the maximum allowed value that you can assign to a Managed Server port number is 60535, instead of 65535.

See [Table 5-2](#) for more information and next steps for configuring Coherence.

For Coherence licensing information, see Oracle Coherence Products in *Licensing Information*.

## Creating a New WebCenter Content Machine

Use the Machines screen to create new machines in the domain. A machine is required so that Node Manager can start and stop servers.

If you plan to create a high availability environment and know the list of machines your target topology requires, you can follow the instructions in this section to create all the machines at this time. For more about scale out steps, see Optional Scale Out Procedure in *Oracle Fusion Middleware High Availability Guide*.

To create a new WebCenter Content machine so that Node Manager can start and stop servers:

1. Select the Machine tab (for Windows) or the UNIX Machine tab (for UNIX), then click **Add** to create a new machine.
2. In the Name field, specify a machine name, such as `wcc_machine_1`.
3. In the Node Manager Listen Address field, select the IP address of the machine in which the Managed Servers are being configured.

You must select a specific interface and not `localhost`. This allows Coherence cluster addresses to be dynamically calculated.

4. Verify the port in the Node Manager Listen Port field.
5. Repeat these steps to add more machines, if required.



### Note:

If you are extending an existing domain, you can assign servers to any existing machine. It is not necessary to create a new machine unless your situation requires it.

For more information about this screen, see Machines in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Assigning Servers to WebCenter Content Machines

Use the Assign Servers to Machines screen to assign the Administration Server and Managed Servers to the new machine you just created.

On the Assign Servers to Machines screen:

1. In the Machines pane, select the machine to which you want to assign the servers; in this case, `wcc_machine_1`.
2. In the Servers pane, assign `AdminServer` to `wcc_machine_1` by doing one of the following:
  - Click once on `AdminServer` to select it, then click the right arrow to move it beneath the selected machine (`wcc_machine_1`) in the Machines pane.



- Double-click on `AdminServer` to move it beneath the selected machine (`wcc_machine_1`) in the **Machines** pane.

3. Repeat these steps to assign all Managed Servers to their respective machines.

For more information about this screen, see *Assign Servers to Machines* in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Virtual Targets

If you have a WebLogic Server Multitenant (MT) environment, you use the Virtual Targets screen to add or delete virtual targets. For this installation (not a WebLogic Server MT environment), you do not enter any values; just select **Next**.

For details about this screen, see *Virtual Targets* in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.



### Note:

WebLogic Server Multitenant virtual targets are deprecated in WebLogic Server 12.2.1.4.0 and will be removed in the next release.

## Partitions

The Partitions screen is used to configure partitions for virtual targets in WebLogic Server Multitenant (MT) environments. Select **Next** without selecting any options.

For details about options on this screen, see *Partitions* in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.



### Note:

WebLogic Server Multitenant domain partitions are deprecated in WebLogic Server 12.2.1.4.0 and will be removed in the next release.

## Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen shows detailed configuration information for the domain you are about to create.

Review each item on the screen and verify that the information is correct. To make any changes, go back to a screen by clicking the **Back** button or selecting the screen in the navigation pane. Domain creation does not start until you click **Create**.

For more details about options on this screen, see *Configuration Summary* in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

## Writing Down Your Domain Home and Administration Server URL

The End of Configuration screen shows information about the domain you just configured.

Make a note of the following items because you need them later:

- Domain Location
- Administration Server URL

You need the domain location to access scripts that start Node Manager and Administration Server, and you need the URL to access the Administration Server.

Click **Finish** to dismiss the Configuration Wizard.

## Starting the Servers

After configuration is complete, start Node Manager, then the WebLogic Administration Server and Managed Servers.

For more information on additional tools you can use to manage your domain, see Overview of Oracle Fusion Middleware Administration Tools in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

- [Starting Node Manager](#)
- [Starting the Administration Server](#)
- [Starting the Managed Servers](#)
- [Oracle WebCenter Content Managed Server Locations \(URLs\)](#)  
After you start the Managed Servers, use this topic to refer to Oracle WebCenter Content Managed Server locations.

## Starting Node Manager

To start the per-domain Node Manager:

1. Change to the following directory:
  - (UNIX) `setenv JAVA_HOME /home/Oracle/Java/jdk1.8.0_211`
  - (Windows) `set JAVA_HOME=C:\home\Oracle\Java\jdk1.8.0_211`
2. Enter the following command:
  - (UNIX) Using `nohup` and `nm.out` as an example output file:  

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

where `LOG_DIR` is the location of directory in which you want to store the log files.
  - (Windows) `startNodeManager.cmd`

### Note:

On Windows operating systems, Oracle recommends that you configure Node Manager to run as a startup service. This allows Node Manager to start up automatically each time the system is restarted.

See Running Node Manager as a Startup Service in *Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server*.

## Starting the Administration Server

To start the Administration Server:

1. Go to the `DOMAIN_HOME/bin` directory.

2. Enter the following command:

- (UNIX)  
`./startWebLogic.sh`
- (Windows)  
`startWebLogic.cmd`

If you selected **Production Mode** on the Domain Mode and JDK screen when you created the domain, you see a prompt for the Administrator user login credentials as provided on the Administrator Account screen.

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

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

You can verify that the Administration Server is up and running by accessing the Administration Server Console. The URL is provided on the End of Configuration screen (`http://administration_server_host:administration_server_port/console`). The default Administration Server port number is 7001.



### Note:

Make sure that the database hosting your product schemas is up and running and accessible by the Administration Server.

For more information about how to use the Administration Console, see Getting Started Using Oracle WebLogic Server Administration Console in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

## Starting the Managed Servers

To start the Managed Servers:

1. Sign in to Oracle Fusion Middleware Control:

`http://administration_server_host:administration_server_port/em`

The Administration Server host and port number were in the URL on the End of Configuration screen ([Writing Down Your Domain Home and Administration Server URL](#)). The default Administration Server port number is 7001.

The login credentials were provided on the Administrator Account screen ([Configuring the Administrator Account](#)).

2. The Enterprise Manager landing page lists the servers configured for this domain and displays their status (such as **Running** or **Shutdown**). For a newly configured domain, only the **AdminServer(admin)** will be running.

Select the first Managed Server.

3. Next to the **WebLogic Server** menu, select **Start Up**.
4. Repeat Steps 3 and 4 to start all Managed Servers.
5. On the main landing page, verify that all the Managed Servers are up and running.

## Oracle WebCenter Content Managed Server Locations (URLs)

After you start the Managed Servers, use this topic to refer to Oracle WebCenter Content Managed Server locations.

| Server                           | URL                                                                                                          |
|----------------------------------|--------------------------------------------------------------------------------------------------------------|
| WebCenter Content                | <code>http://hostname:wcc-server-port/cs</code><br>Example: <code>http://host1:16200/cs</code>               |
| WebCenter Content User Interface | <code>http://hostname:wccui-server-port/wcc</code><br>Example: <code>http://host1:16225/wcc</code>           |
| Inbound Refinery                 | <code>http://hostname:ibr-server-port/ibr</code><br>Example: <code>http://host1:16250/ibr</code>             |
| Capture                          | <code>http://hostname:cpt-server-port/</code><br>Example: <code>http://host1:7004/cpt</code>                 |
| WebCenter Content: Imaging       | <code>http://hostname:imaging-server-port/imaging</code><br>Example: <code>http://host1:16000/imaging</code> |

## Verifying the Configuration

After completing all configuration steps, you can perform additional steps to verify that your domain is properly configured.

To verify that the domain is configured properly, see [Performing Additional Domain Configuration Tasks](#).

## Configuring Inbound Refinery Settings (Single Node)

After you start the Inbound Refinery Managed Servers, configure the settings on the post-installation configuration screen. In most cases, you can accept the default settings.

To configure the settings:

1. Access the Inbound Refinery post-installation configuration screen at the following URL:  
`http://managedServerHost:managedServerPort/ibr/`
2. Review the settings. See [Inbound Refinery Configuration Page](#) for a description of each field.

3. Click **Submit**.
  4. Restart the Inbound Refinery Managed Server, using the WebLogic Server Administration Console.
- [Inbound Refinery Configuration Page](#)  
Use descriptions of Inbound Refinery configuration page fields as you complete configuration steps in [Configuring Inbound Refinery Settings \(Single Node\)](#).

## Inbound Refinery Configuration Page

Use descriptions of Inbound Refinery configuration page fields as you complete configuration steps in [Configuring Inbound Refinery Settings \(Single Node\)](#).

The following table describes Inbound Refinery configuration page fields.

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inbound Refinery Instance Folder | Absolute path to the Oracle instance directory of Inbound Refinery. Default is <code>DomainHome/ucm/</code> . The default Oracle instance directory for Inbound Refinery is <code>ORACLE_HOME/user_projects/domains/DomainHome/ucm/ibr</code> . The top-level folder in the folder hierarchy for the Content Server instance is <code>ibr</code> . The path to the Oracle instance directory is the value of the <code>IntradocDir</code> variable for the Inbound Refinery instance. Oracle recommends that you make this directory path unique to this Managed Server, or node. For installations that you will probably upgrade, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside any Oracle WebLogic Server domain directories or installation directories. |
| Native File Repository Location  | Directory that stores conversion jobs during their processing. After a job converts and Content Server picks it up, it is removed from this directory. You do not need to change this path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Weblayout Folder                 | URL for the Inbound Refinery web interface. You do not need to change this path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Register Start Menu Actions      | Whether or not to register Start Menu actions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Socket Port | <p>Number of the port to call top-level services. To set up a provider from Inbound Refinery back to Content Server, you can leave the default</p> <p><b>Server Socket Port</b> value 5555 or change it to an unused port number.</p> <p>Changing this field value also changes the <code>IntradocServerPort</code> entry in <code>ORACLE_HOME/user_projects/domains/DomainHome/ucm/ibr/config/config.cfg</code></p> |



**Note:**

You must set Server Socket Port correctly to use Inbound Refinery.



**Note:**

The default port number for Node Manager and Inbound Refinery is 5555. If both run on the same server, you must configure a different port number for Node Manager or Inbound Refinery.

| Field                                                                                                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Incoming Socket Connection Address Security Filter                                                                                                                                                                                   | <p>Restricts Inbound Refinery access to a computer or computers with a specified IP address or addresses. To enable access from Content Server, enter a value for this field. For example:</p> <pre>127.0.0.1 0:0:0:0:0:0:0:1 <br/>your.server.IP.address</pre> <p>This value should be the Content Server instance IP address of the or instances that will send jobs to Inbound Refinery, not the IP address of Inbound Refinery. (In a test or demo environment, these IP addresses could be the same.)</p> <p>This field accepts wildcards such as 10.*.*. You can change this value by setting <code>SocketHostAddressSecurityFilter</code> in <code>DomainHome/ucm/ibr/config/config.cfg</code> and restarting Inbound Refinery.</p> |
| <div> <b>Note:</b></div> <div>To use Inbound Refinery, you must set the Incoming Socket Connection Address Security Filter value correctly.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Web Server HTTP/HTTPS Address                                                                                                                                                                                                        | The name of the web server. ( <code>HttpServerAddress</code> property).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| WebAddress Is HTTPS                                                                                                                                                                                                                  | Whether or not the URL for the web server starts with HTTPS, for a server that has SSL enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Inbound Refinery URL Prefix                                                                                                                                                                                                          | Relative URL for the Inbound Refinery instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server Instance Name                                                                                                                                                                                                                 | Inbound Refinery instance name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server Instance Label                                                                                                                                                                                                                | Instance name shown for Inbound Refinery.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Service Instance Description                                                                                                                                                                                                         | Inbound Refinery Instance description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Configuring WebCenter Content Settings

You must complete the WebCenter Content configuration on the post-installation configuration page in Content Server.

WebCenter Content shows the configuration page when you first sign in to Managed Server at `http://managedServerHost:managedServerPort/cs`



### Note:

The domain administrator must be the first user to sign in to the WebCenter Content Managed Server so that they can complete configuration. For more details about administration, see *Introduction in Oracle Fusion Middleware Administering Oracle WebCenter Content*

To complete WebCenter Content configuration:

1. Start the Administration Server. See [Starting the Administration Server](#).
2. Start the WebCenter Content Managed Server. See [Starting the Managed Servers](#).
3. Go to the Content Server post-installation page at `http://managedServerHost:16200/cs/`

4. Enter or edit any configuration values you want to change.

You can select a full-text search engine in the **FullText Search Option** field. Leave the field blank to set up the system as metadata only.

5. Enter a value in **Incoming Socket Connection Address Security Filter** to enable access from Inbound Refinery. For example:

```
127.0.0.1|your.server.IP.address|0:0:0:0:0:0:1|
```

This field accepts wildcards such as `10.*.*.*`. You can change this value later by setting `SocketHostAddressSecurityFilter` in `DomainHome/ucm/cs/config/config.cfg` and restarting WebCenter Content Managed Server.

For Oracle WSM security, the `SocketHostAddressSecurityFilter` value must be set as follows:

```
SocketHostAddressSecurityFilter=.*.*.*|0:0:0:0:0:0:1
```

6. Verify that the **Server Socket Port** setting is 4444. The Managed Server configuration file stores this value as `IntradocServerPort=4444`
  7. Click **Submit**.
  8. Restart the WebCenter Content Managed Server. See [Starting the Managed Servers](#)
- [WebCenter Content Configuration Page](#)  
You enter or verify values in the WebCenter Content configuration page fields to complete WebCenter Content configuration.
  - [Completing the Imaging Configuration](#)  
You can complete the initial configuration of Oracle WebCenter Content: Imaging in an Oracle WebLogic Server domain.
  - [Configuring Capture](#)  
The Capture System Administrator requires system administration privileges to configure and monitor an Oracle WebCenter Enterprise Capture system environment. The configuration consists of tasks such as starting the Capture Managed Server, assigning roles to Capture users in Fusion Middleware Control, and modifying system-level settings through MBeans.

## WebCenter Content Configuration Page

You enter or verify values in the WebCenter Content configuration page fields to complete WebCenter Content configuration.

You can use descriptions of these fields while completing steps in [Configuring WebCenter Content Settings](#)



| Field                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content Server Instance Folder                     | <p>Absolute path to the Oracle instance directory of WebCenter Content. Default is <code>DomainHome/ucm/</code>. The default Oracle instance directory for Inbound Refinery is <code>ORACLE_HOME/user_projects/domains/DomainHome/ucm/cs</code>. The top-level folder in the folder hierarchy for the Content Server instance is <code>cs</code>.</p> <p>The path to the Oracle instance directory is the value of the <code>IntradocDir</code> variable for the WebCenter Content instance. Oracle recommends that you make this directory path unique to this Managed Server, or node. For installations that you will probably upgrade, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside any Oracle WebLogic Server domain directories or installation directories.</p> |
| Native File Repository Location                    | Path to the vault directory for storing native content checked into WebCenter Content.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Weblayout Folder                                   | Path to the weblayout directory for storing web-viewable renditions of native and alternate files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Register Start Menu Actions                        | Whether or not to register Start Menu actions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Is New Content Server Instance                     | Whether or not the WebCenter Content instance is new.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server Socket Port                                 | <p>Number of the port to call top-level services. Default: 5555</p> <p>To set up a provider from Inbound Refinery back to Content Server, you can leave the default</p> <p>Changing this field value also changes the <code>IntradocServerPort</code> entry in <code>DOMAIN_HOME/ucm/ibr/config/config.cfg</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Incoming Socket Connection Address Security Filter | <p>Restricts WebCenter Content access to a computer or computers with a specified IP address or addresses.</p> <p>The default value of this field is the local host's IP address, such as <code>127.0.0.1</code>.</p> <p>You can specify multiple IP addresses, separated by pipes ( ). Make sure that there are no spaces on either side of the pipe character. For example:</p> <pre>127.0.0.1 0:0:0:0:0:0:0:1  your.server.IP.address</pre> <p>This field accepts wildcards * for zero or many characters, and ? for any one character. (For example, <code>10.10.3.*</code>)</p> <p>Typically, use the <b>IP Address Filter</b> field only (most common) or <b>Hostname Filter</b> field, not both.</p>                                                                                                                               |
| Web Server HTTP/HTTPS Address                      | Name of the web server. ( <code>HttpServerAddress</code> property).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| WebAddress Is HTTPS                                | Whether or not the URL for the web server starts with HTTPS, for a server that has SSL enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Inbound Refinery URL Prefix                        | Relative URL for the Inbound Refinery instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Instance Name                               | Inbound Refinery instance name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Instance Label                              | Instance name shown for Inbound Refinery.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Service Instance Description                       | Inbound Refinery Instance description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Field                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Is Auto Number Enabled | Whether or not automatic numbering of WebCenter Content instances is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Auto Number Prefix     | Unique prefix for an WebCenter Content instance number, to avoid conflicts among multiple WebCenter Content instances (Auto Number Prefix system property).                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| FullText Search Option | <p>Search engine for full-text search:</p> <p><b>None:</b> The Oracle Content Server instance uses DATABASE.METADATA as the search engine.</p> <p><b>Internal:</b> If using Oracle Database, the WebCenter Content instance uses OracleTextSearch with the system database. If using Microsoft SQL Server, it will use DATABASE.FULLTEXT.</p> <p><b>External:</b> The Oracle Content Server instance uses OracleTextSearch with an external provider to an Oracle Database (not the system database). If you select this option, you must enter the Data Source name in the External DataSource field.</p> |
| External DataSource    | Name of the Data Source, which you must create in Oracle WebLogic Server and target to the Managed Server, using an OCSSEARCH schema created with Repository Creation Utility (RCU).                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Completing the Imaging Configuration

You can complete the initial configuration of Oracle WebCenter Content: Imaging in an Oracle WebLogic Server domain.

This section explains the steps to complete the Imaging configuration.

