Oracle® Fusion Middleware

Installing and Configuring Oracle WebCenter Sites

ORACLE®

Oracle Fusion Middleware Installing and Configuring Oracle WebCenter Sites, 12*c* (12.2.1.3.0)

E95519-03

Copyright © 2015, 2020, 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

Part I   Installing and Configuring Oracle WebCenter Sites

1   About the Oracle WebCenter Sites Installation

2   Preparing to Install and Configure Oracle WebCenter Sites

3   Installing the Oracle WebCenter Sites Software

4   Configuring WebCenter Sites Domain

5   Next Steps After Configuring the Domain

Part II   Configuring WebCenter Sites Components

6   Sites Configuration Setup

7   Configuring WebCenter Sites

8   Configuring Site Capture

9   Configuring Visitor Services

10   Configuring Remote Satellite Server

11   Switching to External Authentication

Preface

This document describes how to install and configure Oracle WebCenter Sites.

- Audience
- Documentation Accessibility
- 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 Sites. 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.

Related Documents

Refer to the Oracle Fusion Middleware Library for additional information.

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

ORACLE®

Part I

Installing and Configuring Oracle WebCenter Sites

Topics in this section describe how to install Oracle WebCenter Sites and configure Oracle WebCenter Sites domains.

- About the Oracle WebCenter Sites Installation

- Preparing to Install and Configure Oracle WebCenter Sites
  To prepare for your Oracle WebCenter Sites installation, verify that your system meets the basic requirements, then obtain the correct installation software.

- Installing the Oracle WebCenter Sites Software

- Configuring WebCenter Sites Domain
  After you have installed WebCenter Sites, you can configure the domain, which you can also extend for high availability.

- Next Steps After Configuring the Domain

1

About the Oracle WebCenter Sites Installation

The standard installation for Oracle WebCenter Sites described in this guide creates the standard topology, which represents a sample starting topology for this product.

> ✎ **Note:**
>
> The product Oracle Identity Manager is referred to as Oracle Identity Manager (OIM) and Oracle Identity Governance (OIG) interchangeably in the guide.

- 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.

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 Sites, see Installing Multiple Products in the Same Domain.

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 Sites. 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 *Planning an Installation of Oracle Fusion Middleware*.

- [About the WebCenter Sites Standard Installation Topology](#)
  This topology represents a standard WebLogic Server domain that contains an Administration Server and one or more clusters containing one or more Managed Servers.

- [About Elements in the Standard Installation Topology Illustration](#)
  The standard installation topology typically includes common elements.

- [About the Oracle WebCenter Sites: Site Capture Standard Installation Topology](#)
  This topology represents the standard installation for Site Capture.

- [About the Oracle WebCenter Sites: Visitor Services Standard Installation Topology](#)
  This topology represents the standard installation for Visitor Services.

- [About Oracle WebCenter Sites: Satellite Server Standalone Topology](#)
  Oracle WebCenter Sites ships with a copy of Oracle WebCenter Sites: Satellite Server that installs and automatically enables on the same machine as Oracle WebCenter Sites software. This is your *co-resident* Satellite Server. It gives development and management systems the ability to simulate page delivery as it occurs on the active site (delivery system).

About the WebCenter Sites Standard Installation Topology

This topology represents a standard WebLogic Server domain that contains an Administration Server and one or more clusters containing one or more Managed Servers.

The following figure shows the standard installation topology for WebCenter Sites.

See Table 1-1 for information on elements of this topology.

Figure 1-1   Standard Topology for Oracle B2B
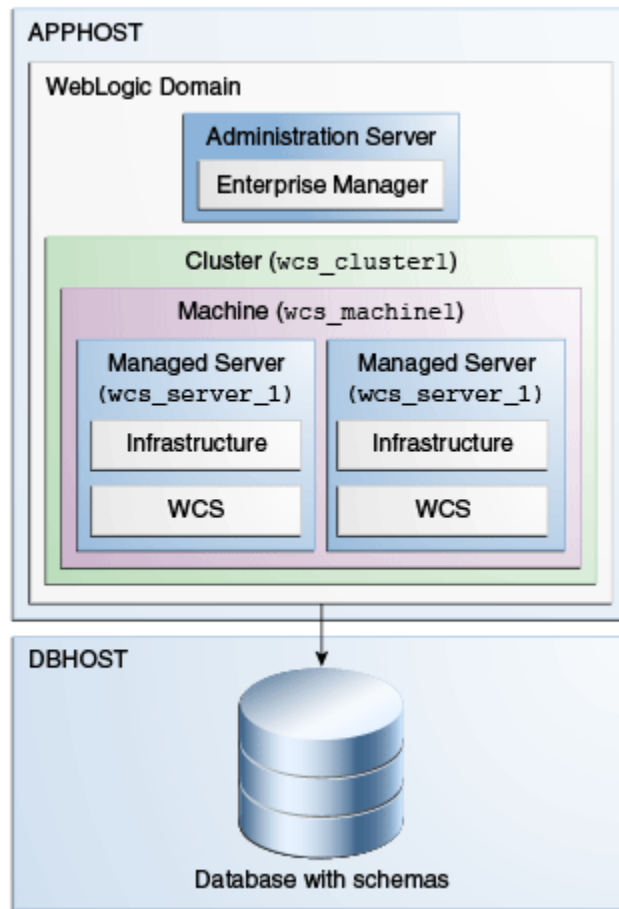
For configuration instructions, see Configuring WebCenter Sites Domain.

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). See What Is an Oracle WebLogic Server Domain? in *Understanding Oracle Fusion Middleware*.

Table 1-1   (Cont.) Description of Elements in Standard Installation Topologies

Element	Description and Links to Related Documentation
Administration Server	Central control entity of a WebLogic domain. It maintains configuration objects for that domain and distributes configuration changes to Managed Servers. See What Is the Administration Server? in *Understanding Oracle Fusion Middleware*.
Enterprise Manager	The Oracle Enterprise Manager Fusion Middleware Control is a primary tool used to manage a domain. See Oracle Enterprise Manager Fusion Middleware Control in *Understanding Oracle Fusion Middleware*.
Cluster	A collection of multiple WebLogic Server instances running simultaneously and working together. See Overview of Managed Servers and Managed Server Clusters in *Understanding Oracle Fusion Middleware.*
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. See Overview of Managed Servers and Managed Server Clusters in *Understanding Oracle Fusion Middleware.*
Infrastructure	A collection of services that include the following: • Metadata repository (MDS) contains the metadata for Oracle Fusion Middleware components, such as the Oracle Application Developer Framework. See What Is the Metadata Repository? in *Understanding Oracle Fusion Middleware*. • Oracle Application Developer Framework (Oracle ADF). • Oracle Web Services Manager (OWSM).

About the Oracle WebCenter Sites: Site Capture Standard Installation Topology

This topology represents the standard installation for Site Capture.

Figure 1-2 shows the standard installation topology for Oracle WebCenter Sites: Site Capture.

See Table 1-1 for information on elements of this topology.

Figure 1-2   Standard Installation Topology for Oracle WebCenter Sites: Site Capture
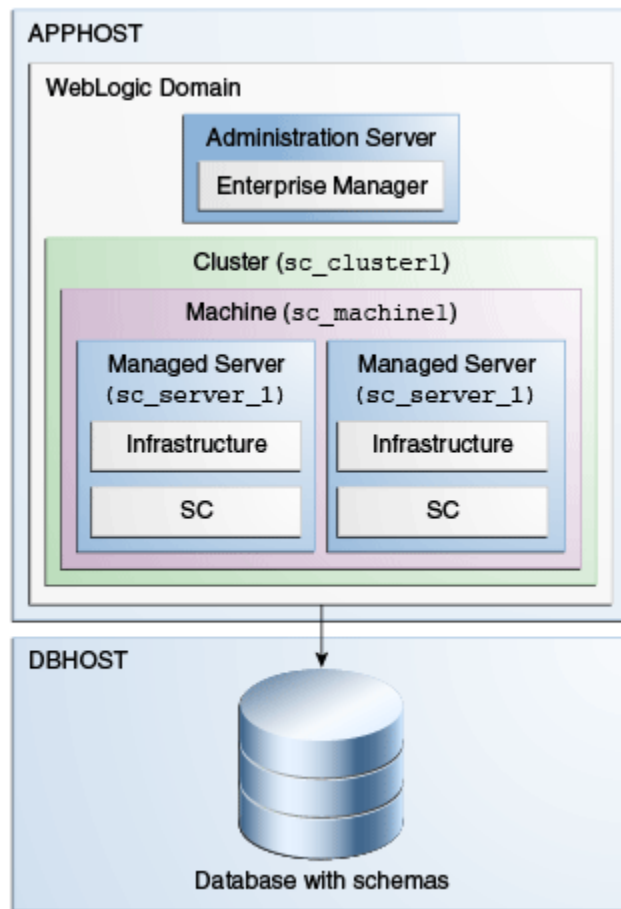
About the Oracle WebCenter Sites: Visitor Services Standard Installation Topology

This topology represents the standard installation for Visitor Services.

The following figure shows the standard installation topology for Oracle WebCenter Sites: Visitor Services.

See Table 1-1 for information on elements of this topology.

Figure 1-3   Standard Installation Topology for Oracle WebCenter Sites: Visitor Services
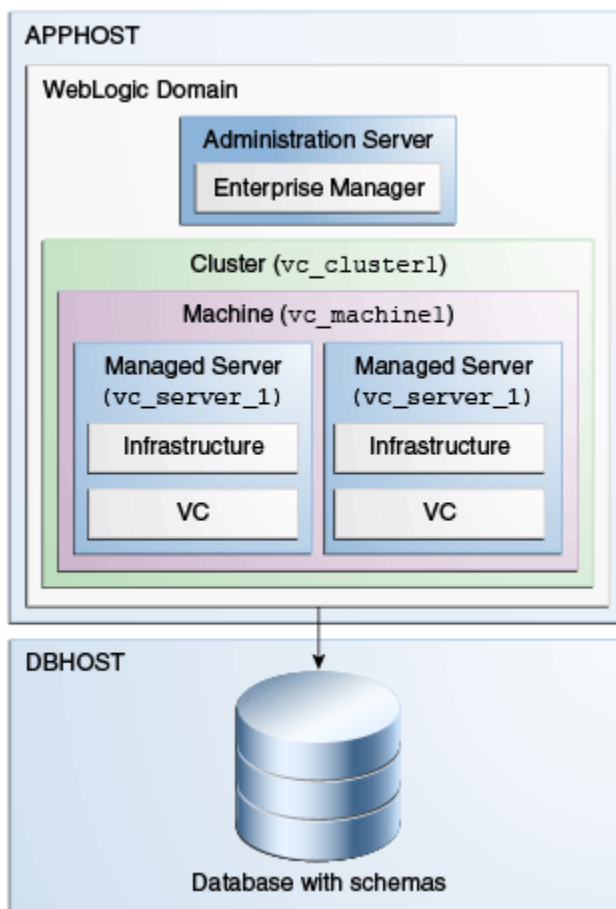
About Oracle WebCenter Sites: Satellite Server Standalone Topology

Oracle WebCenter Sites ships with a copy of Oracle WebCenter Sites: Satellite Server that installs and automatically enables on the same machine as Oracle WebCenter Sites software. This is your *co-resident* Satellite Server. It gives development and management systems the ability to simulate page delivery as it occurs on the active site (delivery system).

The following figure shows the topology for a Satellite Server co-resident installation. For more information on Satellite Server, see Caching to Optimize Performance in *Developing with Oracle WebCenter Sites*.

Figure 1-4   Standard Installation Topology for Oracle WebCenter Sites: Satellite Server
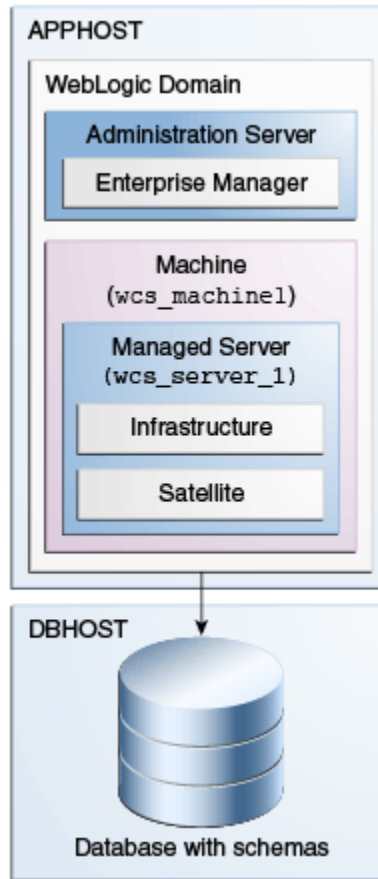
2

Preparing to Install and Configure Oracle WebCenter Sites

To prepare for your Oracle WebCenter Sites installation, verify that your system meets the basic requirements, then obtain the correct installation software.

- Roadmap for Installing and Configuring the Standard Installation Topologies
  This guide has all the 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.

- Roadmap for Verifying Your System Environment
  Before you begin the installation and configuration process, you must verify your system environment.

- About Product Distributions
  You create the initial Oracle WebCenter Sites domain using the Oracle Fusion Middleware Infrastructure distribution, which contains both Oracle WebLogic Server software and Oracle Java Required Files (JRF) software.

- Obtaining the Product Distribution
  You can obtain the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites distribution on the Oracle Technology Network (OTN).

- Prerequisites
  It is important to understand the prerequisites before you install the WebCenter Sites.

Roadmap for Installing and Configuring the Standard Installation Topologies

This guide has all the 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.

Table 2-1 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 Roadmap for Verifying Your System Environment.

Table 2-1   (Cont.) Standard Installation Roadmap

Task	Description	Documentation
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 *Release Notes for Oracle Fusion Middleware Infrastructure*.
Obtain the appropriate distributions	Obtain the Oracle Fusion Middleware Infrastructure and the Oracle WebCenter Sites installation files.	See About Product Distributions.
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 *Understanding Oracle Fusion Middleware*.
Install prerequisite software	Install Oracle Fusion Middleware Infrastructure to create the Oracle home directory for Oracle WebCenter Sites.	See *Oracle Fusion Middleware Installing and Configuring the Oracle Fusion Middleware Infrastructure*. There is no need to configure a domain for Infrastructure; the purpose of this task is to install oracle_common into the Oracle home.
Install the software	Run the Oracle Universal Installer to install Oracle WebCenter Sites. Installing the software transfers the software to your system and creates the Oracle home directory.	See Installing the Oracle WebCenter Sites Software.
Select a database profile and review any required custom variables.	Before you install required schemas in the database, review information about any custom variables you need to set for Oracle WebCenter Sites schemas.	See Understanding Database Requirements for an Oracle Fusion Middleware Installation.
Create the schemas	Run the Repository Creation Utility to create the schemas required for configuration.	See Creating the Database Schemas.
Create a WebLogic domain	Use the Configuration Wizard to create and configure the WebLogic domain.	See Configuring the Domain if you are creating the topology for Oracle WebCenter Sites.
Verify that you meet deployment prerequisites	Verify that your environment meets deployment requirements	See Completing Prerequisites for Configuring Visitor Services
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 Next Steps After Configuring the Domain.

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 Sites.

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 Verifying Certification, System, and Interoperability Requirements.
Identify a proper installation user.	Verify that the installation user has the required permissions to install and configure the software.	See Selecting an Installation User.
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 About the Directories for Installation and Configuration.
Install a certified JDK.	The installation program for the distribution requires a certified JDK present on your system.	See Understanding JDK Requirements for an Oracle Fusion Middleware Installation.
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 Sites.	See Understanding Database Requirements for an Oracle Fusion Middleware Installation.

- 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.

- About the 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.

- Understanding Database Requirements for an Oracle Fusion Middleware Installation
  Many 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.

ORACLE

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 *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.

- About Non-Default User Permissions on UNIX Operating Systems
  Changing the default permission setting reduces the security of the installation and your system. Oracle does not recommend that change the 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
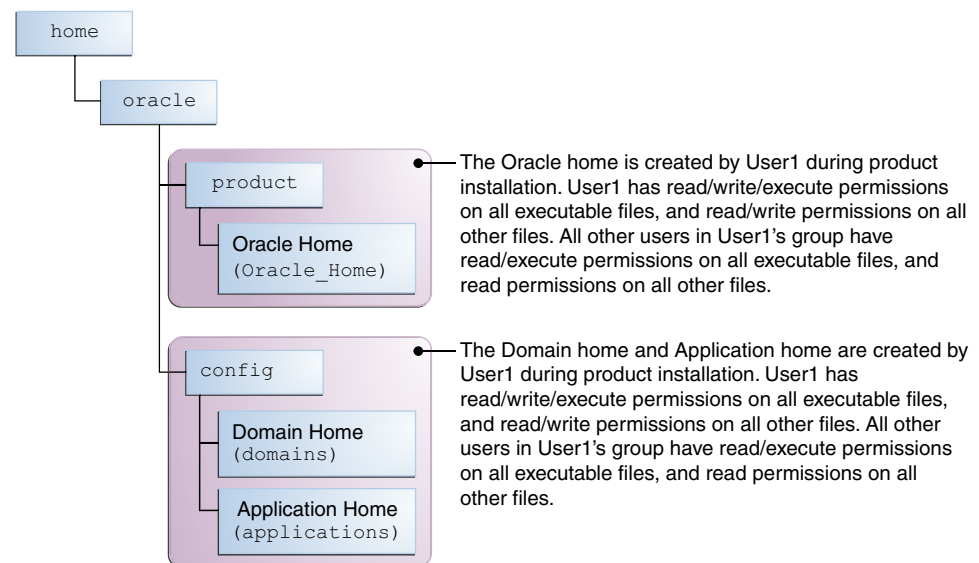
If the user who creates the domain is different than the user who installed the software, then both users must have the same privileges, as shown in the next example.