- [Completing the Initial Imaging Configuration](#)  
Before you complete the configuration of Imaging, your system should have Oracle WebCenter Content installed and configured. Imaging uses WebCenter Content for its repository.
- [Configuring the Full-Text Features in the WebCenter Content Repository](#)  
Imaging supports two types of full-text searching under WebCenter Content: DATABASE.FULLTEXT and OracleTextSearch. Imaging can use the full-text features if you configure full-text searching in the WebCenter Content repository.
- [Setting Imaging System Security](#)  
On a new Imaging system, the first user to log in is automatically granted full permissions. Typically, this initial user associates other users or groups, after which the initial user's permissions are changed or revoked as needed.
- [Configuring the Imaging Viewer Cache](#)  
The Imaging viewer can cache documents on the server outside of the repository to increase rendering speed on the client machine. Security for the cached documents is controlled by authentication for the server on which the documents are stored.
- [Installing and Configuring AXF BPM and AXF for BPEL](#)  
Oracle WebCenter Content: AXF for BPM and Oracle Application Extensions Framework (AXF) for BPEL are installed automatically with Imaging, and AXF for BPEL is automatically deployed to the Imaging Managed Server.

## Completing the Initial Imaging Configuration

Before you complete the configuration of Imaging, your system should have Oracle WebCenter Content installed and configured. Imaging uses WebCenter Content for its repository.

Your Imaging system uses WebCenter Content 12c as its document repository. For information about configuring WebCenter Content, see [Configuring WebCenter Content Domain](#).



### Note:

In a production system, Oracle WebCenter Content applications use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. If you want to reassociate the identity store for Imaging with an external LDAP authentication provider, it is easier to do this association before you complete the configuration of the Imaging Managed Server and before you connect it to the WebCenter Content 12c repository. For more information, see [Reassociating the Identity Store with an External LDAP Authentication Provider](#).

The user who logs in first to an Imaging Managed Server is provisioned with full security throughout the server. When this user first logs in, Imaging provides a user interface to complete the configuration, including connecting to a repository or repositories and, optionally, to a workflow server.

If a value is specified in the `DefaultSecurityGroup` MBean before Imaging security is initialized, then when the first user logs in, the specified group as well as the user logging in is given full administrative permissions.

To complete the Imaging configuration, you have to perform all the tasks that apply to your system:

- [Configuring a WebCenter Content Repository for Imaging](#)  
You can configure WebCenter Content 12c as the repository for Imaging. You will not be able to import or upload content to the Imaging system unless you have created a repository connection.
- [Starting the Imaging Managed Server and Accessing the Web Client](#)  
You can access the Imaging web client after you start the Administration server and the Imaging and WebCenter Content Managed Servers.
- [Connecting to a WebCenter Content Repository](#)  
Before Imaging can use the WebCenter Content repository, you need to configure a connection to Content Server. You can create a connection to it from Imaging.
- [Connecting to a Workflow Server](#)  
A connection to a workflow server (Oracle SOA Suite) is required before you import the definition files. This connection is necessary for your solution to retrieve your task list. Imaging connects to a workflow server when application fields are mapped to workflow payload elements.

- [Configuring the GDFontPath MBean for a UNIX System](#)  
For conversions to work correctly on a UNIX operating system, the operating system needs to have TrueType fonts available. If these fonts are not available on your system, you need to install them. To set the font path on a UNIX operating system, you need to configure the GDFontpath MBean. You can configure it through the System MBean Browser in Oracle Enterprise Manager Fusion Middleware Control.
- [Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 12c](#)  
In an Exalogic environment with Solaris 12c, you need to set the DISPLAY environment variable for the Imaging Viewer to work correctly in the basic mode.
- [Importing Definitions](#)  
At this point in the installation process, you can import previously exported Imaging definitions (applications, searches, and inputs).

## Configuring a WebCenter Content Repository for Imaging

You can configure WebCenter Content 12c as the repository for Imaging. You will not be able to import or upload content to the Imaging system unless you have created a repository connection.

- [Configuring WebCenter Content 12c to Work with Imaging](#)
- [Configuring a File Store Provider for Content Storage](#)

## Configuring WebCenter Content 12c to Work with Imaging

WebCenter Content 12c is installed with Oracle WebCenter Content. When a WebCenter Content Managed Server and Imaging Managed Server are configured in an Oracle WebLogic Server domain on the same host machine, the configuration of WebCenter Content 12c to work with Imaging is automatic.

If WebCenter Content is installed in a domain that is later extended with Imaging, then WebCenter Content will not be reconfigured to work with Imaging until the next restart of the WebCenter Content Managed Server. In this case, you must restart WebCenter Content before you connect to Oracle WebCenter Content Server from the Imaging web client, as described in [Connecting to a WebCenter Content Repository](#).

If the WebCenter Content and Imaging Managed Servers are configured to run on different machines, configuring Imaging will not configure WebCenter Content to work with it. In this case, you must follow the manual configuration steps to configure WebCenter Content.

To configure WebCenter Content 12c manually to work with Imaging:

1. Start the WebCenter Content Managed Server, as described in [Starting the Managed Servers](#).
2. Access Content Server.
3. Enable the `IpmRepository` component:
  - a. From the **Administration** tray or menu, select **Admin Server**, and then select **Component Manager**.
  - b. On the Component Manager page, select **Integration**.
  - c. Select **IpmRepository**, and click **Update**.

This option is selected by default if the Oracle WebLogic Server domain is configured with Fusion Middleware Configuration Wizard. If this option is already selected, you can close Component Manager without clicking **Update** or restarting Content Server.

- d. Click **OK**.
- e. Restart Content Server.

If you have already selected **IpmRepository**, you do not need to restart the server.

## Configuring a File Store Provider for Content Storage

An administrator can configure a file store provider in Content Server 11g to control how and where files are stored and managed within Content Server. Instead of storing all content on a single file system, you can use a file store provider to store content across multiple file systems as well as within a database. The File Store Provider component is installed and enabled by default with WebCenter Content installation and configuration

For Imaging, you should add a file store provider to use instead of the default file store provider. Also, you should disable the traditional web layout functionality for the file store.

You can configure a file store provider for Oracle Database.

If your WebCenter Content installation uses a Microsoft SQL Server or IBM DB2 database, do not configure a file store provider. If you are configuring a WebCenter Content Managed Server with one of these databases, you need to disable the file store provider that is enabled by default for Content Server. See Managing a File Store System in *Oracle Fusion Middleware Administering Oracle WebCenter Content*

- [Configuring a File Store Provider](#)
- [Disabling Web Layout Functionality for Imaging](#)

### Configuring a File Store Provider

A file store provider can be a combination of any media supported by Content Server. Because the document storage location is not defined by the media that is being used for storage, the term *volume* is used to represent a storage location when an application is defined in the Imaging user interface. Imaging connects to a volume that an administrator defines and configures in Content Server. You cannot use Imaging to create or define a volume.

A Content Server administrator can configure a file store provider. See Managing the File Store Provider in *Oracle Fusion Middleware Administering Oracle WebCenter Content*

### Disabling Web Layout Functionality for Imaging

Content Server traditionally uses a `weblayout/` directory on a file system to store content in a format for viewing in a web browser, even if the main storage volume is set up in a database. This file system store is useful for making content retrieval faster for a website or for storing a secondary file that describes the primary content item, but it does not have much use in an Imaging solution. Files copied to a `weblayout/` directory in an exclusively Imaging solution would never get used, taking up unnecessary storage space. Oracle recommends that you disable the web layout functionality for any file store provider that is configured for use as an Imaging volume.

 **Note:**

If your Imaging system will use redactions, do not implement Web Layout. Users might be able to see an unredacted version of a document in the `weblayout/` directory if Web Layout (IBR) is turned on in an Imaging file store provider.

An administrator can disable the web layout functionality by selecting the **Is Webless File Store** option on the Add/Edit Storage Rule page for a file store provider in Content Server. See Adding or Editing a Storage Rule in *Oracle Fusion Middleware Administering Oracle WebCenter Content*

## Starting the Imaging Managed Server and Accessing the Web Client

You can access the Imaging web client after you start the Administration server and the Imaging and WebCenter Content Managed Servers.

To access the Imaging web client:

1. Start the Imaging Managed Server, as described [Starting the Managed Servers](#).

 **Note:**

If Oracle WebCenter Content: AXF for BPM is deployed to the domain, proceed to [Configuring and Verifying AXF for BPM](#) before you perform any configuration on the Imaging server.

2. Access the web client at this URL: `http://managedServerHost:16000/imaging`. Log in with the administrator user name and password.

 **Note:**

This first user who connects to the Imaging system is registered as the Imaging administrator.

## Connecting to a WebCenter Content Repository

Before Imaging can use the WebCenter Content repository, you need to configure a connection to Content Server. You can create a connection to it from Imaging.

To connect to a WebCenter Content repository:

1. Open a web browser, and navigate to this website: `http://managedServerHost:16000/imaging`.
2. Log in with the administrator user name and password.
3. Navigate to the **Manage Connections** tray and select **Create Content Server Connection** from the list.
4. Enter a name for the connection on the Basic Information page and, optionally, a description, and then click **Next**.

5. Change the selections, if required, on the Connection Settings page:
  - **SSL**: Selected for secure SSL communications.
  - **Server Port**: The IDC port of the WebCenter Content instance. By default, 4444 for Imaging.
  - **Use Local Content Server**: Selected by default if Content Server is on the same machine as the Imaging server.

If the servers are not installed on the same machine, configure the Content Server machine name as part of the Content Server Pool.
6. Click **Next**.
7. Enter a **Connection Security** value for the connection.

Select which users and groups should have permission to access, modify, delete, or grant other users access to this connection definition. At least one user or group must have the grant access permission.
8. Click **Next**.
9. At the Summary screen, click **Submit**.

## Connecting to a Workflow Server

A connection to a workflow server (Oracle SOA Suite) is required before you import the definition files. This connection is necessary for your solution to retrieve your task list. Imaging connects to a workflow server when application fields are mapped to workflow payload elements.

To connect, the provider, port, and credential information is passed using Web Services Inspection Language (WSIL). WSIL uses the HTTP protocol and a specific XML format to allow for the discovery of the web service end points on a server. Imaging follows links in the WSIL that meet certain criteria to discover deployed composites.

The connection can be to an Oracle Business Process Management (Oracle BPM) or Business Process Execution Language (BPEL) server. For Imaging to take advantage of BPM and Oracle BPEL Process Manager within an existing domain, the domain must be extended with **Oracle BPM Suite - 12.2.1.4.0**. When Oracle BPM Suite is installed, it automatically selects **Oracle SOA Suite - 12.2.1.4.0** as its dependency. If you want to use Oracle BPEL Process Manager and not Oracle BPM, you can extend the domain with an Oracle SOA Suite installation and configuration. See *About the Oracle SOA Suite and Oracle Business Process Management Installation in Oracle Fusion Middleware Installing and Configuring Oracle SOA Suite and Business Process Management*.

This section describes the procedure to configure a connection to a workflow server and register the connection in your database. For additional information, see *Creating a Workflow Connection in Administering Oracle WebCenter Content: Imaging*.

- [Configuring a Connection to a Workflow Server](#)
- [Adding the Connection to the Database](#)

## Configuring a Connection to a Workflow Server

If you have installed the Oracle SOA Suite for use with Imaging, such as for AXF for BPM or AXF for BPEL, you need to configure a connection to a workflow server.



To configure a connection to a workflow server:

1. Open a web browser, and navigate to this website: `http://managedServerHost:16000/imaging`.
2. Log in with the administrator user name and password.
3. Navigate to the **Manage Connections** tray and select **Create Workflow Connection** from the list.
4. Enter a name for the connection on the Basic Information page and, optionally, a description, and then click **Next**.
5. Optionally, change one or more of the following selections on the Connection Settings page:
  - **HTTP Front End Address:** The front end address of the workflow server, including the listening port, which is `http://<server>:8001` for Oracle SOA Suite, by default.
  - **Credential Alias:** The credential store key for obtaining user and password credentials for the workflow server.
  - **Provider:** The provider setting can be either the host name or IP address of a single machine, or a comma-separated list of host names or IP addresses for multiple machines in a cluster. The listening port and transport mechanism should be included in the setting.
6. Click **Test Connection** to verify the settings.
7. Click **Next**.
8. Enter a **Connection Security** value for the connection.

Select which users and groups should have permission to access, modify, delete, or grant other users access to this connection definition. At least one user or group must have the grant access permission.
9. Click **Next**.
10. At the Summary screen, click **Submit**.

## Adding the Connection to the Database

After you have created a workflow connection, enter the name of that connection in the `AXF_SOLUTION_ATTRIBUTES` table for your solution. For example, the parameter key for a BPEL server is named `WORKFLOW_CONNECTION`, and the `HelloBPEL` sample script uses the connection name `test`.

## Configuring the GDFontPath MBean for a UNIX System

For conversions to work correctly on a UNIX operating system, the operating system needs to have TrueType fonts available. If these fonts are not available on your system, you need to install them. To set the font path on a UNIX operating system, you need to configure the GDFontpath MBean. You can configure it through the System MBean Browser in Oracle Enterprise Manager Fusion Middleware Control.

To configure the GDFontPath MBean for a UNIX system:

1. Access the Imaging domain in Fusion Middleware Control by using the URL: `http://adminServerHost:adminServerPort/em`

For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the



Administration Server. The default number is 7001. For example: `http://myHost.example.com:7001/em`

To log in, provide the user name and password that were specified on the Configure Administrator User Name and Password screen in the Configuration Wizard.

2. In the navigation tree on the left, expand **WebLogic Domain** and the deployed domain.
3. Right-click **IPM\_server1**, and select **System MBean Browser** from the menu.
4. In the navigation tree on the System MBean Browser page, under **Configuration MBeans**, close the **com.bea** folder.
5. Under **Application Defined MBeans**, expand the **oracle.imaging** folder.
6. Expand the **Server: IPM\_server1** and **config** folders.
7. Click **config**.
8. Set the value of the **GDFontPath** attribute to the location of your True Type Fonts (TTF) files; for example: `/usr/share/X11/fonts/TTF`

For systems on which Oracle WebLogic Server includes a JDK, you can find some TTF files in the `JDK/jre/lib/fonts` directory.

Some standard font locations on different UNIX platforms follow:

- Solaris SPARC: `/usr/openwin/lib/X11/fonts/TrueType`
- AIX: `/usr/lpp/X11/lib/X11/fonts/TrueType`
- HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`
- Linux: `/usr/lib/X11/fonts/TrueType`

9. Click **Apply**.
10. Restart Imaging.

## Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 12c

In an Exalogic environment with Solaris 12c, you need to set the **DISPLAY** environment variable for the Imaging Viewer to work correctly in the basic mode.

To set **DISPLAY** for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 12c:

1. Open a new terminal window and run this command:

```
xhost +
```

2. In the Imaging terminal, set the **DISPLAY** environment variable to the server where Imaging is running and specify the port, in this format:

```
servername:port
```

3. Restart Imaging.

## Importing Definitions

At this point in the installation process, you can import previously exported Imaging definitions (applications, searches, and inputs).

For more information, see *Exporting and Importing Definitions in Administering Oracle WebCenter Content: Imaging*.

For additional information about how to import definitions, see [Importing Definition Files into Imaging](#).

## Configuring the Full-Text Features in the WebCenter Content Repository

Imaging supports two types of full-text searching under WebCenter Content: `DATABASE.FULLTEXT` and `OracleTextSearch`. Imaging can use the full-text features if you configure full-text searching in the WebCenter Content repository.

For `DATABASE.FULLTEXT` systems, after the indexes are rebuilt, nothing needs to be done on the Imaging side. `OracleTextSearch`, however, requires that the index be rebuilt any time an application with `FullText` enabled is created, deleted, or has modifications that involve field definitions.

For more information on configuring full-text searching, see [Configuring OracleTextSearch for Content Server](#).

For additional full-text configuration options, see *Configuring the Search Index in Oracle Fusion Middleware Administering Oracle WebCenter Content*.

After full-text is enabled in WebCenter Content, you will need to create an application and check the `FullText` option on the application. See *Configuring System Properties in Oracle Fusion Middleware Administering Oracle WebCenter Content*.

## Setting Imaging System Security

On a new Imaging system, the first user to log in is automatically granted full permissions. Typically, this initial user associates other users or groups, after which the initial user's permissions are changed or revoked as needed.



### Note:

If you configure Imaging for use with Oracle Access Manager, you must protect the `imaging/faces/` directory. Otherwise, you will not get access to the Imaging Viewer.

If security provider changes are made after this initial user login to Imaging, take the following steps to reset Imaging system security. For example, if you later change the security configuration to point to an Oracle Internet Directory provider or a Microsoft Active Directory provider, you must reset the Imaging system security.

1. Manually create or migrate users and groups to the new external security provider, using utilities as needed. See [Reassociating the Identity Store with an External LDAP Authentication Provider](#).

2. Run the `refreshIPMSecurity()` WLST MBean command. See `refreshIPMSecurity` in *WebCenter WLST Command Reference*.

 **Note:**

During the refresh, users or groups for whom matching identifying information is not found are ignored. As security changes are made, invalid users or groups are removed from the Imaging database.

## Configuring the Imaging Viewer Cache

The Imaging viewer can cache documents on the server outside of the repository to increase rendering speed on the client machine. Security for the cached documents is controlled by authentication for the server on which the documents are stored.

If the server is considered secure, no additional security is necessary. If additional security is required, you can encrypt cached documents as described in [Encrypting Cached Documents](#).

To set the Imaging viewer to use cached documents:

1. Verify that the Imaging Viewer Cache was successfully deployed:
  - a. In the WebLogic Server Administration Console, click **Deployments** under Domain Structure.
  - b. In the **imaging-vc** row of the **Deployments** table, confirm that the **State** value is *Active* and the **Health** value is *OK*.

If the **State** or **Health** value is different for **imaging-vc**, you need to fix the deployment, or redeploy the feature before you proceed.

2. Enable viewer caching by setting the **ViewerCachePath** MBean to the location where the documents must be cached, as described in [Configuring the GDFontPath MBean for a UNIX System](#). For example, to enable caching on an Imaging system that runs on a single computer, you can use the relative path `imaging/ViewerCache`. If no path is set, then caching of documents is disabled.

 **Note:**

The **ViewerCachePath** MBean must be set to a location that is available to all the servers in the cluster. If the directory path is not available to all the servers, each server will cache documents locally, resulting in multiple instances of the entire cache.

3. Specify the number of days for documents to remain in the cache location after being viewed, by setting the **ViewerCacheDays** MBean. Cached documents not viewed within the specified number of days are purged from the cache. If a document is viewed within the specified number of days, the **ViewerCacheDays** timer for that document is reset. If you set **ViewerCacheDays** equal to 0 (the default), you cannot purge the documents from cache.

4. Set the **ViewerCacheEnablePrecache** MBean to `true` to cache documents when they are ingested into Imaging (pre-cache) or set the value to `false` to cache documents when they are first called by the viewer.
- [Changing the Viewer Cache Path](#)  
You can move the viewer cache to a new location if the Imaging server is shut down and the new location uses the same file hierarchy as the old location.
- [Encrypting Cached Documents](#)  
For additional security, you can configure Imaging to encrypt the cached documents. Encryption makes additional processing necessary to decrypt a document for viewing, and reduces the rendering speed. Even if you configure Imaging to encrypt the cached documents, there is a brief period of time during caching when the documents that are generated are not encrypted.
- [Disabling Encryption of Cached Documents](#)  
You can disable the encryption of cached documents by setting the value of the **ViewerCacheEnableEncryption** MBean to `false`.

## Changing the Viewer Cache Path

You can move the viewer cache to a new location if the Imaging server is shut down and the new location uses the same file hierarchy as the old location.

To change the viewer cache path:

1. Shut down the Imaging server.
2. Move the cached files to the new location. Ensure that you preserve the file hierarchy.
3. Set the new path in the **ViewerCachePath** MBean.
4. Start the Imaging server.

## Encrypting Cached Documents

For additional security, you can configure Imaging to encrypt the cached documents. Encryption makes additional processing necessary to decrypt a document for viewing, and reduces the rendering speed. Even if you configure Imaging to encrypt the cached documents, there is a brief period of time during caching when the documents that are generated are not encrypted.

To enable encryption of cached documents:

1. Add a new password credential to the domain with Oracle Enterprise Manager Fusion Middleware Control:
  - a. Select the WebLogic Server domain for Oracle WebCenter Content.
  - b. From the **WebLogic Domain** menu, select **Security**, and then **Credentials**.
  - c. Select the map **oracle.imaging**. If there is no map named `oracle.imaging`, click **Create Map**, specify `oracle.imaging` for the map name, and then select it.
  - d. Click **Create Key**. Name the key `viewer.cache`, and select the type **Password**.
  - e. Enter a user name. The user name does not need to exist in any system.
  - f. Enter a password, confirm it, and then click **OK**.
2. Enable encryption by setting the **ViewerCacheEnableEncryption** MBean, as described in [Configuring the GDFontPath MBean for a UNIX System](#).

 **Note:**

The password credential must exist on the domain before you set the **ViewerCacheEnableEncryption** MBean.

## Disabling Encryption of Cached Documents

You can disable the encryption of cached documents by setting the value of the **ViewerCacheEnableEncryption** MBean to `false`.

Subsequent calls to the viewer causes unencrypted documents to be cached. You can decrypt and view any encrypted documents that are already in the cache if the password credential remains unaltered in the domain.

If you removed or alter the password credential, you must manually purge the encrypted documents that are still cached.

To purge the `imaging.jks` file:

1. Shut down the Imaging server.
2. Delete the cached files from the cache directory.
3. Delete the `imaging.jks` file from the cache directory.
4. Start the Imaging server.

## Installing and Configuring AXF BPM and AXF for BPEL

Oracle WebCenter Content: AXF for BPM and Oracle Application Extensions Framework (AXF) for BPEL are installed automatically with Imaging, and AXF for BPEL is automatically deployed to the Imaging Managed Server.

Before you can deploy AXF for BPM to the Imaging server, you need to create the required schemas with the Repository Creation Utility. Then when the domain is created or extended, you can select AXF for BPM to use it with Imaging.

You can configure either AXF for BPM or AXF for BPEL, or both, to run on the Imaging Managed Server:

- AXF for BPM

The newer AXF for BPM infrastructure takes advantage of the application development and configuration capabilities that are provided by technologies such as Oracle Business Process Management (Oracle BPM), Oracle Application Development Framework (Oracle ADF), Oracle Metadata Services Repository (Oracle MDS Repository), and Oracle Business Rules to create configurable business components. These business components help administrators to configure and develop integration solutions for WebCenter Content business applications. See [Configuring and Verifying AXF for BPM](#).

- AXF for BPEL

You can configure AXF for BPEL to run on the Imaging Managed Server. The older AXF for BPEL infrastructure relies on AXF database tables (Imaging tables) as the basis for configuring AXF solutions, commands, and web tools. A solution developer or solution accelerator can implement and customize these solutions, commands, and tools. See [Configuring and Verifying AXF for BPEL](#).

For additional information about configuring and using AXF for BPM or AXF for BPEL and the AXF for BPEL database tables (Imaging tables), see *Configuring the BPEL Imaging Solution* in *Oracle Fusion Middleware Administering the Application Adapters for Oracle WebCenter*.

- [Configuring and Verifying AXF for BPM](#)
- [Configuring and Verifying AXF for BPEL](#)

## Configuring and Verifying AXF for BPM

Before you configure AXF for BPM with Imaging, you need to install and configure Oracle WebCenter Content and Oracle SOA Suite, and create an AXF schema with the Repository Creation Utility, as well as schemas for the following components:

- **Metadata Services**
- **Oracle WebCenter Content Server - Complete**
- **Oracle WebCenter Content: Imaging**
- **SOA Infrastructure**
- **User Messaging Service**

When you create or extend the WebLogic Server domain, be sure the following product templates are selected:

- **Oracle SOA Suite**
- **Oracle WebCenter Content: AXF for BPM**

### **Note:**

If AXF for BPM is on a separate host machine from the Oracle SOA Suite Managed Server, you need to extend the domain with Oracle WSM Policy Manager.

- **Oracle WebCenter Content: Imaging**
- **Oracle Universal Content Management - Content Server** (for WebCenter Content)
- **Oracle Enterprise Manager**
- **Oracle BPM Suite**

After you create or extend a domain to include AXF for BPM and the components and products it depends on, you can configure it to work with Imaging using the WebLogic Server Administration Console, Oracle WebLogic Server Scripting Tool (WLST), and Oracle Enterprise Manager Fusion Middleware Control. You can also set up communications with Oracle Coherence between AXF for BPM and Imaging servers running on multiple domains or machines or to prevent multicast interference between AXF for BPM and Imaging in a single domain. See [Configuring AXF for BPM](#).

To verify that you have installed and configured the AXF for BPM infrastructure properly, AXF for BPM includes the *HelloBPM* solution, which uses an Oracle BPM process to verify the BPM integration. See [Verifying the AXF for BPM Installation](#).

- [Configuring AXF for BPM](#)
- [Verifying the AXF for BPM Installation](#)

## Configuring AXF for BPM

Use the following procedure to configure AXF for BPM with the Imaging server. You can set up the Imaging server through the WebLogic Server Administration Console, create foreign JNDI with WLST, and configure the AXF for BPM CSF key through Fusion Middleware Control.

To configure AXF for BPM to work with Imaging Managed Servers that run in a cluster or other distributed configuration, you need to set up communications with Oracle Coherence. See [Oracle Coherence Communications for Imaging Clusters, Multiple Domains, or Multiple Machines](#). In a single domain, you can set up communications with Oracle Coherence to avoid interference from multicast traffic. See [Oracle Coherence Communications for a Single Server or Domain](#).

To configure AXF for BPM:

1. Set up the Imaging server through the WebLogic Server Administration Console:
  - a. The Administration Server should be running. If not, start the Administration Server for your Oracle WebLogic Server domain. See [Starting the Administration Server](#).
  - b. Log in to the Administration Console.
  - c. Under **Domain Structure** on the left, expand **Environment**, and click **Servers**.
  - d. In the **Servers** table, click the Imaging server instance, such as **IPM\_server1**.
  - e. Click the **Protocols** tab.

If the server is in production mode, click **Lock & Edit** in the Change Center on the left before you make changes.

- f. Click the **HTTP** tab and set these values:
    - **Frontend Host:** The name of the host machine for the Imaging server, such as `myserver.example.com`.
    - **Frontend HTTP Port:** The port number for the Imaging instance, such as `16000`.
  - g. Save the changes.

If the server is in production mode, activate changes after you save them, unless you have enabled configuration editing.

2. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, set the targeting for the `IPMDS` and `mds-axf` data sources to the Oracle SOA Suite server:
  - a. Log in to the Administration Console on the Oracle SOA Suite machine.
  - b. Under **Domain Structure** on the left, expand **Services**, and click **Data Sources**.
  - c. Select **Generic Data Source** from the **New** menu.
  - d. Enter `jdbc/IPMDS` in the **JNDI Name** field.
  - e. Select your database type in the **Database Type** list, and click **Next**.
  - f. Configure values for **Data Source Properties** to match the connection of the same name on the corresponding Imaging server, including using the same schema.

- g. Test the configuration to ensure everything is valid.
  - h. Click **Finish**.
  - i. On the **Configuration** tab of the Summary of JDBC Data Sources page, click **IPMDS**.
  - j. Click the **Targets** tab.
  - k. Select the name of the Oracle SOA Suite server.
  - l. Click **Save**.
  - m. Return to the **Configuration** tab on the Summary of JDBC Data Sources page, and click **mds-axf**.
  - n. Click the **Targets** tab.
  - o. Select the name of the Oracle SOA Suite server.
  - p. Click **Save**.
3. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, create a `SOALocalTxDataSource` data source on the Imaging server as it is set up on the Oracle SOA Suite server:
- a. Log in to the Administration Console on the Imaging machine.
  - b. Under **Domain Structure** on the left, expand **Services**, and click **Data Sources**.
  - c. On the **Configuration** tab of the Summary of JDBC Data Sources page, select **Generic Data Source** from the **New** menu.
  - d. In the **Name** field, specify `SOALocalTxDataSource`.
  - e. In the **JNDI Name** field, specify `jdbc/SOALocalTxDataSource`.
  - f. Select your database type in the **Database Type** list, and click **Next**.
  - g. Configure values for **Data Source Properties** to match the connection of the same name on the corresponding Oracle SOA Suite server, including using the same schema.
  - h. Test the configuration to ensure everything is valid.
  - i. Click **Next** to select targets.
  - j. Select the name of the Imaging server.
  - k. Click **Finish**.
4. Create the foreign JNDI with the Oracle WebLogic Scripting Tool (WLST):
- a. Change to the `WCC_ORACLE_HOME/axf_bpm/scripts` directory.
  - b. Edit the `create-foreign-JNDI.py` script by using a text editor.
  - c. Set the following variables at the top of the file:

```
host to login to for executing script
var_host = "" # (-h) WebLogic Server Administration Server host name
var_hostPort = "" # (-p) Administration Server port
var_user = "" # (-u) WebLogic Server User Name
var_credential = "" # (-c) WebLogic Server Password
JNDI settings
var_jndiURIServer = "" # (-t) JNDI target URI of Oracle SOA Suite host
var_jndiURIServerPort = "" # (-v) JNDI target URI port
var_serverTargetName = "" # (-s) Managed Server name, for targeting
```



```
the Imaging server
var_jndiUser = "" # (-n) JNDI user name
var_jndiPassword = "" # (-d) JNDI password
```

- d. Save the file.
- e. Run the `create-foreign-JNDI.py` script against the Imaging server with WLST.

The WebLogic Server should be the only server running when you execute the script, as follows:

```
cd WCC_ORACLE_HOME/common/bin
./wlst.sh create-foreign-JNDI.py
```

5. Configure the AXF for BPM CSF key:
  - a. Log in to Oracle Enterprise Manager Fusion Middleware Control.
  - b. Navigate to the WebLogic Server domain and right-click the deployed domain (`base_domain` by default).
  - c. In the resulting menu, select **Security**, and then **Credentials**.
  - d. Create a new map, specify the map name as `oracle.wsm.security`.
  - e. Create a new key:
    - Specify a key name, such as `ipmadmin`.
    - Specify a valid administrator user, such as `weblogic`.
    - Specify the password.
    - Click **OK**.
- [Oracle Coherence Communications for Imaging Clusters, Multiple Domains, or Multiple Machines](#)
- [Oracle Coherence Communications for a Single Server or Domain](#)

#### Oracle Coherence Communications for Imaging Clusters, Multiple Domains, or Multiple Machines

If you are configuring AXF for BPM, you should configure communications with Oracle Coherence, which AXF for BPM utilizes. By default, the server is set up for clustering with the following settings configured in the `DOMAIN_HOME/bin/setDomainEnv.sh` script:

```
-Dtangosol.coherence.clusteraddress=224.3.1.99
-Dtangosol.coherence.clusterport=3199
-Dtangosol.coherence.log=jdk
```

In an Imaging cluster, you need to set up AXF for BPM communications with Oracle Coherence with a unique multicast address and port to avoid unwanted multicast traffic from interfering with the system. For more information about configuring Oracle Coherence in clusters, Using Coherence Clusters in *Oracle Fusion Middleware Developing Applications with Oracle Coherence*

## Oracle Coherence Communications for a Single Server or Domain

For a single-server or domain installation, you can configure Oracle Coherence to avoid the multicast traffic of other machines by editing the `DOMAIN_HOME/bin/setDomainEnv.sh` script as follows:

1. Open the `DOMAIN_HOME/bin/setDomainEnv.sh` script in a text editor.
2. Perform a search for `coherence` to locate existing settings.
3. Append the following two setting after any existing Oracle Coherence settings; for instance, after `-Dtangosol.coherence.log=jdk:`

```
-Dtangosol.coherence.localhost=127.0.0.1
-Dtangosol.coherence.ttl=0
```

4. Save the settings.
5. Restart any running Managed Servers on the domain for the changes to take effect.

## Verifying the AXF for BPM Installation

You can verify the AXF for BPM installation and configuration with the *HelloBPM* solution, which uses a BPM process. This section describes the procedure to deploy and use this solution.

- [Configuring the HelloBPM Solution](#)
- [Importing Definition Files into Imaging](#)
- [Accessing the Solution Administration Page](#)
- [Injecting Tasks into Imaging](#)

## Configuring the HelloBPM Solution

Before you can use the *HelloBPM* solution to validate the installation and configuration of AXF for BPM, you need to deploy and configure the solution on the Imaging Managed Server.

To configure the HelloBPM solution:

1. Set up the database:
  - a. Change to the `WCC_ORACLE_HOME/axf_bpm/scripts` directory.
  - b. Run the `AXF_HELLO_BPM_DATA.sql` script while connected to the Imaging database schema as the Imaging database user, with the following three parameters, which will insert the data necessary to run the HelloBPM solution:
    - `SOAMachineName:Port`
    - `IPMMachineName:Port`
    - `CSFKEY`
2. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, you will need to manually deploy the Hello BPM process. Copy the `WCC_ORACLE_HOME/axf_bpm/bpm/sca_axfHelloBPM_rev1.0.jar` file to `DOMAIN_HOME/soa/autodeploy/` prior to starting the Oracle SOA Suite Managed Server.
3. Start up the remaining servers in the following order:
  - a. Weblogic Server Administration Server (should already be running)
  - b. Oracle SOA Suite Managed Server

- c. Imaging Managed Server
- d. WebCenter Content Managed Server
4. Verify that a URI is set on the deployed process:
  - a. Log in to Oracle Enterprise Manager Fusion Middleware Control.
  - b. Navigate to the Oracle SOA Suite Managed Server, then `soa-infra` (`soa_server1`), and then `default`, and click **axfHelloBPM**.
  - c. In the Component Metrics section, click **SalesQuoteEntry**.
  - d. Click the **Administration** tab.
  - e. If a valid URI is not set, create one with these settings:
    - **Application Name:** `worklist`
    - **Host Name:** The name of the host machine for the server
    - **HTTP Port:** The port of the host machine for the server
    - **HTTPS Port:** The secure port of the host machine for the server, or the default value if SSL is not configured
    - **URI:** `/workflow/axfSolutionHelloBPM/faces/adf.task-flow?_id=SalesQuoteEntry_TaskFlow&_document=WEB-INF/SalesQuoteEntry_TaskFlow.xml`

#### Importing Definition Files into Imaging

You can import definition files for tasks into the Imaging server through the Imaging Injector.

To import definition files into Imaging:

1. Create the connections:
  - a. Log in to Imaging as an administrator user, such as `ipmadmin`.

#### Note:

This first user to connect to the Imaging system is registered as the Imaging administrator. See [Completing the Initial Imaging Configuration](#).

- b. In the navigation tree on the left, expand **Manage Connections**.
- c. Select **Create Content Server Connection** from the drop-down menu, and configure the connection:
  - On the Create Connection: Basic Information page, specify a name for the connection, and click **Next**.
  - On the Create Connection: Content Server Settings page, specify whether to use SSL, then specify whether to use a local Content Server (default) or specify an external server through the Content Server Pool section, and then click **Next**.
  - On the Create Connection: Security page, add the Administrators group with full rights, and click **Next**.
  - Review your settings, and click **Submit**.

- d. Select **Create Workflow Connection** from the drop-down menu, and configure the connection:

- On the Create Connection: Basic Information page, specify a name for the connection, and click **Next**.
- On the Create Connection: Workflow Settings page, specify the following information, and then click **Next**.

**HTTP Front End Address:** Specify the fully qualified HTTP address for the Oracle SOA Suite server:

```
http://managedServerHost:managedServerPort/
```

**Credential Alias:** This should be the CSF key name that was specified in Step 5 of [Configuring and Verifying AXF for BPM](#), such as `ipmadmin`.

**Provider:** Specify the fully qualified t3 address for the Oracle SOA Suite Server:

```
t3://managedServerHost:managedServerPort/
```

- On the Create Connection: Security page, add the `Administrators` group with full rights, and click **Next**.
- Review your settings, and click **Submit**.

2. Import the definition file, `WCC_ORACLE_HOME/axf_bpm/ipm` into Imaging, using the definition import tool.

For more information on uploading definitions and resolving environment configurations, including the repository connection and BPEL server connection as well as the security configurations of the applications, see About Imaging in *Administering Oracle WebCenter Content: Imaging*.

- a. In the navigation tree on the left, expand **Tools**.
- b. Select **Import Definitions**.
- c. Browse to and select the `WCC_ORACLE_HOME/axf_bpm/ipm/HelloBPM.xml` file.
- d. Click **Next**.
- e. On the Select Definitions step, select **Action** for **HelloBPM Application**, **HelloBPM Input**, and **HelloBPM Search**.
- f. Click **Next**.
- g. On the Validation step, select **Choose New** for the **Application Security** field, and select the **Administrators** group. Also, select the **Administrators** group for the **Applications**, **Document Security**, **Inputs Security**, and **Searches Security** fields.
- h. For the **Workflow** field, select **Workflow Connection**.
- i. Click **Submit**.