- **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

The Oracle home is created by User1 during product installation. User1 has read/write/execute permissions on all executable files, and read/write permissions on all other files. All other users in User1's group have read/execute permissions on all executable files, and read permissions on all other files.

The Domain home and Application home are created by User2 during product installation. User2 has read/write/execute permissions on all executable files, and read/write permissions on all other files. All other users in User2's group (including User1) have read/execute permissions on all executable files, and read permissions on all other files.

> **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.

About Non-Default User Permissions on UNIX Operating Systems

Changing the default permission setting reduces the security of the installation and your system. Oracle does not recommend that change the default permission settings.

If other users require access to a particular file or executable, use the UNIX `sudo` command or other similar commands to change the 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.

   > **Note:**
   >
   > For Oracle Identity and Access Management components, ensure that you have enabled User Account Control (UAC). If you have not done so already, enable UAC by following the instructions in the *Enabling User Account Control (UAC)* section from the appropriate version of *Oracle Fusion Middleware System Requirements and Specifications* for your installation.

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
```

About the 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.

- About 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.

About 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
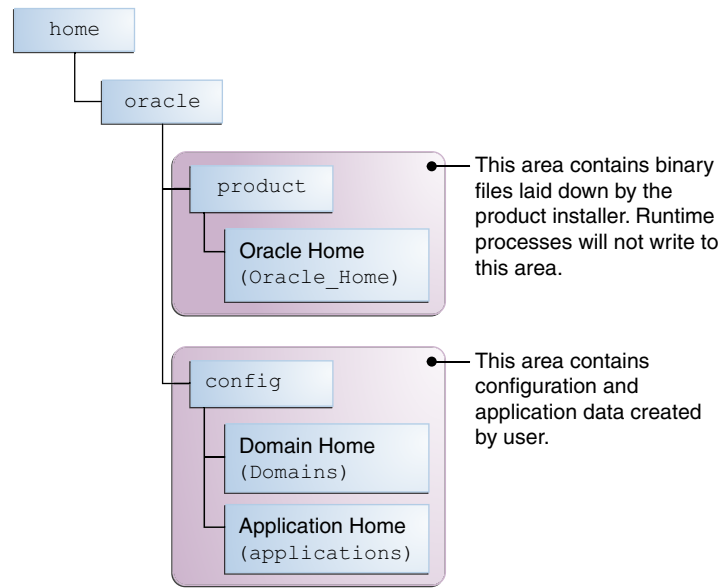
A base location (Oracle base) should be established on your system (for example, `/home/oracle`). From this base location, create two separate branches, namely, the `product` directory and the `config` directory. The `product` directory should contain the product binary files and all the Oracle home directories. The `config` directory should contain your domain and application data.

Oracle recommends that you do not keep your configuration datain the Oracle home directory; if you upgrade your product to another major release, are required to create a new Oracle home for binaries. You must also make sure that your configuration data exists in a location where 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 the 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 12*c* (12.2.1.3.0) Interoperability and Compatibility in *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 About 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 About 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 *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 *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 12*c* (12.2.1.3.0) Interoperability and Compatibility in *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 *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 12*c* (12.2.1.3.0), the certified JDK is 1.8.0_131 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

Understanding Database Requirements for an Oracle Fusion Middleware Installation

Many 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.

To make sure 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 Understanding Repository Creation Utility in *Creating Schemas with the Repository Creation Utility*.

About Product Distributions

You create the initial Oracle WebCenter Sites 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 Sites.

> **Note:**
>
> - **Dependant Softwares for Oracle Access Management:**
>
>   To configure Oracle Access Management, you must install Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0) prior to installing Oracle Identity and Access Management.
>
>   For information about installing Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0), see Installing the Infrastructure Software in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.
>
> - **Dependant Softwares for Oracle Identity Governance:**
>
>   Oracle Identity Governance requires Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0) and Oracle SOA Suite 12*c* (12.2.1.3.0). A quick installer is available for Oracle Identity Governance 12*c* (12.2.1.3.0), which installs Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12*c* (12.2.1.3.0) in one go. In other words, no separate installers are required for installing all the three softwares. If you wish to use the simplified installation process for Oracle Identity Governance, see Installing and Configuring Oracle Identity Governance Using Simplified Installation Process.
>
>   The other way is to install and configure Oracle Identity Governance in a traditional method, that is, installing Oracle Fusion Middleware Infrastructure and Oracle SOA Suite 12*c* (12.2.1.3.0) first, using their respective installers, and then installing Oracle Identity Governance.
>
>   For information about installing Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0), see Installing the Infrastructure Software in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.
>
>   For information about installing Oracle SOA Suite 12*c* (12.2.1.3.0), see Installing the Oracle SOA Suite and Oracle Business Process Management Software in *Installing and Configuring Oracle SOA Suite and Business Process Management*.
>
> For more information about the modes of installation supported for Oracle Identity and Access Management, see About the Modes of Installation.

Obtaining the Product Distribution

You can obtain the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites distribution on the Oracle Technology Network (OTN).

To prepare to install Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites:

1. Enter `java -version` on the command line to verify that a certified JDK is installed on your system. For 12*c* (12.2.1.3.0), the certified JDK is 1.8.0_131 and later.

   See Understanding JDK Requirements for an Oracle Fusion Middleware Installation.

2. Locate and download the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites software. To configure Oracle Identity Governance in collocated mode, you must download Oracle SOA Suite 12.2.1.3.0.

See Obtaining Product Distributions in *Planning an Installation of Oracle Fusion Middleware*.

Prerequisites

It is important to understand the prerequisites before you install the WebCenter Sites.

To prepare to install Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites, ensure to fulfill the following prerequisites:

- Oracle Database
  It is important to install Oracle database before you install the WebCenter Sites.

- Configuring a DB2 Database for WebCenter Sites
  Oracle recommends a specific database configuration for your DB2 database.

- MSSQL Server
  You need to install SQLServer before installing Oracle WebCenter Sites.

Oracle Database

It is important to install Oracle database before you install the WebCenter Sites.

You need to install Oracle database and create a database in order to install Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites. For more information about installing Oracle database and creating a database, see Installing Oracle Database and Creating a Database

Configuring a DB2 Database for WebCenter Sites

Oracle recommends a specific database configuration for your DB2 database.

To configure the DB2 database:

1. Create a file with the following DB2 commands. (For example, create `db.sql` and modify the database name, path, and user variables to match your installation):

```
CONNECT TO <DBNAME>;
UPDATE DATABASE CONFIGURATION USING APPLHEAPSZ 1024 DEFERRED;
UPDATE DATABASE CONFIGURATION USING LOCKTIMEOUT 30 DEFERRED;
UPDATE DATABASE CONFIGURATION USING APP_CTL_HEAP_SZ 1024 DEFERRED;
UPDATE DATABASE CONFIGURATION USING LOGFILSIZ 32768 DEFERRED;
UPDATE DATABASE CONFIGURATION USING LOGSECOND 8 IMMEDIATE ;
CONNECT RESET;
```

2. Run the SQL script.

MSSQL Server

You need to install SQLServer before installing Oracle WebCenter Sites.

To install SQLServer Management Studio, follow the steps below:

1. Login to SQLServer Management Studio.

2. Sign in with administrator rights.

3. Select Database and right-click to select **New Database**.

4. Right-click the RCU database and select **New Query**.

5. Enter the following queries:

```
ALTER DATABASE RCU SET READ_COMMITTED_SNAPSHOT ON
ALTER DATABASE RCU COLLATE LATIN1_GENERAL_CS_AS
```

6. Right-click the queries and select **Execute.**

7. Ensure the SQLServer and SQLServer browser runs in the SQLServer Configuration Manager.

3
Installing the Oracle WebCenter Sites Software

Follow the steps in this section to install the Oracle WebCenter Sites 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 Sites.

> **Note:**
>
> The product Oracle Identity Manager is referred to as Oracle Identity Manager (OIM) and Oracle Identity Governance (OIG) interchangeably in the guide.

> **Note:**
>
> The supported mode of installation for Oracle Access Management and Oracle Identity Governance 12*c* (12.2.1.3.0) is the collocated mode. The collocated mode requires some dependant softwares to be installed prior to installing Oracle Identity and Access Management.
>
> - Dependant Software for Oracle Access Management:
>   - Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0)
>
>   In case of Oracle Access Management, install Infrastructure first, and then proceed with the Oracle Identity and Access Management installation.
>
> - Dependant Softwares for Oracle Identity Governance:
>   - Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0)
>   - Oracle SOA Suite 12*c* (12.2.1.3.0)
>
>   For Oracle Identity Governance, a quick installer is available, which installs Infrastructure, Oracle SOA Suite, and Oracle Identity and Access Management 12*c* (12.2.1.3.0) in one go. You do not have to install these softwares using separate installers. If you wish to use a simplified installation process for Oracle Identity Governance, that is, installing Oracle Identity Governance using a quick installer, see Installing and Configuring Oracle Identity Governance Using Simplified Installation Process.
>
>   If you choose to install Oracle Identity Governance using the generic Oracle Identity and Access Management installer, then you must manually install Infrastructure and Oracle SOA Suite using their respective installers.
>
> For information about installing Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0), see Installing the Infrastructure Softwarein *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.
>
> For information about installing Oracle SOA Suite 12*c* (12.2.1.3.0), see Installing the Oracle SOA Suite and Oracle Business Process Management Software in *Installing and Configuring Oracle SOA Suite and Business Process Management*.
>
> The standalone mode of installation is supported only for the Oracle Identity Governance Design Console. In other words, if you wish to configure only the Design Console, you can install Oracle Identity and Access Management in a standalone mode, and then configure the Design Console.
>
> For more information about the modes of installation supported for Oracle Identity and Access Management, see About the Modes of Installation.

- 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 installation program shows a series of screens; see the following table for the order in which they appear.

- Verifying the Installation
  After you complete the installation, verify whether it was successful by completing a series of tasks.

- Creating the Database Schemas
  Before you can configure an Oracle WebCenter Sites 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.

- 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.

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 Sites installation.

Table 3-1   Installation Checklist

Information	Example Value	Description
`JAVA_HOME`	`/home/Oracle/Java/jdk1.8.0_131`	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`.
DBA password	`myDBApw957`	Password of the user with database administration privileges.
`ORACLE_HOME`	`/home/Oracle/product/ORACLE_HOME`	Directory in which you will install your software. This directory will include Oracle Fusion Middleware Infrastructure and Oracle WebCenter Sites, as needed.

Table 3-1   (Cont.) Installation Checklist

Information	Example Value	Description
WebLogic Server hostname	`examplehost.exampledomain`	Host name for Oracle WebLogic Server and Oracle WebCenter Sites consoles.
Console port	`7001`	Port for Oracle WebLogic Server and Oracle WebCenter Sites consoles.
DOMAIN_HOME	`/home/Oracle/config/domains/wcs_domain`	Location in which your domain data is stored.
APPLICATION_HOME	`/home/Oracle/config/applications/wcs_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	`ORACLE_HOME/oracle_common/bin`	Path to the Repository Creation Utility (RCU).
RCU schema prefix	`WCS`	Prefix for names of database schemas used by Oracle WebCenter Sites.
RCU schema password	`myRCUpw674`	Password for the database schemas used by Oracle WebCenter Sites.
Configuration utility	`ORACLE_HOME/oracle_common/common/bin`	Path to the Configuration Wizard for domain creation and configuration.
Configuration Assistant	`ORACLE_HOME/bi/bin`	Path to the Configuration Assistant for domain creation and configuration. Oracle recommends that you use the Configuration Assistant to configure your BI domain.

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. Change to the directory where you downloaded the installation program.

3. Start the installation program by running the `java` executable from the JDK directory. For example:

- **(UNIX)** `/home/Oracle/Java/jdk1.8.0_131/bin/java —jar fmw_12.2.1.2.0_wcsites_generic.jar`

- **(Windows)** `C:\home\Oracle\Java\jdk1.8.0_131\bin\java -jar fmw_12.2.1.2.0_wcsites_generic.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 *Installing Software with the Oracle Universal Installer*.

When the installation program appears, you are ready to begin the installation.

Navigating the Installation Screens

The installation program shows a series of screens; see the following table for the order in which they appear.

If you need additional help with an installation screen, click the screen name. You can also click **Help** on the installation screens for additional instructions.

Table 3-2   Oracle WebCenter Sites 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.
	For more about the central inventory, see Understanding the Oracle Central Inventory in *Installing Software with the Oracle Universal Installer*.
	This screen does not appear on Windows operating systems.
Welcome	This screen introduces you to the product installer.
Auto Updates	Use this screen to search for the latest software updates, including important security updates, via your My Oracle Support account.
Installation Location	Use this screen to specify your Oracle home directory location. This Oracle home should already contain Oracle Fusion Middleware Infrastructure.
	You can click **View** to verify and ensure that you are installing Oracle WebCenter Sites in the correct Oracle home.
	For more about Oracle Fusion Middleware directory structure, see Selecting Directories for Installation and Configuration in *Planning an Installation of Oracle Fusion Middleware*.

Table 3-2   (Cont.) Oracle WebCenter Sites Install Screens

Screen	Description
Installation Type	Choose the **WebCenter Sites** install option. If you want to install examples, choose **WebCenter Sites — With Examples**. To install Satellite Server *only*, choose **WebCenter Sites — Satellite Server**. All three options install Satellite Server.
	If you want to install Visitor Services, you can optionally select the **With Samples** option. If the **With Samples** option is selected, the distribution includes the samples folder. The samples folder contains the source code and JAR for the default provider bundles available in WebCenter Sites. This sample code can be used for modifying the code in the default provider bundles, or it can be used as a starting tool for creating custom provider bundles.
Prerequisite Checks	Verifies that your system meets the minimum necessary requirements.
	To view the list of tasks that gets verified, select **View Successful Tasks**. To view log details, select **View Log**.
	If there are warning or error messages, see one of the documents in Roadmap for Verifying Your System Environment.
Installation Summary	Use this screen to verify installation options you selected. If you want to save these options to a response file, click **Save Response File** and enter the response file location and name. You can use response files later if you perform a silent installation.
	All feature sets that are installed after installation is complete are listed here.
	For more about silent or command line installation, see Using the Oracle Universal Installer in Silent Mode in *Installing Software with the Oracle Universal Installer*.
	Click **Install** to begin the installation.
Installation Progress	Shows the installation progress.
	When the progress bar reaches 100% complete, click **Finish** to dismiss the installer or click **Next** to see a summary.
Installation Complete	Review the summary information on this screen, then click **Finish** to dismiss 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 *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 *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 *Installing Software with the Oracle Universal Installer*.

Creating the Database Schemas

Before you can configure an Oracle WebCenter Sites 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.

See Understanding 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 12*c* (12.2.1.3.0), the certified JDK is 1.8.0_131 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_131`

    *   (Windows) `set JAVA_HOME=C:\home\Oracle\Java\jdk1.8.0_131`

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
    The custom prefix logically groups together schemas together for use in this domain only; you must create a unique set of schemas for each domain. Schema sharing across domains is not supported.

- 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 *Creating Schemas with the Repository Creation Utility*.

- If the DBA has already run the SQL script for System Load, select **Perform 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 service name for your database, 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 example:

Database Type: `Oracle Database`
Host Name: `examplehost.exampledomain.com`
Port: `1521`
Service Name: `Orcl.exampledomain.com`
User Name: `sys`

Password: ******
Role: SYSDBA

Click **Next** to proceed, then click **OK** in the dialog window that confirms a successful database connection.

Specifying a Custom Prefix and Selecting Schemas

The custom prefix logically groups together schemas together for use in this domain only; you must create a unique set of schemas for each domain. Schema sharing across domains is not supported.

Select **Create new prefix**, specify a custom prefix, then select **WebCenter Sites**. This action automatically selects the following schemas as dependencies:

- Oracle Platform Security Services

- Audit Services

- Audit Services Append

- Audit Services Viewer

- WebCenter Sites

- WebCenter Sites—Visitor Services

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.

The Configuration Wizard also automatically creates the schema Common Infrastructure Services. This schema is grayed out; you cannot select or deselect it. This schema enables you to retrieve information from RCU during domain configuration. For more details about schemas, see Understanding the Service Table Schema in *Creating Schemas with the Repository Creation Utility*.

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 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.

You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

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. Select the **Encrypt Tablespace** check box if you want to encrypt all new tablespaces that the RCU creates.

When you reach the Completion Summary screen, click **Close** to dismiss the RCU.

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 *Creating WebLogic Domains Using the Configuration Wizard*.

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.

- Starting the Configuration Wizard
  Start the Configuration Wizard to begin configuring a domain.

- 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.

- 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 Configuration Templates for Oracle WebCenter Sites

- 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).

ORACLE®

- **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.

- **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 Sites**
  You configure Oracle WebCenter Sites components in a standalone domain. See the following topics to configure Managed Servers for Oracle WebCenter Sites.

- **Configuring a Cluster for WebCenter Sites**

- **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 Sites 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 Sites 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 Sites 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.

- Completing WebCenter Sites Configuration
  The End of Configuration screen shows information about the domain you just configured.

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 12*c* (12.2.1.3.0) Oracle home.

2. Enter the following command:

   (UNIX) `./config.sh`

   (Windows) `config.cmd`

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 *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 *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 *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.

    This is the recommended option for Oracle Identity and Access Management 12*c* (12.2.1.3.0).

Selecting the Configuration Templates for Oracle WebCenter Sites

On the Templates screen, make sure **Create Domain Using Product Templates** is selected, then select the following templates:

- Oracle WebCenter Sites - 12.2.1.3.0 [wcsites]

- Oracle WebCenter Sites - Visitor Services- 12.2.1.3.0 [wcsites]

- Oracle WebCenter Sites - Satellite Server - 12.2.1.3.0 [wcsites]

- Oracle WebCenter Sites - SiteCapture - 12.2.1.3.0 [wcsites]

- 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]

See Templates in *Creating WebLogic Domains Using the Configuration Wizard* for more information about options on this screen.

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 *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 *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 *Creating WebLogic Domains Using the Configuration Wizard*.

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.

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. Example: `orcl.exampledomain.com`
Host Name	Enter the name of the server hosting the database. Example: `examplehost.exampledomain.com`
Port	Enter the port number on which the database listens. Example: `1521`
Schema Owner 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 Specifying Schema Passwords). The default username is `prefix_STB`, where `prefix` is the custom prefix that you defined in the RCU.

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 *Creating Schemas with the Repository Creation Utility*.

See Database Configuration Type in *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. If you selected **Manual configuration** on the Database Configuration screen, you must configure the schemas listed in the table manually, before you proceed.

For high availability environments, see the following sections in *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 *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 *Creating WebLogic Domains Using the Configuration Wizard*.

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 Sites 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 *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 *Creating WebLogic Domains Using the Configuration Wizard*.

For more about Node Manager types, see Node Manager Overview in *Administering Node Manager for Oracle WebLogic Server*.

Configuring Managed Servers for Oracle WebCenter Sites

You configure Oracle WebCenter Sites components in a standalone domain. See the following topics to configure Managed Servers for Oracle WebCenter Sites.

> **Note:**
>
> See Log File Location for Oracle Fusion Middleware Components in *Administering Oracle Fusion Middleware* for the log file location of Oracle WebCenter Sites components.

- Configuring Managed Servers for WebCenter Sites
- Configuring Managed Servers for Oracle WebCenter Sites: Site Capture
- Configuring Managed Servers for Oracle WebCenter Sites: Satellite Server

- Configuring Managed Servers for Oracle WebCenter Sites: Visitor Services

Configuring Managed Servers for WebCenter Sites

Use the Managed Servers screen to configure multiple Managed Servers.

On the *Managed Servers* screen, a new Managed Server named `wcs_server_1` is created:

1. In the *Listen Address* drop-down list, select the IP address of the host that the Managed Server 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. Click **Enable SSL** to enable security.

   The Server Group field has **WCSITES-MGD-SVR** selected by default. **Server groups** target Fusion Middleware applications and services to one or more servers by mapping defined application service groups to each defined server group. A given application service group may be mapped to multiple server groups if needed. Any application services that map to a given server group are automatically targeted to all servers that are assigned to that group. For more information, see Application Service Groups, Server Groups, and Application Service Mappings in *Domain Template Reference*.

3. Click **Add** and repeat this process to create a second Managed Server named `wcs_server_2`. You must select the Server Group **WCSITES-MGD-SVR** for additional Managed Servers that you add.

   Configuring a second Managed Server is one of the steps needed to configure the standard topology for high availability. If you are *not* creating a highly available environment, then this step is optional.

   For more information about the high availability standard topology, see Understanding the Fusion Middleware Standard HA Topology in *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.

These Managed Server names are example names; this guide references them in other topics. If you choose different names, be sure to substitute them for the example names.

For more information about options on this screen, see Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring Managed Servers for Oracle WebCenter Sites: Site Capture

Use the Managed Servers screen to configure multiple Managed Servers.

On the *Managed Servers* screen, a new Managed Server named `sc_server_1` is created:

1. In the *Listen Address* drop-down list, select the IP address of the host that the Managed Server 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. Click **Enable SSL** to enable security.

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. An application service group may map to multiple server groups if needed. Any application services that map to a specific server group automatically target all servers assigned to that group. For more information on server groups, see Application Service Groups, Server Groups, and Application Service Mappings in *Domain Template Reference*.

4. Click **Add** and repeat this process to create a second Managed Server named `sc_server_2`. You must select the Server Group **SITECAPTURE-MGD-SVR** for additional Managed Servers that you add.

   Configuring a second Managed Server is one of the steps needed to configure the standard topology for high availability. If you are *not* creating a highly available environment, then this step is optional.

   For more information about the high availability standard topology, see Understanding the Fusion Middleware Standard HA Topology in *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.

These Managed Server names are example names; this guide references them in other topics. If you choose different Managed Server names, be sure to substitute them for the example names as needed.

For more information about options on this screen, see Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring Managed Servers for Oracle WebCenter Sites: Satellite Server

Use this screen to configure a Managed Server.

On the *Managed Servers* screen, a new Managed Server named `ss_server_1` is created:

1. In the *Listen Address* drop-down list, select the IP address of the host that the Managed Server 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. Click **Enable SSL** to enable security.

3. In the Server Groups drop-down list, select **SATELLITE-MGD-SVR**. This server group ensures that Oracle WebCenter Sites: Satellite Server services target the Managed Server 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. A given application service group may be mapped to multiple server groups if needed. Any application services that map to a given server group are automatically targeted to all servers that are assigned to that group. For more information about managed servers, see Application Service Groups, Server Groups, and Application Service Mappings in *Domain Template Reference*.

These server names and will be referenced throughout this document; if you choose different names be sure to replace them as needed.

For more information about options on this screen, see Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring Managed Servers for Oracle WebCenter Sites: Visitor Services

Use this screen to configure Managed Servers.

On the *Managed Servers* screen, a new Managed Server named `vs_server_1` is created:

1. In the *Listen Address* drop-down list, select the IP address of the host that the Managed Server 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. Click **Enable SSL** to enable security.

3. In the Server Groups drop-down list, select **VS-MGD-SVR**. This server group ensures that Oracle WebCenter Sites: Visitor Services and Oracle Web Services Manager (OWSM) services target the 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. A given application service group may be mapped to multiple server groups if needed. Any application services that map to a given server group are automatically targeted to all servers that are assigned to that group. For more information about server groups, see Application Service Groups, Server Groups, and Application Service Mappings in *Domain Template Reference*.

4. Click **Add** and repeat this process to create a second Managed Server named `vs_server_2` You must select the Server Group **VS-MGD-SVR** for additional Managed Servers that you add.

    Configuring a second Managed Server is one of the steps needed to configure the standard topology for high availability. If you are *not* creating a highly available environment, then this step is optional.

    For more information about the high availability standard topology, see Understanding the Fusion Middleware Standard HA Topology in *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.

These server names and will be referenced throughout this document; if you choose different names be sure to replace them as needed.

For more information about options on this screen, see Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring a Cluster for WebCenter Sites

Use the Clusters screen to create a new cluster:

1. Click **Add**.

2. Specify `wcs_cluster_1` in the Cluster Name field.

3. Leave the Cluster Address field blank.

Repeat the preceding steps to create `sc_cluster_1`, `ins_cluster_1` and `vs_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 *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. For more information about clusters, see Create and Configure Clusters in *Oracle WebLogic Server Administration Console Online Help*.

For more information about options on this screen, see Clusters in *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 *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 *High Availability Guide*.

Assigning WebCenter Sites 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 *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, `wcs_cluster_1`.

2. In the Servers pane, assign `wcs_server_1` to `wcs_cluster_1` by doing one of the following:

    • Click once on `wcs_server_1` to select it, then click the right arrow to move it beneath the selected cluster (`wcs_cluster_1`) in the Clusters pane.

    • Double-click on `wcs_server_1` to move it beneath the selected cluster (`wcs_cluster_1`) in the Clusters pane.

3. Repeat to assign `wcs_server_2` to `wcs_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 *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 Sites 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 *High Availability Guide*.

To create a new WebCenter Sites 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 `wcs_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 *Creating WebLogic Domains Using the Configuration Wizard*.

Assigning Servers to WebCenter Sites 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, `wcs_machine_1`.

2. In the Servers pane, assign `AdminServer` to `wcs_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 (`wcs_machine_1`) in the Machines pane.

   - Double-click on `AdminServer` to move it beneath the selected machine (`wcs_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 *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 *Creating WebLogic Domains Using the Configuration Wizard*.

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 *Creating WebLogic Domains Using the Configuration Wizard*.

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 *Creating WebLogic Domains Using the Configuration Wizard*.

Completing WebCenter Sites Configuration

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

    — Needed to access scripts that start Node Manager and Administration Server.

*   Administration Server URL

    — Needed to access the Administration Server.

Links at the bottom of the screen go to this guide and the Satellite Server Guide

Click **Finish** to dismiss the Configuration Wizard and continue installation.

4

Configuring WebCenter Sites Domain

After you have installed WebCenter Sites, 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 Sites
- Installing the Oracle WebCenter Sites Software

Refer to the following sections to create the database schemas, configure a WebLogic domain, and verify the configuration:

- 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.

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 *Administering Oracle Fusion Middleware*.

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

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_131`
   - (Windows) `set JAVA_HOME=C:\home\Oracle\Java\jdk1.8.0_131`
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 *Administering Node Manager for Oracle WebLogic Server*.

Starting the Administration Server

To start the Administration Server:

1. Change to the following directory:
   - (UNIX) `setenv JAVA_HOME /home/Oracle/Java/jdk1.8.0_131`
   - (Windows) `set JAVA_HOME=C:\home\Oracle\Java\jdk1.8.0_131`
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 the Administrator Account screen provides.

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

In production mode, you can create a boot identity file to bypass the need to provide a user name and password when starting the Administration Server. See Creating a Boot Identity File for an Administration Server in *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 *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 (Completing WebCenter Sites Configuration). 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 servers configured for this domain and shows their status (such as **Running** or **Shutdown**). For a newly configured domain, only the **AdminServer(admin)** will be running.

3. Select the first Managed Server.

4. Next to the **WebLogic Server** menu, select **Start Up**.

5. Repeat Steps 3 and 4 to start all Managed Servers.

6. On the main landing page, verify that all Managed Servers are up and running.

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.

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.

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 *Administering Oracle Fusion Middleware*.
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 *Administering Oracle Fusion Middleware*.
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 *Administering Oracle Fusion Middleware*.
Monitoring Oracle Fusion Middleware	Learn how to keep track of the status of Oracle Fusion Middleware components.	See Monitoring Oracle Fusion Middleware in *Administering Oracle Fusion Middleware*.
Understanding Backup and Recovery Procedures	Learn recommended backup and recovery procedures for Oracle Fusion Middleware.	See Introducing Backup and Recovery in *Administering Oracle Fusion Middleware*.

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 *Administering Oracle Fusion Middleware*.
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 *Installing and Configuring Oracle HTTP Server*. See also Installing Multiple Products in the Same Domain for important 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.	For more information about Coherence clusters, see Configuring and Managing Coherence Clusters in *Administering Clusters for Oracle WebLogic Server*. For information on tuning Coherence, see Performance Tuning in *Administering Oracle Coherence*. For information on storing HTTP session data in Coherence, see Using Coherence*Web with WebLogic Server in *Administering HTTP Session Management with Oracle Coherence*Web*. For more about creating and deploying Coherence applications, see Getting Started in *Developing Oracle Coherence Applications for Oracle WebLogic Server*.

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 Scaling Out a Topology (Machine Scale Out) in the *High Availability Guide*.

Table 5-3   (Cont.) Tasks Required to Prepare Your Environment for High Availability

Task	Description	More Information
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 Configuring High Availability for Web Tier Components in *High Availability Guide*.
Setting up a front-end load balancer	A load balancer can be used to distribute requests across servers more evenly.	See Server Load Balancing in a High Availability Environment and Configuring Load Balancer Virtual Server Names and Ports in *High Availability Guide*.
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 *Administering Node Manager for Oracle WebLogic Server*.
Configuring high availability for Oracle BI components	To configure Oracle BI for high availability, ensure that the system has no single points of failure by scaling out the Oracle BI Server, Presentation Services, and the JavaHost so that you have at least two of each component types, distributed across at least two computers.	See Deploying Oracle Business Intelligence for High Availability in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.
Managing performance tuning and query caching	For Oracle BI Server database queries to return quickly, the underlying databases must be configured, tuned, and indexed correctly. The BI Server can store query results for reuse by subsequent queries. Query caching can dramatically improve the performance of the system for users, particularly for commonly used dashboards. However, it does not improve performance for most ad-hoc analysis.	See Managing Performance Tuning and Query Caching in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Part II

Configuring WebCenter Sites Components

After you install and configure Oracle WebCenter Sites, you need to configure its component applications. See the topics in this section to configure component applications.

- Sites Configuration Setup

- Configuring WebCenter Sites
  After you configure the Oracle WebCenter Sites Managed Servers, you can configure a WebCenter Sites instance by completing the browser-based WebCenter Sites Configurator. WebCenter Sites runtime consists of WebCenter Sites and CAS web applications (WAR files) and the following components shared across cluster members: a `config` directory, a `data` directory, and a database instance.

- Configuring Site Capture
  After you configure Oracle WebCenter Sites: Site Capture Managed Servers, you can configure Site Capture with the Site Capture Configurator. You can also integrate Site Capture with the WebCenter Sites publishing process.

- Configuring Visitor Services
  After you set up the Oracle WebCenter Sites: Visitor Services Managed Servers, you can configure Visitor Services with the browser-based Visitor Services Configurator. Visitor Services runtime consists of `visitors-webapp` applications (WAR files), a `config` directory, a database instance, sample bundle code, providers, and a visitors client.

- Configuring Remote Satellite Server
  After you set up a WebLogic domain for Oracle WebCenter Sites: Satellite Server, you can run the Satellite Server Configurator to complete the configuration process.

- Switching to External Authentication
  For maximum security in production environments, Oracle recommends integrating Oracle WebCenter Sites with Oracle Access Management, for an advanced identity management solution and a seamless single sign-on user experience. You also have the option of integrating WebCenter Sites with an external LDAP authentication provider directory.

- Setting Up a CAS Cluster
  You can set up a Central Authentication Server (CAS) cluster in the same WebLogic domain as Oracle WebCenter Sites, in a different WebLogic domain on the same machine, or for high availability, in a different WebLogic domain on a different machine.

- Setting Up a Cluster
  For high availability, you can set up a WebCenter Sites cluster in a WebLogic domain with a primary cluster node on one machine and one or more secondary cluster nodes on the same or different machines. The first WebCenter Sites Managed Server you create is the primary node, and any additional WebCenter Sites Managed Servers in the same domain are secondary nodes.

ORACLE®

- Moving the Shared File System to a Database
  WebCenter Sites can leverage a database to store its shared file system using the Java Nonblocking I/O (NIO) API. This eliminates the need for a network file share in a clustered environment and allows file locking to be handled by a Coherence cache.

- Switching from Test Mode to Production Mode
  After you install and configure an Oracle WebCenter Sites domain in a Fusion Middleware test environment, you can switch WebCenter Sites (and its component applications) to an equivalent production environment.

6
Sites Configuration Setup

Before configuring the WebCenter Sites Configuration Setup, ensure the following prerequisites are met:

- Oracle Database must be installed
- Infrastructure Binary files must be installed
- WebCenter Sites Binary files must be installed
- Execution of Repository Creation Unit
- Execution of Domain Configuration Utility

To configure the Sites configuration set:

1. Start the services by running `http://<hostname>:<port>/sites/sitesconfigsetup` url.

   You can see Oracle WebCenter Sites Configurator screen, which contains the version number.

2. Click **Begin** button. The WebCenter Sites Shared Directory screen appears.

3. In the WebCenter Sites Shared Directory, you can either **browse** and navigate to the required path or mention the path where you want to store your shared files.

   > **Note:**
   >
   > In a typical installation, the files are usually stored in the `Domainhome` folder but for Cluster installations or any other customer specific installations, you can specify the required path.

4. Click **Next**. The Database Parameters screen appears.

5. In the Database Parameters screen, provide the `JNDI Database` source name.

6. Click **Next**. The Web Application Parameter screen appears.

7. In the Web Application Parameter screen,

   a. Enter the `host name` for WebCenter Sites

   b. Enter the `port number` for WebCenter Sites

   c. Select **Yes** if you are installed through a secure connection

   > **Note:**
   >
   > If you have installed only Weblogic Server then you need to provide Weblogic Server host and port number. In case, you have integrated your Weblogic Server with any application server, for example : Apache Server then you need to provide the Apache server details.

8. Click **Next**. The CAS Deployment Information screen appears.

9. In the CAS Deployment Information screen, enter the following:

    a. Server host name where is WebCenter Sites is installed

    b. Server port number where is WebCenter Sites is installed

    c. Server host name of internally accessible CAS

    d. Server port number of internally accessible CAS

    > **Note:**
    >
    > Provide the Weblogic server Host name for examplem, Server host name where CAS is actually deployed irrespective whether WebLogic got integrated with Webserver(Apache) or not.

10. Click **Next**. The WebCenter Sites Administrator Accounts screen appears.

11. In the WebCenter Sites Administrator Accounts screen, click Next button if you want to retain the default passwords provided in the UI. In case you want to change these passwords enter the new password and reenter to confirm the same.

    > **Note:**
    >
    > If you want to change these passwords, ensure to make a note of them.

12. Click **Next**. The Configuration Summary screen appears.

13. In the Configuration Summary screen, you can test these setting if they are connecting to the Database values that you have provided in the earlier screens, by clicking **Test** button. If the test is successful you can start the services by clicking **Start** button. The schema is created that is required for the WebCenter sites installation in the database.

14. Restart the services.

15. Enter WebCenter Sites URL in the browse and log in to the application.

7

Configuring WebCenter Sites

After you configure the Oracle WebCenter Sites Managed Servers, you can configure a WebCenter Sites instance by completing the browser-based WebCenter Sites Configurator. WebCenter Sites runtime consists of WebCenter Sites and CAS web applications (WAR files) and the following components shared across cluster members: a `config` directory, a `data` directory, and a database instance.

The following topics describe how to configure WebCenter Sites:

- Completing Prerequisites for Configuring WebCenter Sites
  Several prerequisite tasks must be done before you use the WebCenter Sites Configurator. These tasks include modifying cache files, creating database schemas, configuring a WebCenter Sites domain, and setting property values for your environment.

- Configuring WebCenter Sites with the Configurator
  The WebCenter Sites Configurator populates the database with tables and data necessary for WebCenter Sites to function. The Configurator also creates the necessary user accounts and sets the required permissions on the database objects.

- Managing Customizations with WebCenter Sites Deployment
  It is recommend to not include any implementation specific customizations to Sites WAR file as the changes will be overwritten during patching process and is redeployed.

- Configuring and Deploying the REST-avisports Sample Site
  REST-avisports is a sample website that demonstrates client-side website development using the WebCenter Sites Aggregate REST API.

- Creating a WebCenter Sites Web Tier
  After you configure a domain, you set up Oracle Web Tier or a third-party web tier.

Completing Prerequisites for Configuring WebCenter Sites

Several prerequisite tasks must be done before you use the WebCenter Sites Configurator. These tasks include modifying cache files, creating database schemas, configuring a WebCenter Sites domain, and setting property values for your environment.

Before configuring WebCenter Sites, make sure these prerequisite tasks are done:

> ✎ **Note:**
>
> If RSS is installed in a separate domain, you need to run `grant-opss-permission.sh` or `grant-opss-permission.bat`. Make sure that these files contains the specified domain name before running it. If necessary, edit the file and update the domain name.

1. In the WebCenter Sites `config` directory, modify the files `cs-cache.xml`, `ss-cache.xml`, `linked-cache.xml`, and `cas-cache.xml` as follows:

   a. Locate the following section:

   ```
   <cacheManagerPeerProviderFactory
   class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFacto
   ry" properties="peerDiscovery=automatic,
   multicastGroupAddress=230.0.0.0, multicastGroupPort=4444,
   timeToLive=0" />
   ```

   b. Change the value of the `peerDiscovery` property to manual. If Sites is run on Cluster the `peerDiscovery` property value should be automatic.

   > **Note:**
   >
   > WebCenter Sites is implemented on multicast to support caching and there could be network issues if another Sites instance or any other application using same multi cast address. Hence it's recommended to change `peerDiscovery` property to manual.

   c. Save and close the file.

   d. Start the WebCenter Sites Managed Server.

   WebCenter Sites is implemented on multicast to support caching and there could be network issues if another Sites instance or any other application using same multi cast address. Hence it's recommended to change `peerDiscovery` property to `manual`.

2. Use the Repository Creation Utility (RCU) to create database schemas for WebCenter Sites, as Creating the Database Schemas describes.

3. Use the Fusion Middleware Configuration Wizard with the `Oracle WebCenter Sites - 12.2.1.3.0[wcsites]` template to create a new domain and configure one or more WebCenter Sites Managed Servers, as Configuring the Domain describes.

Typically, Sites uses the time zone setting of the WebLogic JVM. However, if you want to use a different time zone, ensure that you change it immediately after you install Sites, that is, before you create any data in the target (12.2.1.3.0) environment.

Data Source for IBM DB2

For IBM DB2 WebCenter Sites does not support the default data source created by the Fusion Middleware Configuration Wizard. To create new data source with a driver that DB2 supports:

1. Add the IBM DB2 Driver JAR files to the class path for the WebCenter Sites domain:

   a. Stop the WebLogic Server Administration Server.

   b. Copy the `db2jcc.jar` and `db2jcc_license_cu.jar` files from DB2 to a location that you can add to the domain classpath.

   c. Edit *DOMAIN_HOME*/bin/setDomainEnv.sh and add the following line after `# ADD EXTENSIONS TO CLASSPATHS`:

```
PRE_CLASSPATH="path_to_db2jcc.jar:path_to_db2jcc_license_cu.jar:$
{PRE_CLASSPATH}"
```

    d. Start the Administration Server.

2. Create a new data source using the preceding DB2 driver. For more information, see Specifying JDBC Component Schema Information.

Data Source for Sites DB2

WebCenter Sites doesn't support the default data source created by Configuration Wizard. Follow the steps listed below to create new data source with supported driver.

1. Add the IBM DB2 Driver jar files to the domain classpath.

    a. Stop WebLogic Administration Server.

    b. Copy the `db2jcc.jar` and `db2jcc_license_cu.jar` from DB2 to a location that can be added to the domain classpath.

    c. Update `<domain_home>`/bin/setDomainEnv.sh and after `# ADD EXTENSIONS TO CLASSPATHS` add the below line:

```
PRE_CLASSPATH="<path_to_db2jcc.jar>:<path_to_db2jcc_license_cu.ja
r>${PRE_CLASSPATH}"
```

    d. Start WebLogic Administration Server.

2. Create new Data Source using above driver. For more information see, Creating and Configuring a Data Source

Configuring WebCenter Sites with the Configurator

The WebCenter Sites Configurator populates the database with tables and data necessary for WebCenter Sites to function. The Configurator also creates the necessary user accounts and sets the required permissions on the database objects.

> **Note:**
>
> If you are configuring WebCenter Sites over a slow network, increase the setting of the `StuckThreadMaxTime` property to 1000 seconds per thread before starting the WebCenter Sites Configurator. The default value is 600 seconds.
>
> In certain environments that potentially have network-related issues, the sample sites import process could take more than 600 seconds per thread during the WebCenter Sites configuration setup process. This can cause the import process or install to fail, and multiple exceptions in the log file. Oracle recommends increasing the setting to 1000 seconds to complete a successful installation of the sample sites.
>
> To change the value of `StuckThreadMaxTime`, in the WebLogic Server Administration Console for the domain, change to **Servers -> wcsites_server1 -> Configuration -> Tuning**.

To run the browser-based WebCenter Sites Configurator after the corresponding WebLogic domain has been successfully set up:

1. (Optional) To run the Configurator in silent mode:

    a. Edit the `DOMAIN_HOME`/wcsites/wcsites/config/`wcs_properties_bootstrap.ini` file, and complete the inline instructions.

    b. Start the WebCenter Sites Managed Server.

    c. Initiate the WebCenter Sites configuration process with the following command:

        •   On UNIX operating systems: xdg-open http://*sites-host*:*sites-port*/sites/sitesconfig

        •   On Windows operating systems: start http://*sites-host*:*sites-port*/sites/sitesconfig

2. To configure WebCenter Sites over a web server, increase the web server `timeout` value to `300 sec` before starting the WebCenter Sites configuration.

3. (Optional) Set the values of the following properties as appropriate for your environment, using the Property Management Tool in the Admin interface. Set these properties for a cluster that uses the NIO database-based file system. If you would like files stored in locations other than the default (individual folders under `DOMAIN_HOME`/wcsites/wcsites/config), specify the locations as property values because they cannot be changed once WebCenter Sites is up and running.

Properties	Description
`xcelerate.transformpath`	Directory where Microsoft Word files are stored before WebCenter Sites transforms those files into assets.
`cs.pgcachefolder`	Deprecated. Only set if instructed to do so by Oracle Support.
`cs.xmlfolder`	Working directory for HTML rendering.
`cs.pgexportfolder`	Base export directory for the HTML files that are created when assets are published with the Export to Disk delivery type.
`vis.path`	Directory where WebCenter Sites is installed. You must include the trailing slash.
`mwb.path`	Directory where WebCenter Sites is installed. You must include the trailing slash.
`contentserver.installation.folder`	Directory where WebCenter Sites is installed. You must include the trailing slash. Applies to installations in which Satellite Server and WebCenter Sites are running in the same web application and must therefore share the user's session. Specifying this enables Satellite Server to access WebCenter Sites resources.
`cs.csdtfolder`	Directory where WebCenter Sites Developer Tools imports are stored.

For more information on the preceding properties, see Overview of the Property Management Tool in *Property Files Reference for Oracle WebCenter Sites*.

4. Start the Managed Server for the WebCenter Sites primary cluster node.

5. In a web browser, access this URL: `http://sites-host:sites-port/sites/sitesconfigsetup`.

6. On the WebCenter Sites Configurator screen, click **Begin**.

7. On the Database Parameters screen, specify the **JNDI Datasource name** for the WebCenter Sites database repository This must be the repository you created using the Repository Creation Utility while setting up the WebLogic domain.

8. On the Web Application Parameters screen, select Yes if you are installing over a secure connection, leave all the parameters at their default (prepopulated) values, and click **Next**.

9. On the CAS Deployment Information screen, leave all parameters at their default (prepopulated) values and click **Next**. If using a cluster and a front-end web server for load balancing, adjust these values as appropriate for your environment.

10. On the WebCenter Sites Administrator Accounts screen, specify the credentials you want, and then click **Next**.

11. (Optional) If you chose the **WebCenter Sites with Examples** installation option when installing WebCenter Sites, the Sample Sites screen appears. On this screen, select the desired sample sites and click **Next**.

12. On the Configuration Summary screen, click **Test** and verify that all tests are successful. Then click **Start** and wait for the configuration process to complete.

13. Restart the Managed Server for the WebCenter Sites application.

14. Verify that WebCenter Sites is up and running by accessing the following URL in a web browser and logging in: `http://sites-host:sites-port/sites`.

> **✎ Note:**
>
> The default location for `cas.log` is `DOMAIN_HOME/servers/wcsites_server1/logs/`.

To get XMLPost and Bulkloader up and running, set the following directories in the `CLASSPATH` environment variable:

```
ORACLE_HOME\wcsites\webcentersites\sites-home\lib\*
ORACLE_HOME\oracle_common\modules\clients\*
```

For information about how to configure additional cluster nodes, see Setting Up a Cluster.

For information about how to configure an external LDAP authentication provider, see Switching to Authentication Against an LDAP Directory.

For information about how to configure Oracle Access Manager integration, see Switching to Authentication Against Oracle Access Manager.

For information about how to use the WebCenter Sites Configuration Import/Export Utility, see Using the Property Management Tool in *Property Files Reference for Oracle WebCenter Sites*.

Managing Customizations with WebCenter Sites Deployment

It is recommend to not include any implementation specific customizations to Sites WAR file as the changes will be overwritten during patching process and is redeployed.

The WebCenter Sites web application is shipped as a WAR file. The web application is deployed during Config Wizard process initially and can be redeployed multiple times during the application lifecycle. It is recommend to not include any implementation specific customizations to Sites WAR file as the changes will be overwritten during patching process and is redeployed.

Extending the WebLogic Server Shared Libraries framework, Sites provides `extend.sites.webapp-lib.war` as a shared library, located under `ORACLE_HOME/wcsites/webcentersites/sites-home/` directory. Any implementation specific customizations such as static web resources or Java libraries can be included in this WAR file. This shared library gets deployed during application lifecycle and shares the same context root as sites (/sites/). The contents of this shared library will not be overwritten during patching process.

> **Note:**
>
> • It is generally recommended to deploy the static artifacts such as images and stylesheet files onto the web server.
>
> • For more information on using the shared library, see Creating Shared Java EE Libraries and Optional Packages.

Configuring and Deploying the REST-avisports Sample Site

REST-avisports is a sample website that demonstrates client-side website development using the WebCenter Sites Aggregate REST API.

Before you configure and deploy the REST-avisports Sample Site, make sure these tasks are done:

• Install WebCenter Sites with **avisports** sample site.

• Start the WebCenter Sites Managed Servers and verify that they are running successfully.

To configure and deploy the REST-avisports Sample Site:

1. Locate the `sites-restavisports.war` file in the `ORACLE_HOME/wcsites/webcentersites/sites-home` directory.

2. Extract this WAR file.

3. Edit the `js/appconfig.js` file and provide this WebCenter Sites information:

   a. SITES_HOST_NAME = *sites-host*

   b. SITES_PORT = *sites-port* (for example: `7003`)

      c. `SITES_CONTEXT = sites context-root` (for example, `sites`)

4. The `sites-restavisports.war` can be deployed on any of the following servers:

      a. On a separate managed server that is available in the same domain as WebCenter Sites.

      b. On a dedicated Domain Server or an Application Server. A typical client-side website follow this setup.

When WebCenter Sites is running, you can access the REST-avisports sample site at this URL:

```
http://<restavisports-host-name>:<restavisports-deployed-port>/
<restavisports-app-context-path>
```

Creating a WebCenter Sites Web Tier

After you configure a domain, you set up Oracle Web Tier or a third-party web tier.

For Oracle Web Tier, see *Installing and Configuring Oracle HTTP Server* or *Installing Oracle Traffic Director* for instructions to do these tasks:

1. Install Oracle HTTP Server (OHS) or Oracle Traffic Director (OTD) in the same Oracle home as WebCenter Sites, or in a different domain.

2. Run the Configuration Wizard again to configure OHS or OTD to add it to (extend) the WebCenter Sites domain, or to create a standalone OHS or OTD domain.

3. Configure the mod_wls web server plug-in, which routes requests to Managed Servers.

For a third-party web server, see the documentation for the web server.

- Configuring the OHS Server
  Steps to configure Oracle HTTP Server (OHS).

Configuring the OHS Server

Steps to configure Oracle HTTP Server (OHS).

Steps for configuring the OHS Server

1. Install OHS version 12.2.1.3.0.

2. Change the configuration to bypass the ROOT of OHS.

- Peform the following change in the `mod_wl_ohs.conf` file located in the `<ORACLE_HOME>/user_projects/domains/<DOMAIN_NAME>/config/fmwconfig/components/OHS/instances/<OHS_INSTANCE_NAME>`

```
<IfModule weblogic_module>
WebLogicHost <WEBLOGIC_HOST_ON_WHICH_SITES_IS_INSTALLED>
WebLogicPort <WEBLOGIC_PORT_ON_WHICH_SITES_IS_INSTALLED>
MatchExpression
</IfModule>
```

3. For configuring Cluster, set the properties in the `mod_wl_ohs.conf` file located in the `<ORACLE_HOME>/user_projects/domains/<DOMAIN_NAME>/config/fmwconfig/components/OHS/instances/<OHS_INSTANCE_NAME>`.

```
<IfModule weblogic_module>
WebLogicCluster <HOST_AND_PORT_DETAILS>
MatchExpression
</IfModule>
<Location /sites>
    SetHandler weblogic-handler
</Location>
<Location /cas>
    SetHandler weblogic-handler
</Location>
```

> **Note:**
>
> If you are installing WebCenter Sites with Sample Sites on different Webservers (for example: On the OHS Server), ensure to add the following paramaters in library file of Weblogic Plug-in as this allows you to import avisports installable during config wizard.
>
> - WLIOTimeoutSecs=1200
>
> - KeepAliveEnabled=true
>
> If you do not add the parameters the config wizard will fail during the installation process. For more information of parameters, see Parameters for Web Server Plug-Ins.

4. After setting properties in the `mod_wl_ohs.conf` file, you be able to preview the crawled sites instead of OHS screen.

5. In addition to the above configuration, the following change is required for OHS version 11.1.0.9. The `DirectoryIndex` configuration in `httpd.conf` file should be modified to update the required change.