#### Accessing the Solution Administration Page

Before you can access the Solution Administration page, you need to set up an `axfadmin` group in WebLogic Server and assign your WebLogic Server user name to this group.

To access administration functions for the solution application:

1. Open the new driver page:

`http://machinename:16000/axf/faces/pages/axfadmin.jspx`

2. Click the **Command Driver** link on the left.
3. Use the following values:
  - a. **solutionNamespace:** SalesQuoteEntry
  - b. **commandNamespace:** StartSalesQuoteEntry
4. Click **Execute Request**.
5. Click **Execute Response**.

The Solution Administration page opens. Table 4-1 shows the example parameters for this page.

**Table 4-1 Parameters for the Solution Administration Page**

| Parameter                | Value                          |
|--------------------------|--------------------------------|
| <i>solutionNamespace</i> | SalesQuoteEntry                |
| <i>commandNamespace</i>  | StartSalesQuoteEntry           |
| <i>Username</i>          | The user name for the request. |

You can access the Business Rule Editor through the Solution Administration page and use this editor to perform any customizations.

#### Injecting Tasks into Imaging

After you deploy the AXF for BPM process, you can inject tasks into Imaging either from the content input files, through the Imaging input agent, or from the Oracle SOA Suite server, through Oracle Enterprise Manager Fusion Middleware Control.

You can inject tasks into the HelloBPM solution from content input files that are installed with the AXF for BPM infrastructure. Injecting tasks through the Imaging input agent enables you to test solution application changes. If needed, you can modify the input files to match the HelloBPM workflows.

These content input files are in the following directory with WCC\_ORACLE\_HOME/axf\_bpm/ipm/HelloBPM.xml, the Imaging application definition:

`$WCC_ORACLE_HOME/axf_bpm/ipm/`

This directory includes three input files:

- TestSalesQuote.pdf
- TestSalesQuote.txt
- TestSalesQuote.xml

The following procedure is based on the assumption that InputDirectory is left with the default configuration (/IPM/InputAgent/Input).

To inject tasks through the input agent:

1. Copy the PDF and XML files into the `DOMAIN_HOME` directory, and copy the TXT file into the `DOMAIN_HOME/IPM/InputAgent/Input` directory (default configuration). You also might need to change file permissions so that `InputAgent` has access to these files. See *Enabling Input Agent in Administering Oracle WebCenter Content: Imaging*.

Within the specified time interval (15 minutes by default), the input agent picks up the input files and creates a document with metadata values from the text input file, an image from the PDF file, and supporting content from the XML file.

Based on the workflow configuration in place with the HelloBPM solution, a task is created for the document that displays in the BPM task list.

2. In the task list, click the newly injected task to view its details in the solution application.
3. As needed, modify the metadata values in the text input file before injecting the input files again. For example, you might inject a task with missing account information to work with its human task flow.

## Configuring and Verifying AXF for BPEL

To configure AXF for BPEL to work with Imaging Managed Servers that run in a cluster or other distributed configuration, you need to configure the Java Object Cache (JOC) to be distributed to all of the Managed Servers. See *Clustering for AXF in Imaging Managed Servers*.

For verification that the AXF for BPEL infrastructure is properly installed, AXF for BPEL includes two simple solutions:

- `HelloWorld`, a basic solution that returns a `Hello` string.
- `HelloBpel`, a solution that includes a BPEL process to verify the BPEL integration.
- [Verifying the AXF for BPEL Installation and Configuration with HelloWorld](#)
- [Verifying the AXF for BPEL Installation and Configuration with HelloBpel](#)

## Verifying the AXF for BPEL Installation and Configuration with HelloWorld

Follow these steps to enable the `HelloWorld` solution:

1. As user who owns the Imaging schema, run the `insertHelloCommand.sql` script from one of the following directories.

- **UNIX path:**

```
MW_HOME/WCC_ORACLE_HOME/axf/drivers/HelloWorld/dbscripts
```

- **Windows path:**

```
MW_HOME\WCC_ORACLE_HOME\axf\drivers\HelloWorld\dbscripts
```

### Note:

For IBM DB2 only, add the following line to beginning of the `insertHelloCommand.sql` script before you run it:

```
CONNECT TO soadb USER am3_ipm USING oracle;
```

2. Access the driver page of the AXF for BPEL web application using the following URL:

`http://host:port/imaging/faces/Driver.jspx`

3. Enter the following values:

- **Solution Namespace:** HelloWorld
- **Command Namespace:** Hi
- **User Name:** jcooper

 **Note:**

This user name is valid only if you are using the application server's built-in `jazn.xml` security.

4. Click **Execute Command**.

An AXF for BPEL response should display with a populated **Conversation ID**. If the response is returned, the AXF for BPEL infrastructure is functioning correctly, and commands can be added and executed.

## Verifying the AXF for BPEL Installation and Configuration with HelloBpel

The `HelloBpel` solution includes a BPEL process and a SQL script to set up the `HelloBPEL` solution namespace for use by that process. The BPEL process and database script are in the following directories.

- **UNIX path:**

`MW_HOME/WCC_ORACLE_HOME/axf/drivers/HelloBpel`

- **Windows path:**

`MW_HOME\WCC_ORACLE_HOME\axf\drivers\HelloBpel`

To enable the `HelloBpel` solution:

1. Run one of the following `HelloBPEL` SQL scripts:

- **UNIX scripts:**

`MW_HOME/WCC_ORACLE_HOME/axf/drivers/HelloBpel/dbscripts  
/oracle/insertHelloBPELData.sql`

`MW_HOME/WCC_ORACLE_HOME/axf/drivers/HelloBpel/dbscripts  
/sqlserver-db2/insertHelloBPELData.sql`

- **Windows scripts:**

```
MW_HOME\WCC_ORACLE_HOME\axf\drivers\HelloBpel\dbscripts
\oracle\insertHelloBPELData.sql
```

```
MW_HOME\WCC_ORACLE_HOME\axf\drivers\HelloBpel\dbscripts
\sqlserver-db2\insertHelloBPELData.sql
```

If you are using Oracle Database, then run the script from the `oracle` directory.

If you are using an IBM DB2 or Microsoft SQL Server database, then run the script from the `sqlserver-db2` directory.

For IBM DB2 only, before you run the `HelloBPEL` SQL script, make the following changes to it:

- Add this line to beginning of the script:

```
CONNECT TO soadb USER am3_ipm USING oracle;
```

- Change the following line to specify whatever the actual BPEL connection is in the Imaging Manage Connections section:

```
Insert into AXF_SOLUTION_ATTRIBUTES
(SOLUTION_NAMESPACE,PARAMETER_KEY,PARAMETER_VALUE) values
('HelloBPEL','BPEL_CONNECTION','test');
```

2. Run the `insertHelloBPELData.sql` script.
3. With Oracle JDeveloper, open `HelloBPEL.jws` from following directory:

- **UNIX path:**

```
MW_HOME/WCC_ORACLE_HOME/axf/drivers/HelloBpel/bpel
```

- **Windows path:**

```
MW_HOME\WCC_ORACLE_HOME\axf\drivers\HelloBpel\bpel
```

Deploy the process to your BPEL server. For assistance with this task, consult the JDeveloper documentation.

 **Note:**

The `HelloBPEL` sample solution assigns instances to a group named `California` by default. You need to add the `California` group to the `myrealm` security realm through the Oracle WebLogic Server Administration Console.

If you are using an alternate identity store, such as Oracle Internet Directory, you can change the group assignment by modifying the `HelloBpelHumanTask.task` file within JDeveloper before deployment.



4. Access the driver page of the AXF for BPEL web application by using the following URL:

```
http://host:port/imaging/faces/Driver.jspx
```

5. In the AXF Command Driver screen, enter the following values:

- **Solution Namespace:** HelloBPEL
- **Command Namespace:** StartHelloBPEL
- **User Name:** A valid Imaging user; for example, weblogic

The preceding Imaging user needs to be part of a group named California. If this group does not exist, then create it, and add the user to the group.

6. Click **Execute Command**.

A response should be displayed in the response screen.

7. Click **Execute Response**, and sign in when prompted.

The AXF Task List screen should be displayed. If there are no tasks in the task list, open the BPEL Console, create a new instance of `HelloBPELProcess`, and refresh the task list.

## Configuring Capture

The Capture System Administrator requires system administration privileges to configure and monitor an Oracle WebCenter Enterprise Capture system environment. The configuration consists of tasks such as starting the Capture Managed Server, assigning roles to Capture users in Fusion Middleware Control, and modifying system-level settings through MBeans.

This appendix explains the configuration tasks in detail.

- [About Completing the Oracle WebCenter Enterprise Capture Configuration](#)  
The Capture System Administrator who performs the installation and initial configuration must have system administration permissions, including access to Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server. Before anyone can use Oracle WebCenter Enterprise Capture, a system administrator must associate users from the LDAP credential store for the WebLogic Server domain with the Capture roles in Fusion Middleware Control.
- [Completing the Initial Configuration of Oracle WebCenter Enterprise Capture](#)  
The Capture System Administrator performs the initial configuration of Capture in a WebLogic Server domain. In addition to starting the Capture Managed Server, the configuration steps also include assigning roles to users and modifying system-level settings.

## About Completing the Oracle WebCenter Enterprise Capture Configuration

The Capture System Administrator who performs the installation and initial configuration must have system administration permissions, including access to Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server. Before anyone can use Oracle WebCenter Enterprise Capture, a system administrator must associate users from the LDAP credential store for the WebLogic Server domain with the Capture roles in Fusion Middleware Control.

The roles `CaptureWorkspaceManager`, `CaptureWorkspaceViewer`, and `CaptureUser` are automatically added to the default WebLogic Server policy store for the domain. The Capture System Administrator can use the file/XML-based policy store, an Oracle Internet Directory policy store, or an Oracle Database policy store and manage the policy store through Fusion Middleware Control.

Through Fusion Middleware Control, you can also configure system settings and loggers for Capture.

## Completing the Initial Configuration of Oracle WebCenter Enterprise Capture

The Capture System Administrator performs the initial configuration of Capture in a WebLogic Server domain. In addition to starting the Capture Managed Server, the configuration steps also include assigning roles to users and modifying system-level settings.

- [Starting the Capture Managed Server](#)
- [Assigning Roles to Capture Users](#)
- [Modifying System-Level Settings](#)

### Starting the Capture Managed Server

The first step to complete Capture configuration is to start the Capture Managed Servers.

### Assigning Roles to Capture Users

Before anyone can use Capture, the Capture System Administrator needs to assign users from the LDAP credential store to the Capture roles in the policy store. You can do this through the Application Roles page in Fusion Middleware Control.

To assign roles to Capture users, see *Assigning Capture Roles in Oracle Enterprise Manager in Oracle Fusion Middleware Administering Oracle WebCenter Enterprise Capture*.

### Modifying System-Level Settings

You can modify system-level configuration settings for Capture, including system properties and SMTP settings for e-mail, through Fusion Middleware Control. The settings on this page configure the Capture MBeans for the domain, which you can also modify with Oracle WebLogic Scripting Tool (WLST) commands.

The following WLST commands also enable you to access or modify system-level settings:

- `listCaptureConfig`
- `getCaptureConfig`
- `setCaptureConfig`

These are online WLST commands that you can use while connected to the Administration Server for the domain. To connect, you need to run the `wlst.sh` script from the Oracle WebCenter Content home directory.

To modify a Capture system-level setting with a WLST command:

1. Start the Administration Server for your Oracle WebLogic Server domain.
2. Sign in to the Oracle WebLogic Server Administration Server.
3. Navigate to the Oracle WebCenter Content home directory at `MW_HOME/WCC_ORACLE_HOME`

**4. Run WLST.**

```
cd common/bin
./wlst.sh
```

**5. Sign in and then enter a custom Capture command:**

```
wls:/offline> connect()
Please enter your username :weblogic
Please enter your password : XXXXXXXXXXXXX
Please enter your server URL [t3://localhost:7001]
:t3://host_name:16401
Connecting to t3://host_name:16401 with userid weblogic ...
Successfully connected to Managed Server 'capture_server1' that
belongs to domain
'domainName'.

wls:/domainName/serverConfig>
setCaptureConfig('CaptureSystemID','CAPTURE_02')

Attribute 'CaptureSystemID' changed to "CAPTURE_02"

wls:/domainName/serverConfig> exit()
```

# 5

## Next Steps After Configuring the Domain

After you configure a product domain, there are additional tasks that you may want to perform.

- [Performing Basic Administrative Tasks](#)  
After you configure your new domain, there are administration tasks that Oracle recommends you perform on the domain.
- [Performing Additional Domain Configuration Tasks](#)  
Review additional configuration tasks you will likely want to perform on a new domain.
- [Preparing Your Environment for High Availability](#)  
Scaling out for high availability requires additional steps.
- [Configuring WebCenter Content User Interface on Additional Nodes](#)  
If you install WebCenter Content User Interface on one node, its configuration is complete. However, if you scale out WebCenter Content User Interface to a second node (in a high availability or enterprise deployment topology, for example), you must complete additional configuration steps.
- [Setting the WebCenter Content User Interface Server Socket Port](#)  
If you are scaling out WebCenter Content User Interface you must change the server socket port.
- [Configuring WebCenter Content User Interface Settings](#)  
You set WebCenter Content User Interface connection and configuration settings with WLST or Fusion Middleware Control.

## Performing Basic Administrative Tasks

After you configure your new domain, there are administration tasks that Oracle recommends you perform on the domain.

The following table lists common administration tasks to perform on your new domain.

**Table 5-1 Basic Administration Tasks for a New Domain**

| Task                                                         | Description                                                                                                                 | More Information                                                                                                                          |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Getting familiar with Fusion Middleware administration tools | Get familiar with various tools that you can use to manage your environment.                                                | See Overview of Oracle Fusion Middleware Administration Tools in <i>Oracle Fusion Middleware Administering Oracle Fusion Middleware</i> . |
| Starting and stopping products and servers                   | Learn how to start and stop Oracle Fusion Middleware, including the Administration Server, Managed Servers, and components. | See Starting and Stopping Oracle Fusion Middleware in <i>Oracle Fusion Middleware Administering Oracle Fusion Middleware</i> .            |

**Table 5-1 (Cont.) Basic Administration Tasks for a New Domain**

| Task                                         | Description                                                                                      | More Information                                                                                                            |
|----------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Configuring Secure Sockets Layer (SSL)       | Learn how to set up secure communications between Oracle Fusion Middleware components using SSL. | See Configuring SSL in Oracle Fusion Middleware in <i>Oracle Fusion Middleware Administering Oracle Fusion Middleware</i> . |
| Monitoring Oracle Fusion Middleware          | Learn how to keep track of the status of Oracle Fusion Middleware components.                    | See Monitoring Oracle Fusion Middleware in <i>Oracle Fusion Middleware Administering Oracle Fusion Middleware</i> .         |
| Understanding Backup and Recovery Procedures | Learn recommended backup and recovery procedures for Oracle Fusion Middleware.                   | See Introducing Backup and Recovery in <i>Oracle Fusion Middleware Administering Oracle Fusion Middleware</i> .             |

## Performing Additional Domain Configuration Tasks

Review additional configuration tasks you will likely want to perform on a new domain.

**Table 5-2 Additional Domain Configuration Tasks**

| Task                                       | Description                                                                                                                                                                                                                  | More Information                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deploying Applications                     | Learn how to deploy your applications to Oracle Fusion Middleware.                                                                                                                                                           | See Deploying Applications in <i>Oracle Fusion Middleware Administering Oracle Fusion Middleware</i> .                                                                                                                                                                                                                                  |
| Adding a Web Tier front-end to your domain | Oracle Web Tier hosts Web pages (static and dynamic), provides security and high performance along with built-in clustering, load balancing, and failover features. In particular, the Web Tier contains Oracle HTTP Server. | To install and configure Oracle HTTP Server in the WebLogic Server domain, see Configuring Oracle HTTP Server in a WebLogic Server Domain in <i>Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server</i> .<br><br>See also <a href="#">Installing Multiple Products in the Same Domain</a> for important information. |

**Table 5-2 (Cont.) Additional Domain Configuration Tasks**

| Task                                               | Description                                                                                                                                                                                                                                                                                                                              | More Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tuning and configuring Coherence for your topology | The standard installation topology includes a Coherence cluster that contains storage-enabled Managed Coherence Servers. This configuration is a good starting point for using Coherence, but depending upon your specific requirements, consider tuning and reconfiguring Coherence to improve performance in a production environment. | <p>For more information about Coherence clusters, see <i>Configuring and Managing Coherence Clusters in Oracle Fusion Middleware Administering Clusters for Oracle WebLogic Server</i>.</p> <p>For information on tuning Coherence, see <i>Performance Tuning in Oracle Fusion Middleware Administering Oracle Coherence</i>.</p> <p>For information on storing HTTP session data in Coherence, see <i>Using Coherence*Web with WebLogic Server in Oracle Fusion Middleware Administering HTTP Session Management with Oracle Coherence*Web</i>.</p> <p>For more about creating and deploying Coherence applications, see <i>Getting Started in Oracle Fusion Middleware Developing Oracle Coherence Applications for Oracle WebLogic Server</i>.</p> |

## Preparing Your Environment for High Availability

Scaling out for high availability requires additional steps.

[Table 5-3](#) provides a list of tasks to perform if you want to scale out your standard installation environment for high availability.

**Table 5-3 Tasks Required to Prepare Your Environment for High Availability**

| Task                                                        | Description                                                                                                                                                                                                                      | More Information                                                                                                                                                                                  |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scaling out to multiple host computers                      | To enable high availability, it is important to provide failover capabilities to another host computer. That way, if one computer goes down, your environment can continue to serve the consumers of your deployed applications. | See <i>Scaling Out a Topology (Machine Scale Out)</i> in the <i>Oracle Fusion Middleware High Availability Guide</i> .                                                                            |
| Configuring high availability for your Web Tier components. | If you have added a Web tier front-end, then you must configure the Web Tier for high availability, as well as the WebLogic Server software.                                                                                     | See <i>Configuring High Availability for Web Tier Components</i> in the <i>Oracle Fusion Middleware High Availability Guide</i> .                                                                 |
| Setting up a front-end load balancer                        | A load balancer can be used to distribute requests across servers more evenly.                                                                                                                                                   | See <i>Server Load Balancing in a High Availability Environment and Configuring Load Balancer Virtual Server Names and Ports</i> in the <i>Oracle Fusion Middleware High Availability Guide</i> . |

**Table 5-3 (Cont.) Tasks Required to Prepare Your Environment for High Availability**

| Task                     | Description                                                                                                                                                                                                                                                                                                                       | More Information                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Configuring Node Manager | Node Manager enables you to start, shut down, and restart the Administration Server and Managed Server instances from a remote location. This document assumes you have configured a per-domain Node Manager. Review the Node Manager documentation, for information on advanced Node Manager configuration options and features. | See Advanced Node Manager Configuration in <i>Oracle Fusion Middleware Administering Node Manager for Oracle WebLogic Server</i> . |

## Configuring WebCenter Content User Interface on Additional Nodes

If you install WebCenter Content User Interface on one node, its configuration is complete. However, if you scale out WebCenter Content User Interface to a second node (in a high availability or enterprise deployment topology, for example), you must complete additional configuration steps.

To run WebCenter Content User Interface on additional nodes, you must:

- Enable WebCenter Content User Interface components.
- Set the server socket port to 4444.

To enable WebCenter Content User Interface components:

1. Sign in to WebCenter Content as a WebCenter Content administrator.
2. From the Administration tray or menu, choose **Admin Server**, then **Component Manager**.
3. On the Component Manager page, select all three components under WebCenter Content UI Components:
  - **AutoSuggestConfig**
  - **DynamicConverter**
  - **FrameworkFolders**
4. Click **Update** then click **OK** to confirm that you want to enable the components.
5. Restart WebCenter Content. See Starting and Stopping Managed Servers in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

Continue to the topic [Setting the WebCenter Content User Interface Server Socket Port](#).

## Setting the WebCenter Content User Interface Server Socket Port

If you are scaling out WebCenter Content User Interface you must change the server socket port.

To change the server socket port:

1. Open `WCC_DOMAIN/ucm/cs/config/config.cfg`
2. Set `IntradocServerPort` to 4444.

```
IntradocServerPort=4444
```

## Configuring WebCenter Content User Interface Settings

You set WebCenter Content User Interface connection and configuration settings with WLST or Fusion Middleware Control.

- [Setting Connection Attributes with WLST](#)  
You can use `displayRIDCConnection` and `updateRIDCConnection` WLST commands to read and update connection properties.
- [Setting Connection Attributes with Fusion Middleware Control](#)  
Instead of using WLST, you can set connection attributes for WebCenter Content User Interface Managed Server with the Fusion Middleware Control System MBean Browser.
- [Setting Configuration Attributes with WLST](#)  
You can use WLST commands `displayWccAdfConfig` and `updateWccAdfConfig` to read and update WebCenter Content User Interface configuration parameters.
- [Setting Configuration Attributes with Fusion Middleware Control](#)  
Instead of using WLST, you can set configuration (**WccAdfConfiguration**) attributes for WebCenter Content User Interface Managed Server with the Fusion Middleware Control System MBean Browser.

## Setting Connection Attributes with WLST

You can use `displayRIDCConnection` and `updateRIDCConnection` WLST commands to read and update connection properties.

For example, to update the RIDC connection to the WebCenter Content User Interface Managed Server:

1. Run WLST from `ORACLE_HOME/oracle_common/common/bin/wlst.sh`.
2. Enter `wls:/offline> connect ()` and enter your username and password at the prompt.
3. Enter the Managed Server URL, for example, `t3://localhost:16225`
4. Update the RIDC connection to the WebCenter Content User Interface Managed Server. For example:



```
wls:/mydomain/serverConfig>updateRIDCConnection('Oracle
WebCenter Content - Web
UI', 'WccAdfServerConnection', connUrl='idc://
contentserver_host:intradoc_port', credUsername='ucm_admin_us
er')
```

5. Restart the Managed Server.

## Setting Connection Attributes with Fusion Middleware Control

Instead of using WLST, you can set connection attributes for WebCenter Content User Interface Managed Server with the Fusion Middleware Control System MBean Browser.

To set connection attributes through Fusion Middleware Control:

1. Sign in to Fusion Middleware Control for the WebCenter Content User Interface Managed Server.
2. In the navigation tree on the left, expand **WebLogic Domain**, then the WebCenter Content User Interface domain folder, then the cluster name, and then click Managed Server name.
3. From the WebLogic Domain drop-down menu at the top of the Managed Server page, choose System MBean Browser.
4. In the System MBean Browser navigation tree, navigate to the **WccAdfServerConnection** MBean. To do this, expand **Application Defined MBeans** → **oracle.adf.share.connections** → **Server: WCCADF\_server1** → **Application: Oracle WebCenter Content – Web UI**. Expand the Mbean **ADFConnections** then the folder **WccConnection**.
  - Instead of opening up the folder, you can enter the connection name **WccAdfServerConnection** in the MBean filtered search.
5. Click the MBean **WccAdfServerConnection**.
6. In the **Attributes** tab, select **PropConnectionURL**. Enter a URL to set up the RIDC connection. Click **Apply** (top right)

If you leave the **PropConnectionSocketTimeout** attribute blank, the default (60 seconds) becomes the RIDC Connection Socket Timeout value. This value can create problems if you download large files that are being converted to TIFF or PDF documents with annotations burned in. You can set the attribute to a larger value if you have large files.

7. Go back to the **ADFConnections** page (**Application Defined MBeans** **oracle.adf.share.connections** **Server: WCCADF\_server1** **Application: Oracle WebCenter Content – Web UI** **ADFConnections**).
8. On the Operations tab, click save. Then click **Invoke**.
9. Restart the WebCenter Content User Interface Managed Server.

## Setting Configuration Attributes with WLST

You can use WLST commands `displayWccAdfConfig` and `updateWccAdfConfig` to read and update WebCenter Content User Interface configuration parameters.

For example, to use `updateWccAdfConfig` to update the application's URL:

1. Run WLST from `ORACLE_HOME/oracle_common/common/bin/wlst.sh`.
2. Enter `wls:/offline> connect()` and enter your username and password at the prompt.
3. Enter the Managed Server URL, for example, `t3://localhost:16225`.
4. Update the WebCenter Content User Interface Managed Server. For example:  

```
wls:/mydomain/serverConfig>updateWccAdfConfig('Oracle WebCenter
Content - Web UI',applicationUrl='idc://
contentserver_host:intradoc_port')
```
5. Restart the WebCenter Content User Interface Managed Server.

## Setting Configuration Attributes with Fusion Middleware Control

Instead of using WLST, you can set configuration (**WccAdfConfiguration**) attributes for WebCenter Content User Interface Managed Server with the Fusion Middleware Control System MBean Browser.

For example, to set the WebCenter Content User Interface application URL:

1. Sign in to Fusion Middleware Control for the WebCenter Content User Interface Managed Server.
2. In the navigation tree on the left, expand **WebLogic Domain**, then the WebCenter Content User Interface domain folder, then the cluster name, and then click Managed Server name.
3. From the WebLogic Domain drop-down menu at the top of the Managed Server page, choose System MBean Browser.
4. In the System MBean Browser navigation tree, navigate to the **WccAdfConfiguration** MBean. To do this, expand **Application Defined MBeans** —> **oracle.adf.share.config** —> **Server: WCCADF\_server1** —> **Application: Oracle WebCenter Content – Web UI**. Expand the folder **ADFConfig**, the Mbean **ADFConfig**, then the folder **ADFConfig**.
  - Instead of opening up a series of folders to reach the MBean, you can enter the connection name **WccAdfConfiguration** in the MBean filtered search.
5. Click the MBean **WccAdfConfiguration**.
6. In the **Attributes** tab, select **ApplicationUrl**. In the **Value** field, enter the base application URL. For example: `https://wcc.example.com:16225`. Click **Apply** (top right).
7. Go back to the **ADFConfig** MBean page (**Application Defined MBeans** —> **oracle.adf.share.config** —> **Server: WCCADF\_server1** —> **Application: Oracle WebCenter Content – Web UI** —> **ADFConfig**).
8. On the Operations tab, click save then **Invoke**.
9. Restart the WebCenter Content User Interface Managed Server.

# 6

## Uninstalling or Reinstalling Oracle WebCenter Content

Follow the instructions in this section to uninstall or reinstall Oracle WebCenter Content.

Oracle recommends that you always use the instructions in this section to remove the software. If you try to remove the software manually, you may encounter problems when you try to reinstall the software again at a later time. Following the procedures in this section ensures that the software is properly removed.

- [About Product Uninstallation](#)  
The Oracle Fusion Middleware uninstaller removes the software from the Oracle home directory.
- [Stopping Oracle Fusion Middleware](#)  
Before running the Uninstall Wizard, Oracle recommends that you stop all servers and processes associated with the Oracle home you are going to remove.
- [Removing Your Database Schemas](#)  
Before you remove the Oracle home, Oracle recommends that you run the Repository Creation Utility (RCU) to remove database schemas associated with this domain.
- [Uninstalling the Software](#)  
Follow the instructions in this section to start the Uninstall Wizard and remove the software.
- [Removing the Oracle Home Directory Manually](#)  
After you uninstall the software, you must manually remove your Oracle home directory and any existing subdirectories that the Uninstall Wizard did not remove.
- [Removing the Program Shortcuts on Windows Operating Systems](#)  
On Windows operating systems, you must also manually remove the program shortcuts; the Deinstallation Wizard does not remove them for you.
- [Removing the Domain and Application Data](#)  
After you uninstall the software, you must remove the domain and application data.
- [Reinstalling the Software](#)  
You can reinstall your software into the same Oracle home as a previous installation only if you uninstalled the software by following the instructions in this section, including manually removing the Oracle home directory.

### About Product Uninstallation

The Oracle Fusion Middleware uninstaller removes the software from the Oracle home directory.

The following table summarizes the tasks to uninstall Fusion Middleware products.

**Table 6-1 Roadmap for Product Uninstallation**

| Task                                    | Description                                                                                                                                                                                                         | Documentation                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Stop Oracle Fusion Middleware           | All servers and processes in your domain should be stopped before running the uninstaller.                                                                                                                          | See <a href="#">Stopping Oracle Fusion Middleware</a> .           |
| Remove your database schemas            | Run Repository Creation Utility to remove your database schemas.                                                                                                                                                    | See <a href="#">Removing Your Database Schemas</a> .              |
| Remove the software                     | Run the product uninstaller to remove Oracle Fusion Middleware Infrastructure.<br><br>Note that if your Oracle home contains multiple products, you must run the uninstaller multiple times, once for each product. | See <a href="#">Uninstalling the Software</a> .                   |
| Remove the Oracle home directory        | The uninstaller does not remove all files and folders from the Oracle home directory. After the uninstaller is finished, you must manually remove the Oracle home to complete your product removal.                 | See <a href="#">Removing the Oracle Home Directory Manually</a> . |
| Remove your domain and application data | The uninstaller does not remove data contained in your Domain home or Application home directories, even if they are located inside the Oracle home. You must remove these directories manually.                    | See <a href="#">Removing the Domain and Application Data</a> .    |

## Stopping Oracle Fusion Middleware

Before running the Uninstall Wizard, Oracle recommends that you stop all servers and processes associated with the Oracle home you are going to remove.

See Stopping an Oracle Fusion Middleware Environment in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

## Removing Your Database Schemas

Before you remove the Oracle home, Oracle recommends that you run the Repository Creation Utility (RCU) to remove database schemas associated with this domain.

Each domain has its own set of schemas, uniquely identified by a custom prefix. For more information about custom prefixes, see About Custom Prefixes in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*. This set of schemas cannot be shared with any other domain. For more information about creating schemas with the RCU, see Planning Your Schema Creation in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

If there are multiple sets of schemas on your database, be sure to identify the schema prefix associated with the domain that you are removing.

For schema removal steps, see Dropping Schemas in *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

## Uninstalling the Software

Follow the instructions in this section to start the Uninstall Wizard and remove the software.

If you want to uninstall the product in a silent (command-line) mode, see *Running the Oracle Universal Installer for Silent Uninstallation in Oracle Fusion Middleware Installing Software with the Oracle Universal Installer*.

- [Starting the Uninstall Wizard](#)
- [Selecting the Product to Uninstall](#)
- [Navigating the Uninstall Wizard Screens](#)

### Starting the Uninstall Wizard

To start the Uninstall Wizard:

1. Change to the following directory:  
(UNIX) `ORACLE_HOME/oui/bin`  
(Windows) `ORACLE_HOME\oui\bin`
2. Enter the following command:  
(UNIX) `./deinstall.sh`  
(Windows) `deinstall.cmd`

### Selecting the Product to Uninstall

Because multiple products exist in the Oracle home, ensure that you are uninstalling the correct product.

After you run the Uninstall Wizard, the Distribution to Uninstall screen opens. From the dropdown menu, select **fmw\_12.2.1.4.0\_wccontent.jar** and click **Uninstall**. The uninstallation program shows the screens listed in [Navigating the Uninstall Wizard Screens](#).



#### Note:

You can uninstall Oracle Fusion Middleware Infrastructure after you uninstall Oracle WebCenter Content software by running the Uninstall Wizard again. Before doing so, make sure that there are no other products using the Infrastructure; those products will no longer function once the Infrastructure is removed. You will not encounter the Distribution to Uninstall screen if no other software depends on Oracle Fusion Middleware Infrastructure. See *Uninstalling Oracle Fusion Middleware Infrastructure in Oracle Fusion Middleware Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

### Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software.

If you need help on screen listed in [Table 6-2](#), click **Help** on the screen.

**Table 6-2 Uninstall Wizard Screens and Descriptions**

| Screen             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Welcome            | Introduces you to the product Uninstall Wizard.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Uninstall Summary  | <p>Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory.</p> <p>If you want to save these options to a response file, click <b>Save Response File</b> and enter the response file location and name. You can use the response file later to uninstall the product in silent (command-line) mode. See <i>Running the Oracle Universal Installer for Silent Uninstall</i> in <i>Installing Software with the Oracle Universal Installer</i>.</p> <p>Click <b>Deinstall</b>, to begin removing the software.</p> |
| Uninstall Progress | Shows the uninstallation progress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Uninstall Complete | Appears when the uninstallation is complete. Review the information on this screen, then click <b>Finish</b> to close the Uninstall Wizard.                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Removing the Oracle Home Directory Manually

After you uninstall the software, you must manually remove your Oracle home directory and any existing subdirectories that the Uninstall Wizard did not remove.

For example, if your Oracle home directory is `/home/Oracle/product/ORACLE_HOME` on a UNIX operating system, enter the following commands:

```
cd /home/Oracle/product
rm -rf ORACLE_HOME
```

On a Windows operating system, if your Oracle home directory is `C:\Oracle\Product\ORACLE_HOME`, use a file manager window and navigate to the `C:\Oracle\Product` directory. Right-click on the `ORACLE_HOME` folder and select **Delete**.

## Removing the Program Shortcuts on Windows Operating Systems

On Windows operating systems, you must also manually remove the program shortcuts; the Deinstallation Wizard does not remove them for you.

To remove the program shortcuts on Windows:

1. Change to the following directory:  
`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Oracle\ORACLE_HOME\Product`
2. If you only have one product installed in your Oracle home, delete the `ORACLE_HOME` directory. If you have multiple products installed in your Oracle home, delete all products before you delete the `ORACLE_HOME` directory.

## Removing the Domain and Application Data

After you uninstall the software, you must remove the domain and application data.

To remove the domain and application data:

1. Manually remove your Domain home directory. For example:

On a UNIX operating system, if your Domain home directory is `/home/Oracle/config/domains/wcc_domain`, enter the following command:

```
cd /home/Oracle/config/domains
rm -rf wcc_domain
```

On a Windows operating system, if your Domain home directory is `C:\Oracle\Config\domains\wcc_domain`, use a file manager window and navigate to the `C:\Oracle\Config\domains` directory. Right-click on the `wcc_domain` folder and select **Delete**.

2. Manually remove your Application home directory. For example:

On a UNIX operating system, if your Application home directory is `/home/Oracle/config/applications/wcc_domain`, enter the following commands:

```
cd /home/Oracle/config/applications
rm -rf wcc_domain
```

On a Windows operating system, if your Application home directory is `C:\Oracle\Config\applications\wcc_domain`, use a file manager window and navigate to the `C:\Oracle\Config\applications` directory. Right-click on the `wcc_domain` folder and select **Delete**.

3. Back up the `domain_registry.xml` file in your Oracle home, then edit the file and remove the line associated with the domain that you are removing. For example, to remove the `wcc_domain`, find the following line and remove it:

```
<domain location="/home/Oracle/config/domains/wcc_domain"/>
```

Save and exit the file when you are finished.

## Reinstalling the Software

You can reinstall your software into the same Oracle home as a previous installation only if you uninstalled the software by following the instructions in this section, including manually removing the Oracle home directory.

When you reinstall, you can then specify the same Oracle home as your previous installation.

If ODI is installed again in the same location where it was previously deleted, delete the entire Oracle Home where it was previously installed.

Consider the following cases where the Oracle home is not empty:

- Installing in an existing Oracle home that contains the same feature sets.  
The installer warns you that the Oracle home that you specified during installation already contains the same software you are trying to install.
- Installing in an existing, non-empty Oracle home.

For example, suppose you chose to create your Domain home or Application home somewhere inside your existing Oracle home. This data is not removed when you uninstall a product, so if you try to reinstall into the same Oracle home, the installer does not allow it. Your options are:

- Uninstall your software from the Oracle home (as this section describes) and then remove the Oracle home directory. After you uninstall the software and remove the Oracle home directory, you can reinstall and reuse the same Oracle home location. Any domain or application data that was in the Oracle home must be re-created.
- Select a different Oracle home directory.



# A

## Configuring Content Server

You can configure Content Server for Desktop, Records Management, and Oracle iPlanet Web Server.