```
<IfModule dir_module>
DirectoryIndex index.html disabled
</IfModule>
```

8

Configuring Site Capture

After you configure Oracle WebCenter Sites: Site Capture Managed Servers, you can configure Site Capture with the Site Capture Configurator. You can also integrate Site Capture with the WebCenter Sites publishing process.

The following topics describe how to complete the configuration of Site Capture:

*   Configuring Site Capture with the Configurator
    The Site Capture Configurator provides instructions to configure Sites Capture in interactive or silent mode, after you complete the prerequisite tasks.

*   Integrating Site Capture with the WebCenter Sites Publishing Process
    The completion of a RealTime publishing session can trigger Site Capture if it is integrated with the WebCenter Sites publishing process. The following procedure integrates the WebCenter Sites publishing system to communicate with your installed Site Capture application.

Configuring Site Capture with the Configurator

The Site Capture Configurator provides instructions to configure Sites Capture in interactive or silent mode, after you complete the prerequisite tasks.

Before configuring Site Capture, ensure that the following prerequisites have been done:

*   Create the necessary database schemas using the Repository Creation Utility, For more information see,Creating the Database Schemas.

*   Deploy at least one fully functional instance of WebCenter Sites.

*   Create Managed Servers for Site Capture using the WebLogic Configuration Wizard and the `Oracle WebCenter Sites — Site Capture - 12.2.1.3.0 [wcsites]` template.

    For instructions, see Configuring the WebCenter Sites Domain.

You can start the Site Capture Configurator from the command line and run it in either interactive mode or silent mode to configure Site Capture. The Configurator provides configuration instructions.

> **Note:**
>
> When sites capture is installed in cluster on SSI using OHS webserver and integrated with OAM, below configuration must be performed.
>
> ```
> SITE OHS
> <IfModule weblogic_module>
> </IfModule>
> <IfModule weblogic_module>
> WebLogicCluster site-capture-host-node1:site-capture-port-
> node1,site-capture-host-node2:site-capture-port-node2
> MatchExpression *
> </IfModule>
> OAM OHS
> <IfModule weblogic_module>
> WebLogicHost load-balancer-host
> WebLogicPort load-balancer-port
> MatchExpression *
>     WLIOTimeoutSecs 1200
> KeepAliveEnabled true
>     ConnectTimeoutSecs 60
> ConnectRetrySecs 5
>     SecureProxy ON
>     WLProxySSL ON
>     WLProxySSLPassThrough ON
>     Debug ALL
> </IfModule>
> ```

Running the Site Capture Configurator in Interactive Mode

To run the Configurator in interactive mode, do these steps:

1. Using the command line, navigate to the `ORACLE_HOME`/wcsites/sitecapture/ directory.

2. Run the Site Capture Configurator: `java -jar sites-sitecapture-configurator.jar -configPath DOMAIN_HOME/wcsites/sitecapture/config`.

3. Follow the instructions displayed in the Configurator.

4. If the client is running Site Capture in an HTTPS environment, set the `cookie-secure` flag to `true` in `weblogic.xml`.

5. Start the Managed Server hosting this Site Capture instance.

Running the Site Capture Configurator in Silent Mode

To run the Configurator in silent mode, do these steps:

1. Edit the `DOMAIN_HOME`/wcsites/sitecapture/config/ `wcs_sitecapture_properties_bootstrap.ini` file and complete the instructions.

2. Use the command line to change to the `ORACLE_HOME`/wcsites/sitecapture/. directory.

3. Execute `java -jar sites-sitecapture-configurator.jar -silent`
   `DOMAIN_HOME/wcsites/sitecapture/config`.

4. Start the Site Capture Managed Server.

Completing the Configuration of Site Capture

1. Log in to WebCenter Sites.

2. Access the Admin interface, click the **Admin** Tab, and navigate to **System Tools**
   and then **Property Management Tool**.

3. Edit the `valid.urls` property, which accepts a comma-separated URLs. For Site
   Capture, add `http://sitecapture-host:sitecapture-Port/__admin/*`.

4. Start the WebCenter Sites Managed Server.

Completing Site Capture Cluster Configuration

For cluster configuration, the Site Capture configuration directory must be shared
across all the nodes in the cluster. The `DOMAIN_HOME/wcsites/sitecapture` directory
from the primary node must be mounted and shared across all other nodes in the
cluster. It should be a single copy of a folder used by all the nodes. This directory
include the following directories:

- `oracle.wcsites.sitecapture.config`
- `oracle.wcsites.sitecapture.crawler`

These paths to new shared location in `setStartupEnv.sh/.cmd` file.

> **Note:**
>
> If the `DOMAIN_HOME/wcsites/sitecapture/config/`
> `wcs_sitecapture_properties_bootstrap.ini` file was manually
> edited to change the WebCenter Sites password
> (`oracle.wcsites.app.password`) to a nonencrypted clear-text value, then the
> `oracle.wcsites.sitecapture.password.replace` value must be set to `true`.
> If both SiteCapture and WCS share the same
> KeyStore, then set the *oracle.wcsites.app.password=<saved in
> keystore>* or*oracle.wcsites.sitecapture.password.replace=true* to avoid any
> error caused by already existing key.

For more information about configuring Site Capture, see Using the Site Capture
Application in *Administering Oracle WebCenter Sites*.

> **Note:**
>
> Because changes you make to a WAR file are not retained during
> redeployment, WAR file changes need to be copied over after each
> redeployment of the web applications. It is generally recommended to deploy
> the static artifacts such as images and stylesheet files onto the web server.

Integrating Site Capture with the WebCenter Sites Publishing Process

The completion of a RealTime publishing session can trigger Site Capture if it is integrated with the WebCenter Sites publishing process. The following procedure integrates the WebCenter Sites publishing system to communicate with your installed Site Capture application.

To integrate Site Capture with the WebCenter Sites publishing process, do the following steps after you install and configure the Site Capture application:

1. On the WebCenter Sites source system, go to the `FW_PublishingEventRegistry` table and change the blocking value from `N` to `Y` for the listener `com.fatwire.cs.crawler.RemoteElementInvokingPublishingEventListener`.

2. On the WebCenter Sites target system, do these steps:

   a. Click the **Admin** tab, and navigate to **System Tools** and then **Property Management**.

   b. Search by category for "`Sitecapture`".

   c. Edit the following four properties, and update the values as follows:

      - `sitecapture.url`: Specify one of the following values:

        – For a single-server installation, specify the URL of the Site Capture application:

          `sc.url=http://site-capture-host:site-capture-port/__admin`

        – For a clustered installation, specify the URL of the load balancer:

          `sc.url=http://load-balancer-host:load-balancer-port/__admin`

      - `sitecapture.cas.url=http://cas-host:cas-port/cas`: Specify the CAS application that is pointed to by the Site Capture application.

      - `sitecapture.cs.username=Rest-Admin-User`: Specify the user name of the WebCenter Sites general Administrator exactly as it was specified during the Site Capture installation and configuration process.

      - `sitecapture.cs.password=Password`: Specify the Administrator user's password exactly as it was specified during the Site Capture installation and configuration process.

9

Configuring Visitor Services

After you set up the Oracle WebCenter Sites: Visitor Services Managed Servers, you can configure Visitor Services with the browser-based Visitor Services Configurator. Visitor Services runtime consists of `visitors-webapp` applications (WAR files), a `config` directory, a database instance, sample bundle code, providers, and a visitors client.

The following topics describe configuring Visitor Services:

- Completing Prerequisites for Configuring Visitor Services
  Before configuring Visitor Services, make sure the prerequisite tasks are done.

- Configuring Visitor Services with the Configurator
  The Visitor Services Configurator supports silent mode and interactive mode.

- Getting the Visitor ID
  The Oracle WebCenter Sites: Visitor Services `OAMIdentityProvider` is supported for Oracle Access Manager 11.1.2.2.0 and 11.1.2.3.0.

- Completing the Visitor Services Cluster Configuration
  Visitor Services is a completely stateless web application, so there is no need for session replication or session management at the cluster level. Cluster configuration of Visitor Services mainly involves taking care of configuration data.

- Visitors Service JMS Cluster Setup
  Configure JMS Cluster setup for Visitor Services using Persistent Store, JMS Server, and JMS Module.

Completing Prerequisites for Configuring Visitor Services

Before configuring Visitor Services, make sure the prerequisite tasks are done.

To complete prerequisites for configuring Visitor Services:

1. Create a WebCenter Sites – Visitor Services database schema with the Repository Creation Utility, as Creating the Database Schemas describes.

2. Create Managed Servers for Visitor Services using the Configuration Wizard and the `Oracle WebCenter Sites Visitor Services – 12.2.1.3.0[wcsites]` template, as Configuring the WebCenter Sites Domain describes.

> **✎ Note:**
>
> For IBM DB2, Visitor Services does not support the default data source that the Configuration Wizard creates. To create new data source with a driver that DB2 supports:
>
> **a.** Add the IBM DB2 Driver JAR files to the class path for the WebLogic domain.
>
>   **i.** Stop the WebLogic Server Administration Server.
>
>   **ii.** Copy the `db2jcc.jar` and `db2jcc_license_cu.jar` files from DB2 to a location that you can add to the domain class path.
>
>   **iii.** Edit `DOMAIN_HOME/bin/setDomainEnv.sh` and add the following line after `# ADD EXTENSIONS TO CLASSPATHS`:
>
>   `PRE_CLASSPATH="path_to_db2jcc.jar:path_to_db2jcc_license_cu.jar:${PRE_CLASSPATH}"`
>
>   **iv.** Start the Administration Server.
>
> **b.** Create a new data source using the preceding DB2 driver. For more information, see Specifying JDBC Component Schema Information.

Configuring Visitor Services with the Configurator

The Visitor Services Configurator supports silent mode and interactive mode.

To configure Visitor Services in silent mode:

1. Edit the `DOMAIN_HOME/wcsites/visitorservices/config/wcs_svs_properties_bootstrap.ini` file and update it with Oracle WebCenter Sites: Visitor Services details.

   If Java Messaging Service (JMS) needs to be configured, update the JMS details; otherwise, keep `visitors.jms_service_in_use=false`.

2. Start the Visitor Services Managed Server.

   Complete the bootstrap process of Visitor Services using this URL: `http://visitorservices-server:visitorservices-port/visitorservices-webcontext/bss`

3. Restart the Visitor Services Managed Server.

To configure Visitor Services in interactive mode:

1. Start the Visitor Services Managed Server.

2. In a web browser, access the Visitor Services Configurator at the following URL: `http://visitorservices-host:visitorservices-port/visitors-webapp/bootstrapconfig`

3. On the Visitor Services Configurator screen that appears, click **Begin**.

4. On the screen that appears, complete the Sites Web Application Parameters section as the following table shows.

Name	Description
Host name or IP address	Host name or IP address of the target WebCenter Sites instance.
Port number	Port number of the target WebCenter Sites instance.
Application context root	Context root of the target WebCenter Sites instance.
Secure connection?	If your environment is set up for SSL connectivity, select **Yes**; otherwise, select **No**.
Site name	Name of the target WebCenter Sites site.
Username	Name of the Administrator user account for the target WebCenter Sites instance.
Password	Password of the Administrator user account for the target WebCenter Sites instance.
Re-enter the Password	Confirm the password entered in the previous field.

5. Complete the Visitor Services Parameters section as follows:

Name	Description
Data Source JNDI Name	Full name of the Visitor Services data source. If you have used the Repository Creation Utility to create the Visitor Services data repository, this is automatically pre-populated.
Have you configured JMS resources?	If you want to integrate Visitor Services with Java Messaging Service, select **Yes**; otherwise, select **No**.
JMS connection factory JNDI name	Full name of the Java Messaging Service connection factory.
JMS enrichment queue JNDI name	Full name of the Java Messaging Service enrichment queue.
JMS profile update queue JNDI name	Full name of the Java Messaging Service profile update queue.
JMS Transaction support	Select **Yes** to enable Java Messaging Service transaction support; otherwise, select **No**.
JMS Persistence support	Select **Yes** to enable Java Messaging Service persistence support; otherwise, select **No**.

6. Click **Test** to test connectivity with the WebCenter Sites instance.

7. When the connectivity test succeeds, click **OK** to initiate the configuration process and wait for the confirmation screen to appear.

8. In the confirmation screen, you **must** click **Close** to commit your configuration; if you do not click **Close**, your configuration will be lost.

9. Restart the Visitor Services Managed Server.

10. Log in to the WebCenter Sites Admin interface.

11. Configure a Visitor Services Administrator user name and password in the WebCenter Sites Property Management Tool:

    a. Select the **Admin** interface icon.

    b. In the **Admin** tree, expand **System Tools**, and then double-click **Property Management**.

    c. Edit the `wcsites.visitors.auth.user` and `wcsites.visitors.auth.password` properties to set the user name and password.

12. Restart the WebCenter Sites Managed Server.

13. Create and enable an identity provider to use with Visitor Services. An identity provider authenticates site visitors to Visitor Services. Visitor Services ships with an Oracle Access Manager identity provider for integration with Oracle Access Manager.

14. (Optional) Create and enable an access provider to use with Visitor Services. An access provider authenticates REST calls made between Visitor Services and WebCenter Sites. Oracle recommends using an access provider to maintain a secure connection between Visitor Services and WebCenter Sites. Visitor Services ships with a basic LDAP access provider for authentication against an LDAP directory.

    You also need to set the following properties:

    - `wcsites.visitors.auth.password`
    - `visitors.rest.authalias`
    - `visitors.rest.authtype`
    - `visitors.rest.authheader`
    - `wcsites.visitors.auth.user`

15. Create and enable one or more profile providers. A profile provider allows the association of a visitor identity with a visitor profile. Visitor Services ships with an Eloqua profile provider for integration with the Eloqua Cloud Marketing Service, and an Oracle Access Manager profile provider for integration with Oracle Access Manager.

16. Create an aggregation template. An aggregation template determines what data, based on visitor profiles, is returned to the site visitors.

    For more information, see Developing WebCenter Sites: Visitor Services in *Developing with Oracle WebCenter Sites*.

17. Restart the WebCenter Sites and Visitor Services Managed Servers.

Getting the Visitor ID

The Oracle WebCenter Sites: Visitor Services `OAMIdentityProvider` is supported for Oracle Access Manager 11.1.2.2.0 and 11.1.2.3.0.

For information about installing Oracle Access Manager, see the *Oracle Identity and Access Management Installation Guide*.

To get the `visitorId` value using `OAMIdentityProvider`:

1. Log in to WebCenter Sites at `http://`*site-host*`:`*site-port*`/sites/`.

2. Select **AdminSite**, Select the **Admin** interface icon, and click **Hide Left Hand Navigation**, **Admin**, and then **Identity Providers List**.

3. Upload the `identity-provider-oam.jar` file located under `ORACLE_HOME/wcsites/visitorservices/providers/identity-providers/`, with appropriate configuration data in the configuration field.

4. Copy the configuration located under `ORACLE_HOME/wcsites/visitorservices/providersConfig/identity-provider-oam/identity-provider-oam.properties`.

5. Click `Profile Provider List`.

6. Make sure that the User Identity Store is configured for User profiles in Oracle Access Manager. (For User Identity Store configuration, see the *Oracle Identity and Access Management Installation Guide*.

7. Upload the `profile-provider-ldap.jar` file with the name `UserIdentityStore1` located under `ORACLE_HOME/wcsites/visitorservices/providers/profile-providers/` with appropriate configuration data in the configuration field.

8. Copy the configuration located under `ORACLE_HOME/wcsites/visitorservices/providersConfig/profile-provider-ldap/profile-provider-ldap.properties`.

9. The `get visitorId for user ex` test belongs to the Oracle Access Manager embedded LDAP using the following URL in a REST client:

   ```
   http://OHS-host:OHS-port/visitor-services-context/rest/v1/visitor/getId
   ```

   Add the headers `content-type` and `application/x-www-form-urlencoded`, and provide the request body:

   ```
   request={
   "parameters":"{}",
   "headers":"{}",
   "cookies":"[{}]"
   "header":"{\"oam_identity_domain\":\"UserIdentityStore1\",\"oam_remote_user\":\"test\"}"
   }
   ```

To get the `visitorId` value using `SampleIdentityProvider`:

1. Log in to WebCenter Sites at `http://sites-host:sites-port/sites/`

2. Select **AdminSite**, Select the **Admin** interface icon, and click **Hide Left Hand Navigation**, **Admin**, and then **Identity Providers List**.

3. Upload the `identity-provider-oam.jar` file located under `ORACLE_HOME/wcsites/visitorservices/providers/identity-providers/`, with appropriate configuration data in the configuration field.

4. Copy the configuration located under `ORACLE_HOME/wcsites/visitorservices/providersConfig/identity-provider-sample/identity-provider-sample.properties`.

5. Click `Profile Provider List`. (Make sure that Oracle Internet Directory or another LDAP authentication provider is installed and configured.

6. Upload the `profile-provider-ldap.jar` file located under `ORACLE_HOME/wcsites/visitorservices/providersConfig/profile-provider-ldap/profile-provider-ldap.properties`.

7. Copy the configuration located under `ORACLE_HOME/wcsites/visitorservices/providersConfig/profile-provider-ldap/profile-provider-ldap.properties`.

8. The `get visitorId for user` test belongs to the Oracle Internet Directory LDAP using the following URL in a REST client:

   ```
   http://visitorservices-host:visitorservices-port/visitorservices-context/rest/v1/visitor/getId
   ```

   Add the headers `content-type` and `application/x-www-form-urlencoded`, and provide the request body:

   ```
   request={
   "parameters":"{\"external_id\":[\"ssoid1\"]}",
   "headers":"{}",
   "cookies":"[{}]"
   "header":"{}"
   }
   ```

Completing the Visitor Services Cluster Configuration