- [Configuring the Content Server for Desktop](#)  
You need to make sure the CoreWebdav system component is enabled, before the client can use the WebCenter Content Desktop with the Content Server.
- [Configuring Records Management in Content Server](#)  
If you are licensed to configure the Records Management in a WebCenter Content Managed Server, you can configure either a standalone Records Management, a universal (or fully functional) Records Management, or the Oracle URM Adapter in Content Server after you configure the WebCenter Content Records Managed Server.
- [About Configuring Oracle iPlanet Web Server as a Web Tier and Configuring Shared Folders](#)  
You can configure the Oracle iPlanet Web Server as a web tier for WebCenter Content. If you are using a cluster of WebCenter Content Managed Servers, you need to configure a shared file system for the WebCenter Content cluster.

## Configuring Records Management in Content Server

If you are licensed to configure the Records Management in a WebCenter Content Managed Server, you can configure either a standalone Records Management, a universal (or fully functional) Records Management, or the Oracle URM Adapter in Content Server after you configure the WebCenter Content Records Managed Server.

- The ContentFolios component is required for access to the Records Management web interface. This component is enabled automatically when you configure Records Management in the Content Server.
- Do not disable the ContentFolios component.

If you don't want to use Records Management in the Content Server, you can remove the configuration user interface by disabling the RMFeatureConfig component. Before you disable the Records Management and restart the Content Server, you need to delete the Report template files that Records Management installs. You cannot delete them after Records Management is disabled.

To configure Records Management in the Content Server:

1. From the **Administration** menu, choose **Configure Records Settings** to go to the Records Management Setup checklist, then click **Configure Installation**.
2. On the Enabled Features page, select a Records Management option, and click **Submit**.
  - **None:** No Records Management functionality is configured.
  - **Standalone:** Enables basic Records Management functionality on Content Server.
  - **Universal:** Enables full Records Management functionality on Content Server. This includes Physical and External sources.

- **Adapter:** Enables Universal Content Management Adapter functionality on Content Server.
3. Restart the WebCenter Content Managed Server. See Starting and Stopping Managed Servers.

After you restart the WebCenter Content, Records Management Setup checklist appears.

4. If you selected **Adapter**, click **Register Source** on the Enabled Features page then enter values for the fields on the Register Source page:

| Option              | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Provider Name       | Outgoing provider used to connect to the Records Managed Server. You can choose from the list of current outgoing providers, or you can click <b>Add</b> and create one. The provider dialog box shows an abbreviated list of provider fields.<br><br>You can also add providers from the regular Providers page. To view information about an existing provider, click <b>Info</b> in the Action column. |
| Source Name         | Name of the external source to be added to the Records Managed Server. The source name is required and cannot contain spaces.                                                                                                                                                                                                                                                                             |
| Source Table Name   | Prefix to use for creating database tables. The default value is the source name.                                                                                                                                                                                                                                                                                                                         |
| Source Display Name | Caption to use for showing the source name. Default value is the source name.                                                                                                                                                                                                                                                                                                                             |

5. Click **Register**.

Before the source is registered, the following tests are run:

- Validate the provider and test the connection to the Records Managed Server.
- Validate the specified source values

Compare the retention schedules of the adapter and the Records Managed Server to determine if any items in the adapter are missing in the Records server. Before you can register the source, you must resolve any differences on the Import Retention Schedule page.

The retention schedule needs to be synchronized between the adapter and server. By default, all of the items that need to be resolved will be imported into the Records server. You will also have the option of deleting any of the items instead of importing them into the server. Before any items are imported or deleted, backups of retention schedules are made on both the adapter and the Records server, and the backups are checked in to Content Server.

6. After the source is successfully registered, click **OK** on the confirmation page.

After the source is registered, the Retention Schedule and Upload Content task will run in the background.

7. Configure the adapter in the Configuration Wizard:

**Table A-1 Adapter Options**

| Option                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure Custom Fields   | <p>Page where you enter custom fields on the external source. When you add or edit custom fields, you map them to existing document metadata fields defined in Content Server. You can use the same name for each field as defined in Content Serve, or you can rename the field. When the content is uploaded to the Records server as external content items, these fields map to their external field names.</p> <p>You can configure the following custom fields:</p> <ul style="list-style-type: none"> <li>• Add or edit an external custom field</li> <li>• Configure the disposition actions or scheduled events</li> <li>• View the external source information</li> </ul> |
| Configure Scheduled Times | <p>Page where you enter when the scheduled tasks run. You can specify the interval at which the tasks are run (in hours, days, or weeks) and the time of day.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

- From the **Records** menu, select **Configure** then **Enabled Features**.

On the Enabled Features page, you can change the selection of features and dispositions. For the adapter, the features you select cannot be more than the features selected on the Records server..

 **Note:**

If you have changed any features or dispositions, restart the WebCenter Content.

## About Configuring Oracle iPlanet Web Server as a Web Tier and Configuring Shared Folders

You can configure the Oracle iPlanet Web Server as a web tier for WebCenter Content. If you are using a cluster of WebCenter Content Managed Servers, you need to configure a shared file system for the WebCenter Content cluster.

## Configuring the Content Server for Desktop

You need to make sure the CoreWebdav system component is enabled, before the client can use the WebCenter Content Desktop with the Content Server.

Additionally, you must enable the following components:

- DesktopIntegrationSuite
- DesktopTag
- FolderStructureArchive
- FrameworkFolders

You can also enable the EmailMetadata, which maps the e-mail message fields to the e-mail metadata fields.



**Note:**

When you enable the FrameworkFolders component (Folders feature), verify that the Folders\_g component (Contribution Folders feature) is disabled; CoreWebdav will not work correctly with both enabled.

To configure the Content Server for Desktop:

1. Sign in to WebCenter Content as an administrator.
2. In the Content Server Administration menu, select **Admin Server** then select **Component Manager**.
3. On the Component Manager page, select **Folders** to display the Folders category of components.
4. Select the following components:
  - FrameworkFolders
  - DesktopIntegrationSuite
  - DesktopTag
  - (Optional) EmailMetadata
5. Click **Update** then click **OK** to confirm your selections.
6. In the Component Manager page, click **advanced component manager**.
7. In the Disabled Components box on the Advanced Component Manager page, select FolderStructureArchive, and click **Enable**.
8. If Folders\_g is in the Enabled Components box, select this component and click the **Disable**.
9. Make sure that the CoreWebdav component is enabled:
  - Under Category Filters on the Advanced Component Manager page, select **Show System Components**.
  - If CoreWebdav is not in the Enabled Components box, select **CoreWebdav** in the Disabled Components box and click **Enable**.
10. Restart the Content Server, as Starting and Stopping Managed Servers describes.

See the remaining topics in this section for more on configuration tasks.

- [About Installing and Configuring the Desktop on a Client Workstation](#)  
WebCenter Content for desktop has a set of embedded applications that help users integrate desktop experiences with Content Server, Oracle Content Database, or other WebDAV-based content repositories.
- [Opening Files from Microsoft Office 2010 Over a Non-SSL Connection](#)  
By default, Microsoft Office 2010 will not open files over WebDAV using basic authentication over a non-SSL connection.

## About Installing and Configuring the Desktop on a Client Workstation

WebCenter Content for desktop has a set of embedded applications that help users integrate desktop experiences with Content Server, Oracle Content Database, or other WebDAV-based content repositories.

These applications provide convenient access to content repositories directly from Microsoft Windows Explorer, Microsoft Office applications, and supported e-mail clients (Microsoft Outlook and Lotus Notes). To install Desktop on a client workstation, see [Setting Up the Desktop Client Software on Your Computer](#).

## Opening Files from Microsoft Office 2010 Over a Non-SSL Connection

By default, Microsoft Office 2010 will not open files over WebDAV using basic authentication over a non-SSL connection.

You can create the following registry entry and set its value to 2:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Internet\BasicAuthLevel
```

For more about this task, see the Microsoft Knowledge Base article 2123563 at: [Office application opens blank from WebDAV](#).

# B

## Inbound Refinery Standalone Topology

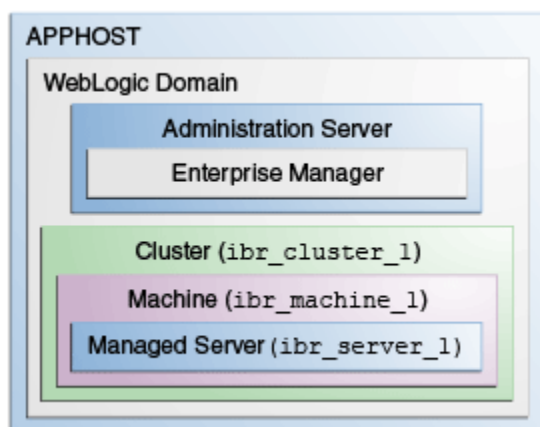
The most common installation topology for Inbound Refinery is a standalone instance of one Inbound Refinery Managed Server on its own host. There are no other components in the domain.

The following figure shows a typical installation topology for Inbound Refinery. This topology consists of an Administration Server and one Oracle WebLogic Server domain on a single host. The cluster has one Inbound Refinery Managed Server.



### Note:

Inbound Refinery in a standalone topology does not need a database connection or database installation. However, you must still run RCU and select certain options.



- [Roadmap for Installing and Configuring the Inbound Refinery Standalone Topology](#)

## Roadmap for Installing and Configuring the Inbound Refinery Standalone Topology

This roadmap has the steps required to install and configure a standalone instance of Inbound Refinery .

Complete each roadmap task in the order that the following table describes.

**Table B-1 Standard Installation Roadmap**

| Task                                                                                   | Description                                                                                                                                                                                                                                               | More Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verify your system environment                                                         | Before beginning the installation, verify that the minimum system and network requirements are met.                                                                                                                                                       | See <a href="#">Roadmap for Verifying Your System Environment</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Check for any mandatory patches that will be required before or after the installation | Review the Oracle Fusion Middleware Infrastructure release notes to see if there are any mandatory patches required for Inbound Refinery.                                                                                                                 | See Install and Configure in <i>Release Notes for Oracle Fusion Middleware Infrastructure</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Obtain the appropriate distributions                                                   | Install Oracle Fusion Middleware Infrastructure to create the Oracle Home for Oracle WebCenter Content                                                                                                                                                    | See <a href="#">About Product Distributions</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Determine your installation directories                                                | Verify that the installer can access or create the installer directories that it must access or create. Also, verify that the directories exist on systems that meet the minimum requirements.                                                            | See What are the Key Oracle Fusion Middleware Directories? in <i>Oracle Fusion Middleware Understanding Oracle Fusion Middleware</i> .                                                                                                                                                                                                                                                                                                                                                                                          |
| Install prerequisite software                                                          | Install Oracle Fusion Middleware Infrastructure to create the Oracle home directory for Inbound Refinery.                                                                                                                                                 | For Oracle Fusion Middleware Infrastructure , see Installing the Infrastructure Software. You only need to perform the installation for Infrastructure. You do not need to configure a domain for Infrastructure.                                                                                                                                                                                                                                                                                                               |
| Install the software                                                                   | Run the Oracle Universal Installer to install Inbound Refinery.<br><br>Installing the software transfers the software to your system and creates the Oracle home directory.                                                                               | See <a href="#">Installing the Oracle WebCenter Content Software</a> . Return to this roadmap for instructions on RCU.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Create the schemas                                                                     | Run the Repository Creation Utility to create the schemas required for configuration.<br><br><b>Note:</b> Configuration Requires requires that you run RCU. However, the Inbound Refinery standalone installation does not require a database connection. | <ol style="list-style-type: none"> <li>1. Navigate to the <code>ORACLE_HOME/oracle_common/bin</code> directory on your system.</li> <li>2. Run RCU. On UNIX systems, enter <code>./rcu</code>. On Microsoft Windows, run <code>rcu.bat</code></li> <li>3. Select <b>System Load and Product Load</b>.</li> <li>4. Click <b>Next</b>.</li> <li>5. Enter database connection details.</li> <li>6. Select <b>Oracle Platform Security Services</b>, which selects other required schemas such as <b>Audit Services</b>.</li> </ol> |
| Create a WebLogic domain                                                               | Use the Configuration Wizard to create and configure the WebLogic domain. Note that the domain will have a cluster that has only <i>one</i> Managed Server.                                                                                               | See <a href="#">Configuring the Domain</a> if you are creating the topology for Oracle WebCenter Content.                                                                                                                                                                                                                                                                                                                                                                                                                       |

# C

## Installing Libraries and Setting Environment Variables

WebCenter Content, Inbound Refinery, Imaging, and the Imaging Advanced Viewer for clients use Oracle Outside In Technology, which requires certain libraries that are not part of Oracle WebCenter Content.

Before a WebCenter Content, Inbound Refinery, or Imaging Managed Server is started, you need to install the libraries for your platform. For a UNIX platform, you also need to set an environment variable to reference the libraries in the library path for the user who will start the Managed Server.



### Note:

The Outside In Technology binaries are 32 bit, so your system needs to be capable of running the 32-bit binaries and have compatible libraries installed.

- [Installing Libraries on UNIX Platforms](#)  
Before you start a WebCenter Content, Inbound Refinery, or Imaging Managed Server, the libraries required for your platform need to be available on your system.
- [Setting Library Paths in Environment Variables on UNIX Platforms](#)  
Before Inbound Refinery or the WebCenter Content Dynamic Converter uses Outside In Technology for document and image conversions, the following environment variables must be set for the WebCenter Content Managed Server on the specified UNIX platforms:

## Installing Libraries on UNIX Platforms

Before you start a WebCenter Content, Inbound Refinery, or Imaging Managed Server, the libraries required for your platform need to be available on your system.

Many of the required libraries are normally installed on the machine, including the C, math, X11, dynamic loader, and pthreads libraries, among others.

Solaris SPARC 32-bit or 64-bit

```
/usr/platform/SUNW,Ultra-60/lib/libc_psr.so.1
libICE.so.6
libSM.so.6
libX11.so.4
libXext.so.0
libXm.so.4
libXt.so.4
libc.so.1
libdl.so.1
libgen.so.1
```



libm.so.1  
libmp.so.2  
libnsl.so.1  
libpthread.so.1  
libsocket.so.1  
libthread.so.1

#### HPUX ia64

libCsup.so.1  
libICE.so.1  
libSM.so.1  
libX11.so.1  
libXext.so.1  
libXm.so.1  
libXp.so.1  
libXt.so.1  
libc.so.1  
libdl.so.1  
libm.so.1  
libpthread.so.1  
libstd\_v2.so.1  
libuca.so.1  
libunwind.so.1

#### AIX 32-bit

/usr/lib/libC.a(ansi\_32.o)  
/usr/lib/libC.a(shr.o)  
/usr/lib/libC.a(shr2.o)  
/usr/lib/libC.a(shr3.o)  
/usr/lib/libICE.a(shr.o)  
/usr/lib/libIM.a(shr.o)  
/usr/lib/libSM.a(shr.o)  
/usr/lib/libX11.a(shr4.o)  
/usr/lib/libXext.a(shr.o)  
/usr/lib/libXi.a(shr.o)  
/usr/lib/libXm.a(shr\_32.o)  
/usr/lib/libXt.a(shr4.o)  
/usr/lib/libc.a(shr.o)  
/usr/lib/libcrypt.a(shr.o)  
/usr/lib/libgaimisc.a(shr.o)  
/usr/lib/libgair4.a(shr.o)  
/usr/lib/libi18n.a(shr.o)  
/usr/lib/libiconv.a(shr4.o)  
/usr/lib/libodm.a(shr.o)  
/usr/lib/libpthreads.a(shr.o)  
/usr/lib/libpthreads.a(shr\_comm.o)  
/usr/lib/libpthreads.a(shr\_xpg5.o)  
/usr/lib/libpthreads\_compat.a(shr.o)

### HPUX PA/RISC 32-bit

```
/lib/libCsup.2
/lib/libCsup_v2.2
/lib/libX11.3
/lib/libXm.4
/lib/libXt.3
/lib/libc.2
/lib/libcl.2
/lib/libm.2
/lib/libstd.2
/lib/libstd_v2.2
/lib/libstream.2
/usr/lib/libCsup.2
/usr/lib/libCsup_v2.2
/usr/lib/libX11.3
/usr/lib/libXm.4
/usr/lib/libXt.3
/usr/lib/libc.2
/usr/lib/libcl.2
/usr/lib/libdld.2
/usr/lib/libisamstub.1
/usr/lib/libm.2
/usr/lib/libstd.2
/usr/lib/libstd_v2.2
/usr/lib/libstream.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libICE.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libSM.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libX11.3
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libXext.3
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libXp.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libXt.3
```

### SUSE Linux

For an SUSE Linux operating system, the file `/usr/lib/libstdc++.so.5` is required. You can find this file in the `compat-libstdc++` or `libstdc++33` package.

### Linux variants

For Linux variants, the file `/lib/libz.so.1` is required.

## Setting Library Paths in Environment Variables on UNIX Platforms

Before Inbound Refinery or the WebCenter Content Dynamic Converter uses Outside In Technology for document and image conversions, the following environment variables must be set for the WebCenter Content Managed Server on the specified UNIX platforms:

- Environment variables for library paths for Imaging

- Add the following line to the Inbound Refinery `intradoc.cfg` file at

`DomainHome/ucm/ibr/bin`

`ContentAccessExtraLibDir=/usr/local/packages/gcc-3.4.2/lib`

Restart inbound Refinery.

- AIX:

`LIBPATH=DomainHome/oracle/imaging/imaging-server`

- HP-UX Itanium:

`LD_LIBRARY_PATH=DomainHome/oracle/imaging/imaging-server:$LD_LIBRARY_PATH`

–

- DISPLAY environment variable

On a UNIX operating system running XWindows, when redirecting the display to a system with suitable graphic capabilities, export `DISPLAY` to a valid X Server before starting the Imaging or Inbound Refinery Managed Server or the WebCenter Content Dynamic Converter.

# D

## Additional Configuration Steps

See the following topics for additional Oracle WebCenter Content configuration steps.

- [Converting Vector Graphics and Spreadsheet Text in UNIX](#)  
Dynamic Converter requires access to a running X-Server in UNIX in order to convert vector graphics and to properly measure text that spans multiple columns in spreadsheets.
- [Setting up Fonts on a UNIX System](#)  
On a UNIX operating system, you need to make sure TrueType fonts are set up for Imaging, Inbound Refinery, and WebCenter Content Dynamic Converter. If you are using a language other than English, you also need to set up fonts for national language support.
- [Reassociating the Identity Store with an External LDAP Authentication Provider](#)  
In a production system, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. You need to reassociate the identity store for your application with one of the following external LDAP authentication providers before you complete the configuration of a Managed Server, before you connect a Managed Server to a repository, and before the first user logs in to the application:
- [Configuring OracleTextSearch for Content Server](#)  
If you have a license to use OracleTextSearch (with Oracle Database 11g), then you can configure it to use Oracle Text 11g as the primary full-text search engine for WebCenter Content. Oracle Text 11g offers state-of-the-art indexing capabilities and provides the underlying search capabilities for Oracle Secure Enterprise Search (Oracle SES). To search auxiliary metadata in Oracle WebCenter Content: Records with Oracle Text 11g, you must configure it to use OracleTextSearch as the search engine.
- [Extracting and Running the Installation File for Desktop Client Software](#)  
After Oracle WebCenter Content is installed, you can use the `desktop_content_setup.exe` command with the `/export` parameter to extract the Desktop installer files:
- [Creating a Hash Partition to Improve Database Performance](#)  
Use a hash partition of the EBATCTITEMS table to minimize the database wait event enq: HW— contention, which prevents the database from scaling.

## Converting Vector Graphics and Spreadsheet Text in UNIX

Dynamic Converter requires access to a running X-Server in UNIX in order to convert vector graphics and to properly measure text that spans multiple columns in spreadsheets.

Access to a running X-server is required only if the OIT internal rendering engine is not used because of either of the following reasons:

- The **Use X-Windows for Rasterization** option is checked on the Dynamic Converter configuration page.
- The OIT internal rendering engine isn't supported on the platform being used.

The internal OIT rendering engine is supported in Linux, Solaris Sparc, AIX, and HP-UX RISC.

## Setting up Fonts on a UNIX System

On a UNIX operating system, you need to make sure TrueType fonts are set up for Imaging, Inbound Refinery, and WebCenter Content Dynamic Converter. If you are using a language other than English, you also need to set up fonts for national language support.

- [Setting Up TrueType Fonts on a UNIX System](#)  
For Imaging and WebCenter Content Dynamic Converter to work best on a UNIX operating system, you can set up TrueType fonts on the machine where Imaging, Inbound Refinery, or the Dynamic Converter is running. If these fonts are not available on your system, you need to install them. Inbound Refinery and Content Server default to the TrueType fonts in the JRE, at `JAVA_HOME/lib/fonts`.
- [Installing Fonts for National Language Support on a UNIX System](#)  
For languages other than English, the following installation steps need to be done on a UNIX operating system before you start a Managed Server:

## Setting Up TrueType Fonts on a UNIX System

For Imaging and WebCenter Content Dynamic Converter to work best on a UNIX operating system, you can set up TrueType fonts on the machine where Imaging, Inbound Refinery, or the Dynamic Converter is running. If these fonts are not available on your system, you need to install them. Inbound Refinery and Content Server default to the TrueType fonts in the JRE, at `JAVA_HOME/lib/fonts`.

Some standard font locations on different UNIX platforms follow:

- Solaris SPARC: `/usr/openwin/lib/X11/fonts/TrueType`
- Solaris X64: `/usr/openwin/lib/X11/fonts/TrueType`
- AIX: `/usr/lpp/X11/lib/X11/fonts/TrueType`
- HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`
- HP-UX PARISC64: `/usr/lib/X11/fonts/TrueType`
- Linux: `/usr/lib/X11/fonts/TrueType`

To set the path to the font directory in Inbound Refinery::

1. Sign in to Inbound Refinery.
2. Select **Conversion Settings**, then **Third-Party Application Settings**, and then **General OutsideIn Filter Options**.
3. Click **Options**
4. Enter the path to the TrueType fonts in the Path to fonts field. For example, `/usr/share/x11/fonts/FTP`
5. Click **Update**.

## Installing Fonts for National Language Support on a UNIX System

For languages other than English, the following installation steps need to be done on a UNIX operating system before you start a Managed Server:

- Copy `MW_HOME/oracle_common/jdk/jre/lib/fonts` to the `/jre/lib/fonts` directory in the Sun JDK installation directory for the Middleware home
- Copy `MW_HOME/oracle_common/jdk/jre/lib/fonts` to the `/jre/lib/fonts` directory in the Oracle JRockit JDK directory for the Middleware home.

## Reassociating the Identity Store with an External LDAP Authentication Provider

In a production system, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. You need to reassociate the identity store for your application with one of the following external LDAP authentication providers before you complete the configuration of a Managed Server, before you connect a Managed Server to a repository, and before the first user logs in to the application:

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Unified Directory
- Third-party LDAP server

For an Imaging application, the user who logs in first to an Imaging Managed Server is provisioned with full security throughout the server. It is easier to reassociate the identity store for Imaging with an external LDAP authentication provider before the first user logs in, completes the configuration of the Imaging Managed Server, and connects it to the Oracle WebCenter Content repository.

For a production installation, Oracle Internet Directory (OID) or Oracle Database 11g is required for using Oracle WebCenter Enterprise Capture because Capture uses Oracle Platform Security Services (OPSS), which works only with Oracle Database for its schema.

For an AXF for BPM application, before you can access the AXF Solution Administration page, you need to set up an `axfadmin` group in the external LDAP authentication provider and assign the AXF users you want to the group.

For an Oracle IRM application, the Oracle IRM domain gets created the first time a user logs in to the Oracle IRM Management Console. An Oracle IRM domain is different from an Oracle WebLogic Server domain. The first user who logs in to the console is made the domain administrator for the Oracle IRM domain. Before you migrate user data for Oracle IRM, the users need to be in the target LDAP identity store. If you do not reassociate the identity store with an external LDAP authentication provider before the first user logs in to the Oracle IRM console, the general process for reassociating Oracle IRM users and migrating data follows:

1. Back up existing data with the `setIRMExportFolder` script.
2. Reassociate the identity store with an external LDAP directory.
3. Verify that all users and groups exist in target LDAP identity store

4. Migrate data with the `setIRMImportFolder` script.
- [Reassociating the Identity Store with Oracle Internet Directory](#)  
You can reassociate the identity store for an Oracle WebLogic Server domain with Oracle Internet Directory and migrate users from the embedded LDAP directory to Oracle Internet Directory. The following procedure describes how to reassociate the identity store with Oracle Internet Directory.

## Reassociating the Identity Store with Oracle Internet Directory

You can reassociate the identity store for an Oracle WebLogic Server domain with Oracle Internet Directory and migrate users from the embedded LDAP directory to Oracle Internet Directory. The following procedure describes how to reassociate the identity store with Oracle Internet Directory.

You can use a similar procedure to reassociate the identity store with other LDAP authentication providers. Each provider has a specific authenticator type, and only that type should be configured.

| LDAP Authentication Provider               | Authentication Type                  |
|--------------------------------------------|--------------------------------------|
| Microsoft AD                               | ActiveDirectoryAuthenticator         |
| SunOne LDAP                                | IPlanetAuthenticator                 |
| Directory Server Enterprise Edition (DSEE) | IPlanetAuthenticator                 |
| Oracle Internet Directory                  | OracleInternetDirectoryAuthenticator |
| Oracle Virtual Directory                   | OracleVirtualDirectoryAuthenticator  |
| Oracle Unified Directory                   | IPlanetAuthenticator                 |
| EDIRECTORY                                 | NovellAuthenticator                  |
| OpenLDAP                                   | OpenLDAPAuthenticator                |
| EmbeddedLDAP                               | DefaultAuthenticator                 |

To reassociate the identity store with Oracle Internet Directory:

1. Ensure that there is no user in Oracle Internet Directory with the same name as the administrator of the Oracle WebLogic Server domain, which is `weblogic` by default.
2. Set the embedded LDAP provider to `SUFFICIENT`.
3. For Oracle IRM, sign in to the management console as a user from Oracle Internet Directory, to be the Oracle IRM domain administrator.  
  
Do not sign in to the management console with the user name of the Oracle WebLogic Server domain administrator. The Oracle recommendation is to not use the `weblogic` user account as the Oracle IRM administrator user account. If you use a different account for the Oracle IRM domain administrator, you can use the Oracle WebLogic Server domain administrator, `weblogic` by default, to start and stop Oracle WebLogic Server as well as to alter server settings. If you have a problem with Oracle Internet Directory, you will not need to fix it before you can do maintenance on Oracle WebLogic Server.
4. For an Oracle IRM Managed Server, if a user has already signed in to the Oracle IRM Management Console, you need to run the WebLogic Scripting Tool (WLST) `setIRMExportFolder` command before identity store reassociation.

Use this command to set an export folder for exporting the user and group details referenced by Oracle IRM, which uses the export folder path to decide where to write out the user and group details. The Oracle IRM Managed Server must have write access to the folder path. The export folder must exist before you run the `setIRMExportFolder` command.

The following example sets `/user/irm-data` as the export folder:

```
cd WCC_ORACLE_HOME/common/bin
./wlst.sh
> connect('weblogic', 'password', 't3://adminServerHost:adminServerPort')
> setIRMExportFolder('/user/irm-data')
```

In the example, `adminServerHost` is the host name and `adminServerPort` is the port number for the Administration Server of the Oracle WebLogic Server domain.

#### Note:

If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the `JVM_ARGS` section of the `wlst.sh` file or set them in the `CONFIG_JVM_ARGS` environment variable:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.TrustKeyStore=KeyStoreName
```

`KeyStoreName` is the name of the keystore in use (DemoTrust for the built-in demonstration certificate). The `wlst.sh` file is in the `bin` subdirectory of the `common` directory in the WebCenter Content Oracle home directory.

After the Oracle IRM Managed Server picks up this configuration change, normally right away, it will write out a series of XML documents in the export folder. This process is complete when a folder named `accounts` appears under the export folder. The `accounts` folder will contain one or more folders named `batchXXX`, with each batch folder containing a set of XML documents that include the user and group details. For example:

```
/user
 /irm-data
 /accounts
 /batch1
 user1.xml
 user2.xml
 group1.xml
```

The batch folders are used to ensure that the operating system limit of the maximum number of files in a folder is not exceeded.

After this process is complete, reset the export folder:

```
setIRMExportFolder('')
```



This reset ensures that Oracle IRM does not perform any further data exporting when the Managed Server restarts.

5. Configure the Oracle Internet Directory authentication provider:
  - a. Start the Administration Server for your Oracle WebLogic Server domain.
  - b. Sign in to the Oracle WebLogic Server Administration Console as the domain administrator user, at this URL: `http://adminServerHost:adminServerPort/console`
  - c. Under Domain Structure on the left, select Security Realms.
  - d. In the Realms table on the Summary of Security Realms page, click myrealm in the Name column to open the Settings for myrealm page.
  - e. Click the Providers tab, and then click New under the Authentication Providers table on the Authentication tab.
  - f. In the Create a new Authentication Provider dialog box, enter a provider name in the Name field, change the type to `OracleInternetDirectoryAuthenticator`, and then click OK.
  - g. In the Authentication Providers table, click Reorder, move the provider you just created to the top of the list, and then click OK
  - h. Click DefaultAuthenticator, change the Control Flag value to `OPTIONAL`, and then click Save
  - i. Click Providers in the breadcrumb trail along the top of the page to navigate back to the Providers tab.
  - j. Click the name of the authentication provider you just created to navigate to the Configuration tab for the provider. On the Common tab, change the Control Flag value to `SUFFICIENT`, and then click Save.

`SUFFICIENT` means that if a user can be authenticated against Oracle Internet Directory, no further authentication is processed.

`REQUIRED` means that the authentication provider must succeed even if another provider already authenticated the user. If the embedded LDAP has been set to `OPTIONAL` and Oracle Internet Directory has been set to `REQUIRED`, the embedded LDAP user is no longer valid.

- k. Click the Provider Specific tab. Set Provider Specific values in the following fields, and leave default values in the other fields:
  - Host: The host name or IP address of the LDAP server.
  - Port: The Oracle Internet Directory Port, 389 by default.
  - Principal: The Distinguished Name (DN) of the LDAP user that Oracle WebLogic Server should use to connect to the LDAP server; for example `cn=orcladmin`
  - Credential: The credential used to connect to the LDAP server (usually a password)
  - Confirm Credential: The same value as for the Credential field.
  - User Base DN: The base distinguished name (DN) of the tree in the LDAP directory that contains users; for example `cn=users,dc=example,dc=com`. In Oracle Internet Directory, this is the value of the User Search Base attribute, which you can look up in the OIDDAS administration dialog.

- Use Retrieved User Name as Principal: Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal value. Select this attribute for Oracle IRM.

— Group Base DN: The base distinguished name (DN) of the tree in the LDAP directory that contains groups; for example: `cn=groups,dc=example,dc=com`. In Oracle Internet Directory, this is the value of the Group Search Base attribute, which you can look up in the OIDDAS administration dialog.

**Note:** Use an exact DN rather than a top-level DN. Using a top-level DN would provide access to all the default users and groups under the DN, giving access to more users than required by the application.

- Propagate Cause For Login Exception: Propagates exceptions thrown by Oracle Internet Directory, like password expired exceptions, to Oracle WebLogic Server so they show in the console and the logs. For Oracle IRM, select this attribute in the General area of the tab.

I. Click **Save**.

6. Restart the Administration Server.

Note: Authentication providers in an Oracle WebLogic Server domain are chained. This means that user authentication needs to run successfully through all authentication providers. With the Control Flag value set to OPTIONAL for the default provider, it is allowed to fail without a server startup or user authentication failure.

7. After the server is up again, sign in to the Administration Console again, and click Security Realms under Domain Structure.

8. In the Realms table on the Summary of Security Realms page, click myrealm in the Name column to open the Settings for myrealm page.

9. Click the Users and Groups tab to see a list of users contained in the configured authentication providers, on the Users subtab, and then click the Groups subtab to see a list of groups. You should see user names from the Oracle Internet Directory configuration, which implicitly verifies that the configuration is working

10. Check that you have switched the security provider successfully, with either or both of these basic tests:

11. For an Oracle IRM Managed Server, if a user has already signed in to the Oracle IRM Management Console, you need to run the `setIRMImportFolder WLST` command after identity store reassociation. Use this command to set the import folder to point to the export folder that was set before identity store reassociation.

**Note:** take a backup of the export folder before performing the import process because the import process deletes the contents of the folder during successful processing of the user and group details.

This operation should be performed with only one Managed Server running a deployed Oracle IRM application, to ensure that only one Managed Server performs the user and group processing. After the import process is complete, all Managed Servers running the Oracle IRM application can be started. The following example sets `/user/irm-data` as the import folder:

```
cd WCC_ORACLE_HOME/common/bin
./wlst.sh
> connect('weblogic', 'password', 't3://adminServerHost:adminServerPort')
> setIRMImportFolder('/user/irm-data')
```

After the Oracle IRM Managed Server picks up this configuration change, it will read the contents of the folder and update the global user ID (GUID) values in the Oracle IRM system to reflect the values in the new identity store. When a user or group has been processed, the import process deletes the corresponding XML file. After the import process is complete, the import folder will be empty:

```
/user
 /irm-data
```

If an error occurs during the processing of a user or group, the import process writes the error to a file that matches the user or group name. For example, if the user details in user1.xml cause an error during processing, the import process writes the error details to the file user1.xml.fail:

```
/user
 /irm-data
 /accounts
 /batch1
 user1.xml
 user1.xml.fail
```

If you can fix the error, then rerun the setIRMImportFolder WLST command to rerun the import process. For example, if user or group processing fails because the user or group does not exist in the new identity store, adding the user or group to Oracle Internet Directory will fix the error, and you can rerun the import process:

```
connect('weblogic', 'password', 'adminServerHost:adminServerPort')
> setIRMImportFolder('/user/irm-data')
```

After this process is complete, reset the import folder:

```
setIRMImportFolder('')
```

This reset ensures that Oracle IRM does not perform any further data importing when the Managed Server restarts.

After the reassociation of the identity store, users in Oracle Internet Directory have the same rights that their namesakes had in the Oracle WebLogic Server embedded LDAP server before the migration of user data. For example, if a user existed in the embedded LDAP server before the migration with the user name weblogic and an Oracle IRM role of Domain Administrator, then, after migration, the user in Oracle Internet Directory with the user name weblogic would have the Oracle IRM role of Domain Administrator.

## Configuring OracleTextSearch for Content Server

If you have a license to use OracleTextSearch (with Oracle Database 11g), then you can configure it to use Oracle Text 11g as the primary full-text search engine for WebCenter Content. Oracle Text 11g offers state-of-the-art indexing capabilities and provides the underlying search capabilities for Oracle Secure Enterprise Search (Oracle SES). To search auxiliary metadata in Oracle WebCenter Content: Records

with Oracle Text 11g, you must configure it to use OracleTextSearch as the search engine.

If you have a license to use Oracle SES, you can configure it for use with OracleTextSearch on WebCenter Content and configure Content Server to use Oracle SES as its back-end search engine.

OracleTextSearch enables administrators to specify certain metadata fields to be optimized for the search index as well as to customize additional fields. OracleTextSearch also enables a fast index rebuild and index optimization.

You can set OracleTextSearch on the WebCenter Content postinstallation configuration page.

To configure OracleTextSearch for Content Server on the postinstallation configuration page:

1. Select Internal or External in the FullText Search Option field.
2. If you selected the External option, provide the name of the external data source in the External DataSource field.

If you have Oracle Database 11g, and you specify Internal for Fulltext Search Option, you do not need to run the Repository Creation Utility (RCU) to create a search schema. You might want to use an external data source so you can put the search engine on another system or in another database. Before you can use an external data source with OracleTextSearch, you need to create a search schema in a database other than the system database and configure the data source.

- [Creating a Search Schema and Configuring an External Data Source](#)  
You might want to use an external data source so you can put the search engine on another system or in another database. Before you can use an external data source with OracleTextSearch, you need to create a search schema in a database other than the system database and configure the data source.
- [Configuring OracleTextSearch for Content Server in a Configuration File](#)  
If you did not configure OracleTextSearch on the configuration page for Content Server or you want to change the configuration, you can configure this search option in the DomainHome/ucm/cs/config/config.cfg configuration file for the Content Server instance.