Visitor Services is a completely stateless web application, so there is no need for session replication or session management at the cluster level. Cluster configuration of Visitor Services mainly involves taking care of configuration data.

After the first node (primary cluster node) has been created, all other nodes should use the configuration files from the primary cluster node. Of particular importance is the `visitors.properties` file. The main configuration file for Visitor Services is `visitors.properties`. This file contains details about the data source in the Visitor Services database, JMS objects, and a URL to a WebCenter Sites instance (either one node or if there is a WebCenter Sites cluster, the load-balancer URL). The secondary nodes can use the `visitors.properties` file from the primary cluster node in either of two ways:

- All nodes in the Visitor Services cluster can have a replica of the same Visitor Services file in their class path.

- All nodes can point to single `visitors.properties` file with file path being in a shared folder.

There is a single database for the entire Visitor Services cluster. The data source property in the `visitors.properties` file for each node should point to this single database.

Other Visitor Services configuration files are not meant for modification. Copy them as is from the primary node to the secondary nodes.

Although JMS is optional, Oracle recommended that JMS be used. Each node should point to same JMS objects. A nodes should not configure a different JMS queue because having that node down would result in losing out on messages present in that queue.

The `visitors-cache.xml` file provides distributed caching configuration for managing a cache of visitors objects (`identity provider`, `access provider`, `profile provider`, `aggregation templates`, and `visitor configuration`). Because this is a distributed cache, all the nodes should have same values for the following properties inside this file:

- `multicastGroupPort`
- `multicastGroupAddress`

Oracle recommends that you set the values for these properties in the `visitors-cache.xml` file on the primary cluster node and then copy the file to each secondary node. You could also do this manually, by making the change in the file locally, on each secondary node.

The `visitors-logging.xml` file provides log-level setting for different loggers. To have a consistent logging experience across nodes, Oracle recommends that all nodes use same file or propagate changes made on one node manually to local copies of this file on all nodes.

> **Note:**
>
> Because changes you make to a WAR file are not retained during redeployment, WAR file changes need to be copied over after each redeployment of the web applications. It is generally recommended to deploy the static artifacts such as images and stylesheet files onto the web server.

Integrating Visitor Services with OAM

If you have to run visitor services with sites integrated with OAM, ensure that the sites should have OAM installed and then run visitor services bootstrap using sites integrated with OAM login URL.

Visitor Services on Cluster

If visitor services needs to be installed on cluster:

- To run bootstrap on Webserver, ensure that only primary node of visitor services should be running.
- Then configuration directory of visitor services should be shared with both nodes or the config directory should be copied from primary node to other nodes, so that all nodes have the same properties.

Visitors Service JMS Cluster Setup

Configure JMS Cluster setup for Visitor Services using Persistent Store, JMS Server, and JMS Module.

Prerequisites

Before setting up the Visitors Services in Java Messaging Service (JMS) Cluster the following prerequisites have be set:

- Create at least two or more sites visitors servers in a cluster.

- Make a note of the host name or address of all cluster members.

- Create a common directory between all servers, for example: Figure 9-1 shows the directory path set for the server `/u01/oracle/12.2.1/tmp/prod/`.

Configuring Persistent Store

Using the **VSjms Support** wizard, configure the Persistent Store:

1. In the Persistent Stores, locate **WL left nav services**.

2. Select **Persistent Store** and then **Vsjms Support**.

3. In **Directory** field, point to valid shared filesystem, for example:`/u01/oracle/12.2.1/tmp/prod/`.

4. In the location on disk `/u01/oracle/12.2.1/tmp/prod/` selected earlier, create `rs_daemons.cfg` file.

5. Save the changes to the Persistence Store.

> **✎ Note:**
>
> On saving the changes, an error occurs click **Ignore** and complete the process.
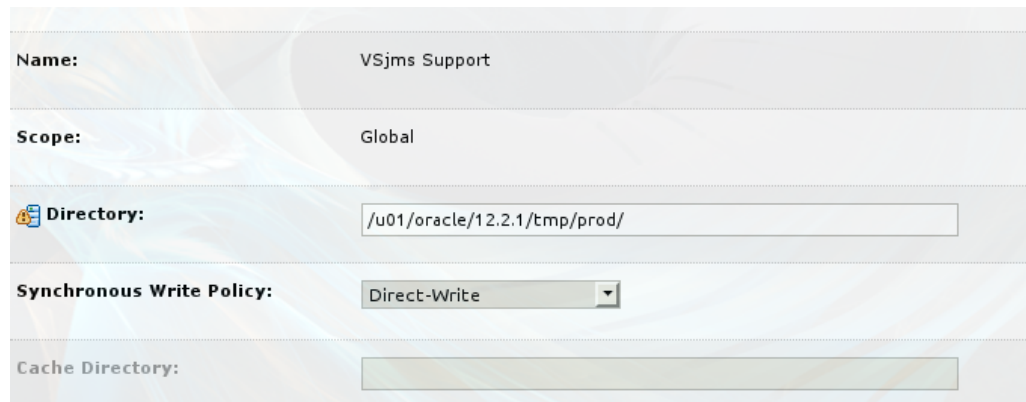
6. Edit the `rs_daemons.cfg` file and enter the values. The following example shows the values that needs to be set for the servers:

#ipaddress	portno	shmkey	memlmt
111.222.2.333	14545	4545	1G
111.666.2.111	14546	4545	1G

7. Save the file `rs_daemons.cfg` file.

For more information on `rs_daemons.cfg` file, see Messaging Services.

Figure 9-1   Persistent Store Configure for Oracle WebCenter Sites: Visitor Services

Configuring JMS Servers

To update the JMS Server :

1. In configuration wizard you will see that it contains VSjms Server already created.

2. On the Persistent Stores, locate **WL left nav services**.

3. Select **JMS Servers>VSjms Server**.

4. In the Setting for VSJMS Server, select **Targets** tab.

5. Select Visitor Services Cluster from the drop-down list. Figure 9-2 shows the example for wcvisitor

6. Click **Save**.

> ✎ **Note:**
>
> On saving the changes, an error occurs click **Ignore** and continue and complete the process.

Figure 9-2   JMS Servers Configuration for Oracle WebCenter Sites: Visitor Services
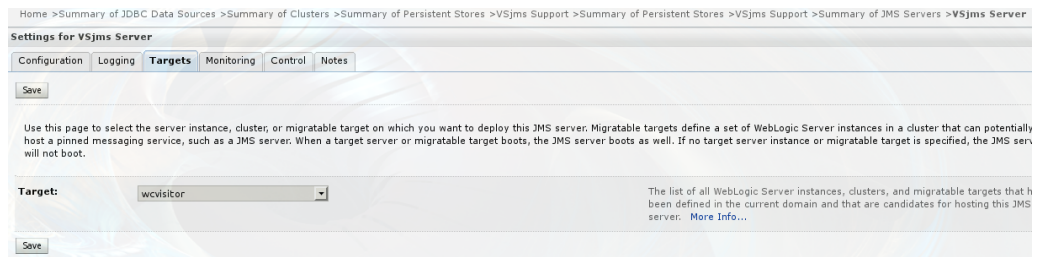
Configuring JMS Module

To update the JMS Module .

1. The configuration wizard you will see that it contains VSjms Module already created.

2. Locate **WL left nav services**.

3. Select **JMS Modules>VSjms Module>VSjms Server**.

4. Click **Targets** tab and select the entire cluster.

5. Click **Save**.

> ✎ **Note:**
>
> On saving the changes, an error occurs click **Ignore** and continue and complete the process.

6. Click **Subdeployments** tab.

7. View the subdelpoyment, `Vsjms Module Sub`.

8. Here it should points to **Vsjms Server**. Do not modify when it points to **Vsjms Server**.

9. Click **Configuration** tab.

10. Select **wcsitesVisitorsEnrichQueue** and **wcsitesVisitorsUpdateQueue**.

11. Click **Delete**, as these are standalone queues and does not work for the cluster.

12. Click **New** .

13. Select **Distributed Queue** and click **Next**.

14. Under **Name** filed enter `wcsitesVisitorsEnrichQueue` and under **JNDI Name** enter `jms/wcsitesVisitorsEnrichQueue`.

15. Click **Save**.

16. Return to the **JMS Module Configuration** tab.

17. Click **New**.

18. Select **Distributed Queue** and click **Next**.

19. In the **Name** filed enter `wcsitesVisitorsUpdateQueue`.

20. In the **JNDI Name** enter `jms/wcsitesVisitorsUpdateQueue`.

21. Click **Save**.

22. The configuration page should now appear similar to Figure 9-3.

> **Note:**
>
> Ensure that after completing this step you should not get any errors displayed in red on the top bar.

Figure 9-3   Settings for VSjms Server for Oracle WebCenter Sites: Visitor Services

10
Configuring Remote Satellite Server

After you set up a WebLogic domain for Oracle WebCenter Sites: Satellite Server, you can run the Satellite Server Configurator to complete the configuration process.

`Completing Prerequisites for Configuring Satellite Server`
Before configuring Satellite Server, ensure that the following prerequisites have been done:

- Create the necessary database schemas using the Repository Creation Utility, as Creating the Database Schemas describes.

- Create a WebLogic domain for Satellite Server using the WebLogic Configuration Wizard and the `Oracle WebCenter Sites – Satellite Server 12.2.1.3.0 [wcsites]` template, as Configuring the WebCenter Sites Domain describes.

- If you plan to manually set the value of the `ss.password` property in *DOMAIN_HOME*/`wcsites/satelliteserver/config/wcs_properties.json` in clear text, you must set the value of the `hidden.encrypted` property to `false`. (If you are using using encrypted passwords, set `hidden.encrypted` to `true`.)

Using the Import/Export Uitlity to Configure Satellite Server

You can use the Import/Export utility to import and export the Satellite Server configuration store in a property file format. The exported property file has all the settings for the product in a `key=value` format.

To run the utility, see Using the Import/Export Utility to Manage Satellite Server Properties in *Property Files Reference for Oracle WebCenter Sites*

You can start the Satellite Server Configurator from the command line and run it in either interactive mode or silent mode to configure Satellite Server. The Configurator provides configuration instructions.

Running the Satellite Server Configurator in Interactive Mode

To run the Configurator in interactive mode, do these steps:

1. Using the command line, navigate to the *ORACLE_HOME*/`wcsites/satelliteserver/` directory.

2. Run the Satellite Server Configurator: `java -jar satellite-configurator.jar -configPath` *DOMAIN_HOME*/`wcsites/satelliteserver/config`

3. Follow the instructions displayed in the Configurator.

4. Start the Satellite Server Managed Server.

Running the Satellite Server Configurator in Silent Mode

To run the Configurator in silent mode:

1. Edit the *DOMAIN_HOME*/`wcsites/satelliteserver/config/wcs_satelliteserver_properties_bootstrap.ini` file and complete the instructions.

2. Using the command line, navigate to the `ORACLE_HOME`/wcsites/
   `satelliteserver/` directory.

3. Run the Satellite Server Configurator: `java -jar satellite-configurator.jar`
   `-silent DOMAIN_HOME/wcsites/satelliteserver/config`.

4. Start the Satellite Server Managed Server.

If you get `nullpointer` exceptions when you start the Managed Server, confirm that
the following steps have been completed then run the Satellite Server Configurator
again.

1. Update the `cs-cache.xml`, `ss-cache.xml`, `linked-cache.xml`, and `cas-cache.xml`
   files, as Completing Prerequisites for Configuring WebCenter Sites describes.

2. Complete initial configuration in the WebCenter Sites configuration setup URL:
   `http://sites-host:sites-port/sites/sitesconfigsetup`

For more information on configuring Satellite Server, see Managing Caching in
Developing with Oracle WebCenter Sites.

> **Note:**
>
> Because changes you make to a WAR file are not retained during
> redeployment, you must copy WAR file changes over after each
> redeployment of the web applications. Oracle recommends deploying static
> artifacts such as images and stylesheet files onto the web server.

11

Switching to External Authentication

For maximum security in production environments, Oracle recommends integrating Oracle WebCenter Sites with Oracle Access Management, for an advanced identity management solution and a seamless single sign-on user experience. You also have the option of integrating WebCenter Sites with an external LDAP authentication provider directory.

The following topics describe how to configure WebCenter Sites for authentication against either external identity management solution:

- Switching to Authentication Against an LDAP Directory
  This topic describes how to switch WebCenter Sites to authentication against an external LDAP authentication provider directory. This is a recommended solution for production environments if integration with Oracle Access Management is not viable.

- Switching to Authentication Against Oracle Access Manager
  You can configureWebCenter Sites for authentication against Oracle Access Manager. This solution is recommended for production environments.

- Switching to Authentication OAM Using Detached Credential Collector
  This topic will show the steps to configure the two webgates and two OHS. You can configure Site Capture, Satellite Server, and Visitor Services to OAM in the similar using the steps in this topic.

Switching to Authentication Against an LDAP Directory

This topic describes how to switch WebCenter Sites to authentication against an external LDAP authentication provider directory. This is a recommended solution for production environments if integration with Oracle Access Management is not viable.

Before you change your authentication provider, install and configure WebCenter Sites.

To switch WebCenter Sites to authentication against an external LDAP directory:

1. (Optional) Modify `ldap.caseAware` property value to `true`, if the LDAP server you are using is case sensitive.

   By default the value of `ldap.caseAware` is set to `false`. Sign in will fail if you are using a case-sensitive LDAP server and this property is set to `false`. To modify the `ldap.caseAware` value to `True` follow the steps:

   - Sign in to the WebCenter Sites Admin interface and navigate to `Admin tree` tab>`System Tools`>`Property Management` option.

   - Search for `ldap` and change the value from `False` to `True`.

   - Restart the Managed server.

> **Note:**
>
> During the integration of Sites with LDAP, if the users data in LDAP is separated by a comma the data does not get fetched. for example: `test,user`. To retrieve the data, you need to change the syntax in the `dir.ini` file located at `..sites/install` directory from `"syntax.escape=\\` to `syntax.escape=\#"`.

2. Access the LDAP Configurator at `http://`*`sites-host`*`:`*`sites-port`*`/`*`sites-context`*`/ldapconfig`, follow the instructions on the screen, and enter the values for your environment.

3. For LDAP rollback, restart the WebCenter Sites Managed Server, and go to the same LDAP Configurator URL.

   Now there is only manual LDAP integration. Nothing is written to your LDAP Server, only an LDIF file is created under the *`DOMAIN_HOME`*`/wcsites/wcsites/config/ldap` folder (This is the default install location of WebCenter Sites application. All customizations and path modifications should be made after successful LDAP integration). The `peopleparent`, `groupparent`, `username`, and other fields are not prepopulated, as in the previous release.

4. (Optional) Modify the `LDIF` file located in *`NEW_DOMAIN_HOME`*`/wcsites/wcsites/config/` with values appropriate for your environment.

   Because the fields are not prepopulated, follow this example for `ORACLEDIR` :

   ```
   ldap server type -- ORACLEDIR
   ldap DSN -- dc=oracle,dc=com
   ldap host -- localhost
   ldap port -- 389
   ldap username -- cn=orcladmin
   ldap password -- password
   ldap peopleParent -- cn=Users,dc=oracle,dc=com
   ldap groupparent -- cn=Groups,dc=oracle,dc=com
   ```

5. If you choose Oracle Virtual Directory as your LDAP authentication provider, WebCenter Sites generates an `LDIF` file, which you can import to your Oracle Internet Directory server and then create an adaptar in Oracle Virtual Directory to connect to the Oracle Internet Directory server.

   You cannot import an LDIF file directly to an Oracle Virtual Directory LDAP server because it does not have a storage of its own.

6. Import the `LDIF` file into the external LDAP authentication provider.

7. Restart the WebLogic Managed Server running this WebCenter Sites instance.

Switching to Authentication Against Oracle Access Manager

You can configureWebCenter Sites for authentication against Oracle Access Manager. This solution is recommended for production environments.

It is assumed that customer already has OAM Server running. This OAM integration would require configuration in the OAM Server using `oamconsole` and some configuration changes in the Sites.

WebCenter Sites integration is supported for Oracle Access Manager 11.1.2.2.0 and 11.1.2.3.0.

To switchWebCenter Sites to authentication against Oracle Access Manager:

1. Sign in to Oracle Access Manager Server through `oamconsole`, for example: `http://<oam_host:oam_port>/<oam console>/` and configure a WebGate.

2. Deploy the `oamlogin.war` and `oamtoken.war` application files located under `NEW_ORACLE_HOME/wcsites/webcentersites/sites-home` on the WebLogic domain containing the targetWebCenter Sites instance.

3. Create the `wemsites_settings.properties` property file under `DOMAIN_HOME/wcsites/wcsites/config/`.

4. Enter the values in the `wemsites_settings.properties` file as follows:

Elements	Properties
`oamredirect`	`http://oam_server_host:oam_port/oam/server/auth_cred_submit`
`oamlogout`	`oamlogout=http://oam_server_host:oam_port/oam/server/logout`
`forgotpassword`	`helpdesk-email-address`

5. Set the following properties in `NEW_DOMAIN_HOME/wcsites/wcsites/config/SSOConfig.xml`. See Step 12 of Integration Steps.

Elements	Properties
`serviceUrl`	`http://{ohs_server_host}:{ohs_port}/{sites_context_root}/REST`
`ticketUrl`	`http://{oamtoken_server_host}:{oamtoken_port}/oamtoken`
`signoutURL`	`http://{oam_server_host}:{oam_port}/oam/server/logout?end_url={end_url}`
	Use this URL when invokingWebCenter Sites logout. It includes the encoded URL where the browser will return after all logout processing has been completed by Oracle Access Manager.
`end_url`	For test (staging) and production (delivery) environments: `http%3A%2F%2F{ohs_server_host}%3A{ohs_port}%2F{sites_context_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome`
`dbUsername`	Name of theWebCenter Sites general Administrator user account.
`dbPassword`	Password for the WebCenter Sites general Administrator user account.

> **Note:**
>
> The `ohs_server` host and `ohs_port` can be WebLogic host and port or any other HTTP server host and port depending on your configuration. For more information on OHS configuration, see Step 2 to Step 9 of Integration Steps. Add the below example for configuration in `OAM OHS`, `mod_wl_ohs.conf` file.
>
> ```
> <IfModule weblogic_module>
>     <Location /oamlogin>
>      SetHandler weblogic-handler
>         WebLogicHost SITES_HOST
> WebLogicPort SITES_PORT
> </Location>
> </IfModule>
>   <IfModule weblogic_module>
>  <Location /sites>
>         SetHandler weblogic-handler
>         WebLogicHost SITES_HOST
>         WebLogicPort SITES_PORT
>  </Location>
>  </IfModule>
> ```

6. Copy the `obAccsessClient.xml` and `cwallet.sso` files from your Oracle Access Manager instance into the *NEW_DOMAIN_HOME/wcsites/wcsites/config/oblix/lib/* directory on the targetWebCenter Sites instance.

> **Note:**
>
> These files are auto-generated after the WebGate is configured.

7. Edit the `oamtoken.xml` file in the `sites-config` directory by setting the compatibility mode and `oblix` path. The compatibility mode should be set to `11g` and the `oblix` path to the `sites-config` folder under which you have the `oblix/lib` folder.

8. In the Oracle Access Manager configuration for WebCenter Sites, update the protected, public, and excluded resources as follows:

Figure 11-1   List of Protected, Public, and Excluded Resources for WebCenter Sites

See Updating the Protected, Public, and Excluded Resources for an Enterprise Deployment.

9. To integrate the OAMSDK Client with WebLogic Server as the `oamtoken.war` application, edit the `jps-config.xml` file for the WebCenter Sites domain. By default, the WebLogic domain runs with this file, which is part of the WebLogic Server 12 *c* startup script:

```
-Doracle.security.jps.config=NEW_ORACLE_HOME/user_projects/domains/
DOMAIN_NAME/config/fmwconfig/jps-config.xml
```

a. Add a service instance, as the following example shows, next to existing service instances in the existing `jsp-config.xml` file:

```
<serviceInstance name="credstore.oamtoken" provider="credstoressp"
location="./oamtoken">

<description>File Based Credential Store Service Instance</
description>

<property name="location" value="./oamtoken"/>

</serviceInstance>
```

`location` is the path to the directory that contains the `cwallet.sso` file. The preceding example sets this path with reference to the current `jsp-`

config.xml file. Make sure the omtoken folder is created with respect to the current directory and the cwallet.sso file is placed there. The location value can also be an absolute path to where the cwallet.sso file is placed

b. Add `<serviceInstanceRef ref="credstore.oamtoken"/>` under `<jpsContext name="default">`.

c. Add following `<jpsContext>` element under `<jpsContexts default="default">`:

`<jpsContext name="OAMASDK">`

`<serviceInstanceRef ref="credstore.oamtoken"/>`

`</jpsContext>`

10. Add permissions so that code in oamtoken.war can be used.

The WebGate instance created in Oracle Access Manager is accessed by the client. You need to add the credential to the WebCenter Sites domain so that the security restriction can be taken care of.

a. Launch the WebLogic Scripting Tool with the wlst.sh script:

`cd NEW_ORACLE_HOME/oracle_common/common/bin/./wlst.sh`

b. Connect to the Administration Server for the WebCenter Sites domain:

`connect('user-name','password','sites-host:admin-port')`

c. Grant the permissions:

```
grantPermission(codeBaseURL="file:/scratch/idc/newoam/rend/
Oracle_Home/user_projects/domains/renddomain/servers/
wcsites_server1/tmp/_WL_user/oamtoken/-",
permClass="oracle.security.jps.service.credstore.CredentialAccessPe
rmission",permTarget="context=SYSTEM,mapName=OAMAgent,keyName=*",pe
rmActions="*")
```

The preceding path is basically the path where WebLogic Server has deployed the oamtoken.war application.

d. Restart the target WebCenter Sites Managed Server.

11. (Optional) If trust betweenWebCenter Sites and Oracle Access Manager has not been established, modify the configuration of theWebCenter Sites web tier as follows:

a. Sign in to the Oracle Access Manager Console.

b. In the WebGate authorization policy (under the protected resource policy), go to the **Responses** tab.

c. Enable (select) the **Identity Assertion** check box.

d. Click **Apply** to save your changes.

12. (Optional) If WebCenter Sites is deployed on a cluster is using OAM Integration. Following steps are required to be replicated on oamticketcache cache.

a. In the config directory, we have cas-cache.xml where oamticketcache is configured by default.

b. Uncomment the commented section in the cache named `oamticketcache` the section appear as:

```
<cacheEventListenerFactory
class="net.sf.ehcache.distribution.RMICacheReplicatorFactory"
properties="replicateAsynchronously=true, replicatePuts=true,
replicateUpdates=true,
    replicateUpdatesViaCopy=false, replicateRemovals=true"/>
<bootstrapCacheLoaderFactory
class="net.sf.ehcache.distribution.RMIBootstrapCacheLoaderFactory
"
        properties="bootstrapAsynchronously=false,
            maximumChunkSizeBytes=5000000"
        propertySeparator="," />
```

c. Change the `cacheManagerPeerProviderFactory` as follows, make sure port is unique.

```
<cacheManagerPeerProviderFactory
class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFac
tory"
    properties="peerDiscovery=automatic,
multicastGroupAddress=230.0.0.8,
        multicastGroupPort=40002, timeToLive=1" />
```

d. The port should be different for `cacheManagerPeerProviderFactory` and `cacheManagerPeerListenerFactory` as specified in the earlier steps.

e. All the cluster nodes should have same port for both the properties.

13. For working on the `SSOConfig.xml` file, follow the steps:

a. Modify the `SSOConfig.xml` file of theWebCenter Sites deployment. This file controls the loaded authentication classes and the properties that are required by those classes.

b. Shutdown the Sites server.

c. Backup the `SSOConfig.xml` file located in the `WEB-INF/classes` directory of the deployed WebCenter Sites application.

For example: `/u01/software/Apps/OraMiddleware/user_projects/domains/ OAMSitesDomain/wcsites/wcsites/config/SSOConfig.xml`.

d. Modify `SSOConfig.xml` as follows:

> ✎ **Note:**
>
> Further steps explains on setting properties for the following:
> `serviceUrl`, `ticketUrl`, `signoutURL`, `dbUsername`, and `dbPassword`.
> See Step 5.

e. The `signoutUrl` property specifies the URL to be used when invoking WebCenter Sites logout. It includes the encoded URL where the browser will return after all logout processing has been completed by OAM.

f. For Sites management, use the following
value for end_url: *http%3A%2F%2F{ohs_server_host}%3A{ohs_port}%2F{sites_context_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome*

g. For Sites delivery, use the following value
for end_url: *http%3A%2F%2F{ohs_server_host}%3A{ohs_port}%2F{sites_context_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome*

For the `dbUsername` and `dbPassword` properties, you can enter the credentials of the WebCenter Sites general administrator, which by default is fwadmin/xceladmin. The values for these properties will be encrypted on startup of the WebCenter Sites application.

> **✎ Note:**
>
> In the code example below, you will set the following properties:
> `csServerUrl`, `serviceUrl`, **ticketUrl**, `signoutURL`, `dbUsername`,
> `dbPassword`. See Step 5.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--

    Copyright (c) 2010 FatWire Corporation. All Rights
Reserved.
    Title, ownership rights, and intellectual property
rights in and
    to this software remain with FatWire Corporation.
This  software
    is protected by international copyright laws and
treaties, and
    may be protected by other law.  Violation of
copyright laws may
    result in civil liability and criminal penalties.

-->

<beans xmlns="http://www.springframework.org/schema/
beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:jdbc="http://www.springframework.org/
schema/jdbc"
    xmlns:p="http://www.springframework.org/schema/p"
xmlns:context="http://www.springframework.org/schema/
context"
    xsi:schemaLocation="http://www.springframework.org/
schema/beans http://www.springframework.org/schema/beans/
spring-beans-3.1.xsd
    http://www.springframework.org/schema/jdbc http://
www.springframework.org/schema/jdbc/spring-jdbc-3.1.xsd
    http://www.springframework.org/schema/context http://
www.springframework.org/schema/context/spring-
context-3.1.xsd">

    <bean id="propertyConfigurer"
class="org.springframework.beans.factory.config.PropertyP
laceholderConfigurer" />
    <!-- Root Context: defines shared resources visible
to all other web components -->

    <jdbc:initialize-database data-
source="dataSource"    enabled="true" ignore-
failures="ALL">
        <!-- For installer the first jdbc:script will
opened. Installer will configure it automatically -->
        <jdbc:script
location="classpath:crawler_oracle_db.sql" />
        <!--jdbc:script
```

```xml
location="classpath:crawler_hsql_db.sql" /-->
        <!--jdbc:script
location="classpath:crawler_sql_server_db.sql" /-->
        <!--jdbc:script
location="classpath:crawler_oracle_db.sql" /-->
        <!--jdbc:script
location="classpath:crawler_db2_db.sql" /-->
    </jdbc:initialize-database>

    <!-- Section# 1 Installer will consume below
configuration to configure a datasource name created on
the appservers -->
    <bean id="dataSource"
class="org.springframework.jndi.JndiObjectFactoryBean">
        <property name="jndiName" value="wcsitesDS"/>
    </bean>

    <!-- Single Sign On provider -->
    <bean id="ssoprovider"
class="com.fatwire.wem.sso.oam.OAMProvider">
        <property name="config" ref="ssoconfig" />
    </bean>
    <!--It is invoked by the OAM filter to resolve an
OAM authenticated user against a remote Site CS
instance.-->
    <bean id="oamIdentity"
class="com.fatwire.auth.identity.RemoteUsernameResolver"
>
        <property name="csServerUrl" value="http://
{ohs_server_host}:{ohs_port}/{sites_context_root}/custom/
customCsResolver.jsp"/>
    </bean>

    <!-- Single Sign On filter -->
    <bean id="ssofilter"
class="com.fatwire.wem.sso.oam.filter.OAMFilter">
        <property name="config" ref="ssoconfig" />
        <property name="provider" ref="ssoprovider" />
        <property name="identityResolver"
ref="oamIdentity" />

        <!-- Set "trustConfigured" to "true" in case of
trust relationship configured between WebGate and WLS.
        It will turn off check for OAM_ASSERTION header.
-->
        <property name="trustConfigured" value="false" />
    </bean>


    <!-- Single Sign On listener -->
    <bean id="ssolistener"
class="com.fatwire.wem.sso.oam.listener.OAMListener">
    </bean>

    <!-- Single Sign On configuration -->
```

```
    <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">
        <!-- URL prefix for REST service endpoint -->
        <property name="serviceUrl" value="http://
{ohs_server_host}:{ohs_port}/{sites_context_root}/
REST" />

        <!-- URL prefix for Token Service servlet -->
        <property name="ticketUrl" value="http://
{oamtoken_server_host}:{oamtoken_port}/oamtoken" />

        <!-- URL to be called when WEM logout is
required. -->
        <property name="signoutUrl" value="http://
{oam_server_host}:{oam_port}/oam/server/logout?
end_url=http%3A%2F%2F{ohs_server_host}%3A{ohs_port}
%2F{sites_context_root}
%2Fwem%2Ffatwire%2Fwem%2FWelcome"/>

        <!-- Do not proxy tickets, tt's the last server
in thecall chain -->
        <property name="proxyTickets" value="false" />

        <!-- Database Credentials needed by user lookup
inOAMFilter -->
        <property name="dbUsername" value="fwadmin" />
        <property name="dbPassword" value="xceladmin"/>

        <!-- Your application protected resources
(relative to applicationUrl) -->
        <property name="protectedMappingIncludes">
            <list>
                <value>/__admin</value>
                <value>/__admin/**</value>
            </list>
        </property>

        <!-- Your application protected resources
excludes (relative to applicationUrl) -->
        <property name="protectedMappingExcludes">
            <list>
                <value>/__admin/layout</value>
            </list>
        </property>
        <property name="applicationProxyCallbackPath"
value="/sso/proxycallback" />
        <property name="gateway" value="false" />
    </bean>

    <context:component-scan base-
package="com.fatwire.crawler.remote.dao" />
    <context:component-scan base-
package="com.fatwire.crawler.remote.support" />
    <context:component-scan base-
package="com.fatwire.crawler.remote.di" />
```

```
      <context:component-scan base-
    package="com.fatwire.crawler.remote.resources.support" />

    </beans>
```

After you authenticate OAM, you need to perform the following integrations:

- Integrating SiteCapture with OAM
  This topics covers steps to integrate SiteCapture with OAM.

- Integrating OAM with Oracle WebCenter Sites: Satellite Server
  This topics covers steps to integrate OAM with Oracle WebCenter Sites: Satellite Server.

- Integrating OAM with Visitor Services
  This topic covers steps to integrate OAM with Visitor Services.

Integrating SiteCapture with OAM

This topics covers steps to integrate SiteCapture with OAM.

Oracle Access Manager integration for SiteCapture you need to follow the steps:

1. Integrate Oracle WebCenter Sites with Oracle Access Manager. For more information see, Integrating OAM with Oracle WebCenter Sites.

2. Additional configuration required for Oracle Access Manager for SiteCapture.

    a. Create additional resource definitions (see table below) for the WebCenter Sites application domain.

Resource URL	Protection level	Authentication	Authorization
`/<sites-context>/REST/roles`	Unprotected	Public	All Allowed
`/<sites-context>/custom/customCsResolver.jsp`	Unprotected	Public	All Allowed
`/resources/.../*`	Excluded	NA	NA
`/__admin/.../*`	Protected	Protected	Protected

    b. Configure the Protected Resource Policy as follows:

    a. Click **Application Domains** and click the Open icon.

    b. Click **Search** and select **WCSitesWebGate**.

    c. Click the **Authentication Policies** tab and select **Authentication Policies** . For Authentication Scheme, select **LDAPWemScheme**, the authentication scheme previously created.

    d. Click **Responses** tab.

    e. Select the **Identity Assertion** checkbox.

    f. When an Authentication policy is satisfied, it can create responses. The responses are required by the WebCenter Sites HTTP filter to recognize LDAP attributes and provide information about the authenticated user. In the following steps, you will create these responses.

    g. Click the **Add (+)** icon. and enter the following:

    a. For **Name**: Enter **FATGATE_CSTIMEOUT**

    b. For **Type**: Select **Header**

    c. For **Value**: Enter **30**

3. SiteCapture Application Installation. During installation process of SiteCapture use parameters that are mentioned below:

Property Description	Property	Value
Content server host name or IP	fw.cs.hostname	{ohs_host}
Content server app server port	fw.cs.port	{ohs_port}
Content server context	fw.cs.context	{sites_context_root}
Content server protocol (http or https)	fw.cs.protocol	{sites.protocol}
Content Server user name having RESTADMIN role	fw.cs.username	{username}
Content server user password	fw.cs.password	{password}
SiteCapture server hostname or IP	fw.sc.hostname	{sc_host}
SiteCapture app server port	fw.sc.port	{sc_port}
SiteCapture protocol (http or https)	fw.sc.protocol	{sc.protocol}
CAS server hostname	fw.cas.host	{ohs_host} in installer. Or Empty in sitecapture.properties
CAS server port	fw.cas.port	{ohs_port} in installer. Or Empty in sitecapture.properties
CAS server context	fw.cas.context	cas in installer. Or Empty in sitecapture.properties

4. Adjust the `root-context.xml` file in SiteCapture Application. SiteCapture shipped with two files:

    a. `root-context.xml`

    Backup `root-context.xml` file and rename to `root-context.xml.bak` file.

    b. `oam_root-context.xml`

    Rename `oam_root-context.xml` file to `root-context.xml` file.