## Creating a Search Schema and Configuring an External Data Source

You might want to use an external data source so you can put the search engine on another system or in another database. Before you can use an external data source with OracleTextSearch, you need to create a search schema in a database other than the system database and configure the data source.

To create a search schema and configure an external data source:

1. Run RCU to create a search schema (prefix\_OCSSEARCH in the database where you want the search engine,
2. Create a JDBC data source that points to the search schema. You can use the Administration Console, WebLogic Scripting Tool Command, or Fusion Middleware Control to create a data source.
3. Use the Administration Console to target the data source to the WebCenter Content Managed Server (UCM\_server1 by default).

If you did not configure OracleTextSearch on the configuration page for Content Server or you want to change the configuration, you can configure this search option in the DomainHome/ucm/cs/config/config.cfg configuration file for the Content Server instance.

After changing the search option, you need to restart Content Server and rebuild the search index.



**Note:**

If you plan to use the WebCenter Content user interface), you may want to optimize the `dOriginalName` field for the search index. The WebCenter Content user interface leverages the file name as its primary identifier presented in the interface. You can sort presentations by file name, which is the value of the `dOriginalName` field in Content Server.

By default, Content Server configures only the document title (`dDocTitle`) as a field available for searching and sorting. The WebCenter Content user interface, by default, does not use document titles in its displays.

The process of enabling `dOriginalName` as a new search or sort field requires a full rebuild of the fulltext index.

## Configuring OracleTextSearch for Content Server in a Configuration File

If you did not configure OracleTextSearch on the configuration page for Content Server or you want to change the configuration, you can configure this search option in the `DomainHome/ucm/cs/config/config.cfg` configuration file for the Content Server instance.

To configure OracleTextSearch for Content Server in the configuration file:

1. Open the `DomainHome/ucm/cs/config/config.cfg` file for the Content Server instance in a text editor.
2. Set the following values:

```
SearchIndexerEngineName=OracleTextSearch
```

```
IndexerDatabaseProviderName=SystemDatabase
```



**Note:**

- You can specify a separate Oracle Database as the value of `IndexerDatabaseProviderName`, instead of `SystemDatabase`. The driver jar `ojdbc6.jar` is provided by Oracle in the `MW_HOME/wlserver_10.3/server/lib` directory. Before Oracle Text Search can function properly with the separate Oracle Database, however, you need to manually copy the `ojdbc6.jar` file from the `MW_HOME/wlserver_10.3/server/lib` directory to the `DomainHome/lib` directory.
- OracleTextSearch requires a JDBC driver version of 10.2.0.4 or higher. The component will not work with older JDBC driver versions.

3. Save the file.

4. Restart Content Server.
5. Rebuild the search index using the Indexer tab of the Repository Manager, located under Administration, in Admin Applets.

## Extracting and Running the Installation File for Desktop Client Software

After Oracle WebCenter Content is installed, you can use the `desktop_content_setup.exe` command with the `/export` parameter to extract the Desktop installer files:

```
desktop_content_setup.exe /export [path]/existing_extraction_directory/
```

You can specify an existing directory to extract the files into. If you omit the directory from the command, it extracts the files into the current directory.



### Note:

If you have an earlier version of Desktop installed, uninstall it before you proceed with the installation.

The `desktop_content_setup.exe` command extracts three files:

- `package.ini`
- `contentdesktop.msi`
- `contentdesktop_x64.msi`

To install Desktop on a client system, use only one of the MSI files in the Desktop installer command. The Desktop client software installers support a number of custom installation options that can help system administrators roll out the software:

- [Using Command-Line Parameters for Automation](#)  
You can use several command-line parameters to automate part of the installation process. If you need to pass any public property to MSI through `desktop_content_setup.exe`, you can do that with the following command:
- [Disabling Integrations](#)  
The Desktop installer provides a number of command-line options to disable specific software integrations. If the installer detects that an integration can be applied to existing software on the computer (Microsoft Word, PowerPoint, Excel, and so on), it usually will automatically attempt to install an integration. To prevent an integration from being installed for a specific software product, you can disable that integration using one of these command-line switches:
- [Performing Silent Roll-Outs](#)  
The Desktop installer enables an administrator to roll out the Desktop client software to multiple client machines with the help of third-party tools such as SMS or netOctopus, which are capable of executing one executable on many machines. The installer for the Desktop client software supports a silent installation option that you can configure with SMS.

- [Configuring Content Server Connections Through the Registry on a Windows System](#)  
You can add Content Server connections by creating a registry file on a Windows system. The file is not included as part of the standard installation files; you must create it.

## Using Command-Line Parameters for Automation

You can use several command-line parameters to automate part of the installation process. If you need to pass any public property to MSI through `desktop_content_setup.exe`, you can do that with the following command:

```
desktop_content_setup.exe /msi ONE_PUBLIC_PROPERTY=public_property_value
```

## Disabling Integrations

The Desktop installer provides a number of command-line options to disable specific software integrations. If the installer detects that an integration can be applied to existing software on the computer (Microsoft Word, PowerPoint, Excel, and so on), it usually will automatically attempt to install an integration. To prevent an integration from being installed for a specific software product, you can disable that integration using one of these command-line switches:

- `EXPLORER=0`
- `WORD=0`
- `POWERPOINT=0`
- `EXCEL=0`
- `OUTLOOK=0`
- `NOTES=0`

Use capital letters for the switch names.

These switches are only for disabling software integrations. They are not necessary to enable software integrations for applications found on client computers.

## Performing Silent Roll-Outs

The Desktop installer enables an administrator to roll out the Desktop client software to multiple client machines with the help of third-party tools such as SMS or netOctopus, which are capable of executing one executable on many machines. The installer for the Desktop client software supports a silent installation option that you can configure with SMS.

For silent install, you can use the following command to control the level of user interface displayed.

```
desktop_content_setup.exe /s UI=user_interface_level
```

In the command, `user_interface_level` can be 1, 2, 3, or 4:

- 1: No user interface during install.
- 2: Displays only a progress bar during install.

- 3: Presents an install screen with different dialog boxes but doesn't require user input to run.
- 4: Runs a fully interactive installer requiring user input.

For example, to silently and selectively disable installing Outlook, PowerPoint, and Lotus Notes, the command would be as follows:

```
desktop_content_setup.exe /s UI=1 /msi OUTLOOK=0 POWERPOINT=0 NOTES=0
```

You will also need to add the `REBOOT=ReallySuppress` and `MSIRESTARTMANAGERCONTROL=Disable` properties to prevent reboots and to prevent any dialogs asking to shut down applications. For example:

```
desktop_content_setup.exe /s UI=2 /msi OUTLOOK=0
POWERPOINT=0 NOTES=0 REBOOT=ReallySuppress MSIRESTARTMANAGERCONTROL=Disable
```

The properties after the `/msi` switch can also be used with the

```
msiexec
```

with the MSI files. For example:

```
start /wait msiexec /i contentdesktop_x64.msi OUTLOOK=0 WORD=0 EXCEL=0
POWERPOINT=0 NOTES=0 REBOOT=ReallySuppress
MSIRESTARTMANAGERCONTROL=Disable /l*v DISUpgrade_x64.log /qn
```

## Configuring Content Server Connections Through the Registry on a Windows System

You can add Content Server connections by creating a registry file on a Windows system. The file is not included as part of the standard installation files; you must create it.

Adding servers in a registry file automates the setup process by saving your users from setting up connections on their computers. When you add a server connection in this manner, the user cannot delete the server connection from their desktop (Windows Explorer, the email client, or any desktop application).

### Sample Registry File Entries

The following sample registry file entries are examples for Content Servers instances, WebDAV servers, and Content DB servers, with comments below the code lines. The sample file registry entries are under `HKEY_LOCAL_MACHINE`. If you would like the user to run the installer, use `HKEY_CURRENT_USER` instead of `HKEY_LOCAL_MACHINE`.

Using `HKEY_LOCAL_MACHINE` means that users cannot change the `ServerAuth` or `RememberMetaData` values because they will not have permission to change `HKEY_LOCAL_MACHINE` entries (unless a Windows policy is set to allow this, or the user is an administrator).

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
```



```
Desktop\Content\WebDAV\Servers\Corporate]
"ServerType"="ucm"
"ServerURL"="http://corporate/cs/idcplg/webdav"
```

(In this registry entry, the server is a Content Server instance, the display name of the server is Corporate, and the server WebDAV URL is http://corporate/cs/idcplg/webdav.)

```
[HKEY_LOCAL_MACHINE\Software\ORACLE\WebCenter
Desktop\Content\Shared\Config\Corporate]
"HostCgiUrl"="http://corporate/cs/idcplg"
"ServerAuth"=REG_DWORD:0x00000000 (0)
"RememberMetaData"=REG_DWORD:0x00000000 (0)
```

In this registry entry, the server is a Content Server instance, the name of the server is Corporate, the CGI URL is http://corporate/cs/idcplg, and the user interface URL is http://corporate/wcc/faces. Content DB servers and WebDAV servers do not use these registry entries.)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\Department]
"ServerType"="dav"
"ServerURL"="http://corporate/content/app/explorerPage.jspx"
"Single Sign-On Url"="http://section/content/app/explorerPage.jspx"
"Use Single Sign-On"=REG_DWORD:0x00000001 (1)
```

(In this registry entry, the server is a WebDAV server, the display name of the server is Department, the server WebDAV URL is http://corporate/content/app/explorerPage.jspx, a single sign-on page has been identified, and single sign-on has been implemented.)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\Section]
"ServerType"="cdb"
"ServerURL"="http://section/content/dav"
"Single Sign-On Url"="http://section/content/app/explorerPage.jspx"
"Use Single Sign-On"=REG_DWORD:0x00000001 (1)
```

(In this registry entry, the server is a Content DB server, the display name of the server is Section, the server WebDAV URL is http://section/content/dav, a single sign-on page has been identified, and single sign-on has been implemented.)

## Creating a Hash Partition to Improve Database Performance

Use a hash partition of the EBATCTITEMS table to minimize the database wait event enq: HW- contention, which prevents the database from scaling.

This event occurs when many threads are trying to update and add new BLOB items to ECBATCHITEMS, as follows:

```
table - "UPDATE ECBATCHITEMS SET ECITEMDATA=:1 WHERE ECITEMID=:2"
```

Creating a hash partition minimizes this contention because different items will be in eight different partitions.

To create a hash partition:

1. Get the definition of the table:

```
SELECT dbms_metadata.get_ddl('OBJECT TYPE','OBJECT NAME', OWNER') FROM
DUAL;
```

2. Append partitioning syntax to the table definition. The following table definition creates a hash partition for the ECBATCHITEMS table:

```
SQL> create table "CAPCLIENT_CAPTURE"."ECBATCHITEMS2"
2 ("ECTENNANTID" VARCHAR2(36 CHAR),
 "ECITEMID" VARCHAR2(36) NOT NULL ENABLE,
3 4 "ECORIGINALITEMID" VARCHAR2(36),
5 "ECORIGINALITEMINDEX" NUMBER(10,0),
6 "ECBARCODES" BLOB,
7 "ECBARCODECOUNT" NUMBER(10,0),
8 "ECSTATUS" VARCHAR2(255),
9 "ECSOURCEFORMAT" VARCHAR2(255),
 "ECANNOTATION" VARCHAR2(255),
10 11 "ECFILELENGTH" NUMBER(19,0),
12 "ECDOCUMENTLINKCOUNT" NUMBER(10,0),
13 "ECPATCHCODE" NUMBER(10,0),
14 "ECENDORSEMENT" VARCHAR2(255),
15 "ECSOURCEFILENAME" VARCHAR2(255),
16 "ECBATCHID" NUMBER(19,0),
17 "ECLASTMODIFIED" NUMBER(19,0),
18 "ECITEMDATA" BLOB,
 PRIMARY KEY ("ECITEMID")) partition by hash(ECITEMID) partitions
8
;
```

# E

## Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product

Consider that you have a JDK version `jdk1.8.0_121` installed on your machine. When you install and configure an Oracle Fusion Middleware product, the utilities, such as Configuration Wizard (`config.sh|exe`), OPatch, or RCU point to a default JDK, for example, `jdk1.8.0_121`. After some time, Oracle releases a new version of the JDK, say `jdk1.8.0_211` that carries security enhancements and bug fixes. From 12c (12.2.1.3.0) onwards, you can upgrade the existing JDK to a newer version, and can have the complete product stack point to the newer version of the JDK.

You can maintain multiple versions of JDK and switch to the required version on need basis.

- [About Updating the JDK Location After Installing an Oracle Fusion Middleware Product](#)  
The binaries and other metadata and utility scripts in the Oracle home and Domain home, such as RCU or Configuration Wizard, use a JDK version that was used while installing the software and continue to refer to the same version of the JDK. The JDK path is stored in a variable called `JAVA_HOME` which is centrally located in `.globalEnv.properties` file inside the `ORACLE_HOME/oui` directory.

## About Updating the JDK Location After Installing an Oracle Fusion Middleware Product

The binaries and other metadata and utility scripts in the Oracle home and Domain home, such as RCU or Configuration Wizard, use a JDK version that was used while installing the software and continue to refer to the same version of the JDK. The JDK path is stored in a variable called `JAVA_HOME` which is centrally located in `.globalEnv.properties` file inside the `ORACLE_HOME/oui` directory.

The utility scripts such as `config.sh|cmd`, `launch.sh`, or `opatch` reside in the `ORACLE_HOME`, and when you invoke them, they refer to the `JAVA_HOME` variable located in `.globalEnv.properties` file. To point these scripts and utilities to the newer version of JDK, you must update the value of the `JAVA_HOME` variable in the `.globalEnv.properties` file by following the directions listed in [Updating the JDK Location in an Existing Oracle Home](#).

To make the scripts and files in your Domain home directory point to the newer version of the JDK, you can follow one of the following approaches:

- Specify the path to the newer JDK on the Domain Mode and JDK screen while running the Configuration Wizard.

For example, consider that you installed Oracle Fusion Middleware Infrastructure with the JDK version 8u121. So while configuring the WebLogic domain with the Configuration Assistant, you can select the path to the newer JDK on the Domain Mode and JDK screen of the Configuration Wizard. Example: `/scratch/jdk/jdk1.8.0_131`.

- Manually locate the files that have references to the JDK using `grep` (UNIX) or `findstr` (Windows) commands and update each reference. See [Updating the JDK Location in an Existing Domain Home](#).



#### Note:

If you install the newer version of the JDK in the same location as the existing JDK by overwriting the files, then you don't need to take any action.

- [Updating the JDK Location in an Existing Oracle Home](#)  
The `getProperty.sh|cmd` script displays the value of a variable, such as `JAVA_HOME`, from the `.globalEnv.properties` file. The `setProperty.sh|cmd` script is used to set the value of variables, such as `OLD_JAVA_HOME` or `JAVA_HOME` that contain the locations of old and new JDKs in the `.globalEnv.properties` file.
- [Updating the JDK Location in an Existing Domain Home](#)  
You must search the references to the current JDK, for example `jdk1.8.0_121` manually, and replace those instances with the location of the new JDK.

## Updating the JDK Location in an Existing Oracle Home

The `getProperty.sh|cmd` script displays the value of a variable, such as `JAVA_HOME`, from the `.globalEnv.properties` file. The `setProperty.sh|cmd` script is used to set the value of variables, such as `OLD_JAVA_HOME` or `JAVA_HOME` that contain the locations of old and new JDKs in the `.globalEnv.properties` file.

The `getProperty.sh|cmd` and `setProperty.sh|cmd` scripts are located in the following location:

(UNIX) `ORACLE_HOME/oui/bin`

(Windows) `ORACLE_HOME\oui\bin`

Where, `ORACLE_HOME` is the directory that contains the products using the current version of the JDK, such as `jdk1.8.0_121`.

To update the JDK location in the `.globalEnv.properties` file:

- Use the `getProperty.sh|cmd` script to display the path of the current JDK from the `JAVA_HOME` variable. For example:

(UNIX) `ORACLE_HOME/oui/bin/getProperty.sh JAVA_HOME`

(Windows) `ORACLE_HOME\oui\bin\getProperty.cmd JAVA_HOME`

`echo JAVA_HOME`

Where `JAVA_HOME` is the variable in the `.globalEnv.properties` file that contains the location of the JDK.

- Back up the path of the current JDK to another variable such as `OLD_JAVA_HOME` in the `.globalEnv.properties` file by entering the following commands:

(UNIX) `ORACLE_HOME/oui/bin/setProperty.sh -name OLD_JAVA_HOME -value specify_the_path_of_current_JDK`

(Windows) `ORACLE_HOME\oui\bin\setProperty.cmd -name OLD_JAVA_HOME -value specify_the_path_of_current_JDK`

This command creates a new variable called `OLD_JAVA_HOME` in the `.globalEnv.properties` file, with a value that you have specified.

3. Set the new location of the JDK in the `JAVA_HOME` variable of the `.globalEnv.properties` file, by entering the following commands:

```
(UNIX) ORACLE_HOME/oui/bin/setProperty.sh -name JAVA_HOME -value
specify_the_location_of_new_JDK
(Windows) ORACLE_HOME\oui\bin\setProperty.cmd -name JAVA_HOME -
value specify_the_location_of_new_JDK
```

After you run this command, the `JAVA_HOME` variable in the `.globalEnv.properties` file now contains the path to the new JDK, such as `jdk1.8.0_131`.

## Updating the JDK Location in an Existing Domain Home

You must search the references to the current JDK, for example `jdk1.8.0_121` manually, and replace those instances with the location of the new JDK.

You can use the `grep` (UNIX) or `findstr` (Windows) commands to search for the jdk-related references.

You'll likely be required to update the location of JDK in the following three files:

```
(UNIX) DOMAIN_HOME/bin/setNMJavaHome.sh
(Windows) DOMAIN_HOME\bin\setNMJavaHome.cmd

(UNIX) DOMAIN_HOME/nodemanager/nodemanager.properties
(Windows) DOMAIN_HOME\nodemanager\nodemanager.properties

(UNIX) DOMAIN_HOME/bin/setDomainEnv.sh
(Windows) DOMAIN_HOME\bin\setDomainEnv.cmd
```

Sistema de Gestión Documental – SGD PRODUCCION

LBR

adminwcc.foncep.local

wcc.foncep.local

adminsoa.foncep.local

soa.foncep.local

DMZ