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
```

ORACLE

```
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:jdbc="http://www.springframework.org/schema/jdbc"
    xmlns:p="http://www.springframework.org/schema/p"
xmlns:context="http://www.springframework.org/schema/context"
    xsi:schemaLocation="http://www.springframework.org/schema/
beans http://www.springframework.org/schema/beans/spring-
beans-3.1.xsd
    http://www.springframework.org/schema/jdbc http://
www.springframework.org/schema/jdbc/spring-jdbc-3.1.xsd
    http://www.springframework.org/schema/context http://
www.springframework.org/schema/context/spring-context-3.1.xsd">

    <bean id="propertyConfigurer"
class="org.springframework.beans.factory.config.PropertyPlacehold
erConfigurer" />
    <!-- Root Context: defines shared resources visible to all
other web components -->

    <jdbc:initialize-database data-source="dataSource"
enabled="true" ignore-failures="ALL">
        <!-- For installer the first jdbc:script will opened.
Installer will configure it automatically -->
        <jdbc:script
location="classpath:crawler_oracle_db.sql" />
        <!--jdbc:script
location="classpath:crawler_hsql_db.sql" /-->
        <!--jdbc:script
location="classpath:crawler_sql_server_db.sql" /-->
        <!--jdbc:script
location="classpath:crawler_oracle_db.sql" /-->
        <!--jdbc:script
location="classpath:crawler_db2_db.sql" /-->
    </jdbc:initialize-database>

    <!-- Section# 1 Installer will consume below configuration
to configure a datasource name created on the appservers -->
    <bean id="dataSource"
class="org.springframework.jndi.JndiObjectFactoryBean">
        <property name="jndiName" value="wcsitesDS"/>
    </bean>

    <!-- Single Sign On provider -->
    <bean id="ssoprovider"
class="com.fatwire.wem.sso.oam.OAMProvider">
        <property name="config" ref="ssoconfig" />
    </bean>
    <!--It is invoked by the OAM filter to resolve an OAM
authenticated user against a remote Site CS instance.-->
    <bean id="oamIdentity"
class="com.fatwire.auth.identity.RemoteUsernameResolver" >
        <property name="csServerUrl" value="http://
{ohs_server_host}:{ohs_port}/{sites_context_root}/custom/
customCsResolver.jsp"/>
    </bean>
```

```
    <!-- Single Sign On filter -->
    <bean id="ssofilter"
class="com.fatwire.wem.sso.oam.filter.OAMFilter">
        <property name="config" ref="ssoconfig" />
        <property name="provider" ref="ssoprovider" />
        <property name="identityResolver" ref="oamIdentity" />

        <!-- Set "trustConfigured" to "true" in case of trust
relationship configured between WebGate and WLS.
        It will turn off check for OAM_ASSERTION header. -->
        <property name="trustConfigured" value="false" />
    </bean>


    <!-- Single Sign On listener -->
    <bean id="ssolistener"
class="com.fatwire.wem.sso.oam.listener.OAMListener">
    </bean>

    <!-- Single Sign On configuration -->
    <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">
        <!-- URL prefix for REST service endpoint -->
        <property name="serviceUrl" value="http://
{ohs_server_host}:{ohs_port}/{sites_context_root}/REST" />

        <!-- URL prefix for Token Service servlet -->
        <property name="ticketUrl" value="http://
{oamtoken_server_host}:{oamtoken_port}/oamtoken" />

        <!-- URL to be called when WEM logout is required. -->
        <property name="signoutUrl" value="http://
{oam_server_host}:{oam_port}/oam/server/logout?
end_url=http%3A%2F%2F{ohs_server_host}%3A{ohs_port}
%2F{sites_context_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome"/>

        <!-- Do not proxy tickets, tt's the last server in
thecall chain -->
        <property name="proxyTickets" value="false" />

        <!-- Database Credentials needed by user lookup
inOAMFilter -->
        <property name="dbUsername" value="fwadmin" />
        <property name="dbPassword" value="xceladmin"/>

        <!-- Your application protected resources (relative to
applicationUrl) -->
        <property name="protectedMappingIncludes">
            <list>
                <value>/__admin</value>
                <value>/__admin/**</value>
            </list>
        </property>

        <!-- Your application protected resources excludes
```

```
(relative to applicationUrl) -->
        <property name="protectedMappingExcludes">
            <list>
                <value>/__admin/layout</value>
            </list>
        </property>
        <property name="applicationProxyCallbackPath"
value="/sso/proxycallback" />
        <property name="gateway" value="false" />
    </bean>

    <context:component-scan base-
package="com.fatwire.crawler.remote.dao" />
    <context:component-scan base-
package="com.fatwire.crawler.remote.support" />
    <context:component-scan base-
package="com.fatwire.crawler.remote.di" />
    <context:component-scan base-
package="com.fatwire.crawler.remote.resources.support" />

</beans>
```

> **Note:**
>
> To update `mod_wl_ohs.conf` file the following code has to be included:

```
<IfModule weblogic_module>
<Location /__admin>
        SetHandler weblogic-handler
        WebLogicHost SITECAPTURE_HOST
    WebLogicPort SITECAPTURE_HOST
</Location>
</IfModule>
```

Integrating OAM with Oracle WebCenter Sites: Satellite Server

This topics covers steps to integrate OAM with Oracle WebCenter Sites: Satellite Server.

Configuring a Satellite Server for Oracle Access Manager integration is a simpler procedure than for WebCenter Sites. For more information on Integrating OAM with WebCenter Sites using Satellite Server, see Integrating OAM with Oracle WebCenter Sites: Satellite Server

> **Note:**
>
> The code example below gives the RSS configuration in `OAM OHS`, and `mod_wl_ohs.conf` file.
>
> ```
> <IfModule weblogic_module>
>  <Location /ss>
>         SetHandler weblogic-handler
>         WebLogicHost SATELLITESERVER_HOST
>      WebLogicPort SATELLITESERVER_HOST
>  </Location>
>  </IfModule>
> ```

Integrating OAM with Visitor Services

This topic covers steps to integrate OAM with Visitor Services.

Before performing steps described in this section, ensure that you have configured the OAMIdentityProvider provided with Visitor Services. The OAM identity provider enables Visitor Services to communicate with OAM. For more information on Integrating OAM with Visitor Services, see *Oracle Fusion Middleware Developing with Oracle WebCenter Sites*.

> **Note:**
>
> The code example below gives the Visitor configuration in `OAM OHS`, and `mod_wl_ohs.conf` file.
>
> ```
> <IfModule weblogic_module>
>      <Location /oamlogin>
>        SetHandler weblogic-handler
>         WebLogicHost SITES_HOST
>         WebLogicPort SITES_PORT
>    </Location>
>  </IfModule>
>  <IfModule weblogic_module>
>  <Location /visitors-webapp>
>    SetHandler weblogic-handler
>     WebLogicHost VISITORSERVICES_HOST
>     WebLogicPort VISITORSERVICES_HOST
>  </Location>
>  </IfModule>
> ```

Switching to Authentication OAM Using Detached Credential Collector

This topic will show the steps to configure the two webgates and two OHS. You can configure Site Capture, Satellite Server, and Visitor Services to OAM in the similar using the steps in this topic.

In the earlier topics, you can see that the credentials are collected directly by OAM server, which is exposed OAM Server's host and post, causing a security threat but with the introduction of DCC (Detached Credential Collector) webgate credentials you can now collect it at the webgate, which is transferred to OAM by webgate for further processing. DCC will not expose OAM server host and port, which mitigates the security threat. DCC can be configured using a single webgate and single OHS or two webgates (For exmaple, DCC webgate and Resource webgate) and two Oracle HTTP Servers (each OHS server will host the respective webgate files).

- Prerequisites
  This chapter lists the prerequisites required for configuring the Detached Credential Collector.

- DCC WebGate Configuration
  This topic describes hot to configure DCC Webgate.

- Resource WebGate Configuration
  This topics provides steps to configure the Resource Webgate.

- Sites OAM Integration
  This topic provides steps to configure the Sites OAM integration with DCC

Prerequisites

This chapter lists the prerequisites required for configuring the Detached Credential Collector.

The following are the prerequisites for configuring DCC:

1. WebCenter Sites 12.2.1.3.0 is installed with CAS and is in working condition.

2. OAM `11.1.2.3.0` is installed and OAM domain is configured along with two OHS configured for webgate. The list below are required softwares for this installation:

   - OAM `11.1.2.3.0`. For example : `ofm_iam_generic_11.1.2.3.0_disk*.zip`.

   - RCU `11.1.1.9.0`. For example : `ofm_rcu_linux_11.1.1.9.0_64_disk*.zip`.

   - Latest version of SOA suite.

   - WebTier `11.1.1.9.0`. For example : `ofm_webtier_linux_11.1.1.9.0_64_disk*.zip`

   - WebGate 11.1.2.3.0. For example : `ofm_webgates_generic_11.1.2.3.0_disk*.zip`

DCC WebGate Configuration

This topic describes hot to configure DCC Webgate.

To configure DCC Webgate, follow the steps:

1. Login to `oamconsole`. The **Launch Pad** of **Application Security** opens.

2. Click **Agents** >**Create Webgate**. The **Create Webgate** form opens.

3. In the **Create Webgate** form, enter the following values as given below:

   a. Version : `11g`

   b. Name : `DCC-11g-WG`. For example, enter Some arbitrary name.

   c. Host Identifier : `DCC-11g-WG`. For example, enter Some arbitrary name.

   d. Security : Select the option of your choice

   e. Auto Create Policies : Leave the default selected option.

4. Click **Apply**.

5. A new webgate named DCC-11g-WG is created with default values. In the webgate form, update the following fields:

   a. Logout URL : `/oamsso-bin/logout.pl`

   b. Logout Callback URL : `/oam_logout_success`

   c. Logout Redirect URL : `http://{OAM_host:OAM_port}/oam/server/logout`

   d. Logout Target URL : `end_url`

   e. Allow Credential Collector Operations : Leave the default selected option.

6. Click **Apply**.

7. Navigate to **Launch Pad** and click on **Access Manager**>**Host Identifiers**.

8. A Search form is displayed, click **Search**

9. Click **Host Identifier** `DCC-11g-WG` as created in Step 3c.

10. Add the Hostname and port by clicking on '+' in Host Name Variations area.

11. After entering all the details, click **Apply**.

> ✎ **Note:**
>
> These are the hostname and port of OHS to where DCC webgate files are copied to display the login challenge.

12. Navigate to **Launch Pad** and click **Authentication Schemes**.

13. A **Search** form is displayed, click **Create**.

14. Create a new Authentication theme that will be used by both the webgates as given in Step 15 a to g.

15. Click **Apply**. Using Weblogic's Embedded LDAP as LDAP authentication module where `fwadmin` user is added to myrealm using the weblogic's Admin console

   a. Name : DCCAuthnScheme11g. For example, enter Some arbitrary name.

    b. Authentication Level : 2

    c. Challenge Method : FORM

    d. Challenge Redirect URL : http://{OHS_Host_of_Resource_Webgate:OHS_Port}

    e. Authentication Module : LDAP

    f. Challenge URL : /oamsso-bin/login.pl

    g. Context Type : external

16. Navigate to **Launch Pad** and click **Application Domains**.

17. A Search form is displayed, click Search, which should display all the application domains available that are created by default when a webgate is created.

18. Click **Application Domain** (created in Step 3b), which should open the application domain with multiple tabs and Summary is opened by default.

    a. Click **Resources** tab, which will display search form along with **Create** button.

    b. Click **Create**, update the form as below:

> ✎ **Note:**
>
> Add other excluded URLS similar to below, with changing **Resource URL** with each **Create**.

    • Type : HTTP

    • Host Identifier : DCC-11g-WG (Name given in Step 3c)

    • Resource URL : /oamsso-bin/login.pl

    • Protection Level : excluded

    c. Click **Apply**.

    d. Click **Authentication Policies** tab and then click **Protected Resource Policy**. Update the form as below and click **Apply**.

        • Authentication Scheme : DCCAuthnScheme11g as created in Step 15.

19. Copy the DCC webgate files as given below created in WebLogic domain ($DOMAIN_HOME/output/DCC-11g-WG) to the OHS folder ($OHS_INSTANCE_HOME/config/OHS/$OHS_NAME /webgate/config) hosting these webgate files.

    • ObAccessClient.xml

    • cwallet.sso

20. Restart the OHS.

Resource WebGate Configuration

This topics provides steps to configure the Resource Webgate.

To configure the Resource WebGate, follow the steps:

1. Login to **oamconsole**, which should display **Launch Pad** of Application Security.

2. Click **Agents** > create **Webgate**, which should display **Create Webgate**form.

3. Input the values as below in the **Create Webgate** form.

    a. Version : 11g

    b. Name : Resource-11g-WG (Some arbitrary name)

    c. Host Identifier : Resource-11g-WG (Same as Name above or some arbitrary name)

    d. Security : Open (select the option of your choice)

    e. Auto Create Policies : Option Selected

4. Click **Apply**

5. A new webgate named Resoruce-11g-WG is created with default values. In the webgate form, update the following fields:

    a. Logout URL : /logout

    b. Logout Callback URL : /oam_logout_success

    c. Logout Redirect URL : http://{OAM_Host_of_DCC_Webgate:OAM_Port}/oamsso-bin/logout.pl

    d. Logout Target URL : end_url

6. Click **Apply**

7. Navigate to **Launch Pad** and click **Access Manager**> **Host Identifiers**, which should display a search form. Click **Search**.

8. Click **Host Identifier Resource-11g-WG** as created in Step 3c.

9. Add the hostname and port by clicking on '+' in Host Name Variations.

10. After all desired Host Name and Port are added then click **Apply**.

> **Note:**
>
> These are the hostname and port of OHS to where Resource webgate files are copied.

11. Navigate to **Launch Pad** and click **Application Domains**, which should display the Search form. Click **Search**, which should display all the application domains available that are created by default when a webgate is created.

12. Click **Application Domain** as created in Step 3b, which should open the application domain with multiple tabs and Summary is opened by default.

    a. Click **Resources** tab, which will display search form along with **Create** button. Click **Create** for each row in below table, update the create form as below and click **Apply**.

Table 11-1   Resource Identifiers

Type	Host Identifier	Resource URL	Protection Level	Authentication Policy	Authorization Policy
HTTP	Resource-11g-WG	/{sites-context}/**	Protected	Protected Resource Policy	Protected Resource Policy
HTTP	Resource-11g-WG	/{sites-context}/ContentServer/*	Protected	Protected Resource Policy	Protected Resource Policy
HTTP	Resource-11g-WG	/{sites-context}/Satellite/*	Protected	Protected Resource Policy	Protected Resource Policy
HTTP	Resource-11g-WG	/{sites-context}/faces/jspx/…/*	Protected	Protected Resource Policy	Protected Resource Policy
HTTP	Resource-11g-WG	/{sites-context}/wem/fatwire/…/*	Protected	Protected Resource Policy	Protected Resource Policy
HTTP	Resource-11g-WG	/{sites-context}/Xcelerate/LoginPage.html	Protected	Protected Resource Policy	Protected Resource Policy

b. Click **Authentication Policies** tab and then click **Protected Resource Policy**. Update the form as below and click **Apply**.

   i.   Authentication Scheme : DCCAuthnScheme11g (Created in Step 8)

   ii. Click **Responses** tab and then select **Identity Assertion**. Click **Add** and include the following responses:

   Table 11-2   Identity Assertion Elements

Type	Name	Value
Header	FATGATE_POLICY	Protected
Header	FATGATE_EMAIL	$user.attr.mail

c. Click **Authorization Policies** tab and then click **Protected Resource Policy**. Update the form as given in the table below.

   i.   Click **Responses** and then select **Identity Assertion**.

   Table 11-3   Identity Assertion Elements

Type	Name	Value
Header	FATGATE_POLICY	Protected
Header	FATGATE_EMAIL	$user.attr.mail

   ii. After adding the above responses, click **Add**

          iii. Click **Apply**.

13. Copy the Resource webgate files as given below that's created in WebLogic domain ($DOMAIN_HOME/output/Resource-11g-WG) to the OHS folder ($OHS_INSTANCE_HOME/config/OHS/$OHS_NAME /webgate/config hosting these webgate files.

    a. ObAccessClient.xml

    b. cwallet.sso

14. Restart OHS.

Sites OAM Integration

This topic provides steps to configure the Sites OAM integration with DCC

To configure the Sites OAM integration, follow the steps:

1. Deploy oamtoken web application to sites server.

> ✏ **Note:**
>
> Do not deploy oamlogin web application since it is not used.

2. Undeploy cas web application from the sites server.

3. Navigate to CS web application and open SSOConfig.xml in edit mode.

4. Add the following bean to the file and **Save** the file.

```
<!-- Single Sign On configuration -->
        <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">
            <!-- URL prefix for REST service endpoint -->

            <property name="serviceUrl" value="http://
{OHS_Host_of_Resource_Webgate:OHS_Port}/{sites-context}/REST" />
            <!-- URL prefix for Token Service servlet -->
            <property name="ticketUrl" value="http://
{Sites_Host:Sites_Port}/oamtoken" />
            <!-- URL to be called when WEM logout is required. -->
            <property name="signoutUrl"
value="http:// {OHS_Host_of_DCC_Webgate:OHS_Port }/oamsso-bin/
logout.pl?end_url=http%3A%2F%2F{OHS_Host_of_Resource_Webgate}
%3A{OHS_Port }%2F{sites-context}%2Fwem%2Ffatwire%2Fwem%2FWelcome" />
            <!-- Do not proxy tickets, tt's the last server in the
call chain -->
            <property name="proxyTickets" value="false" />
            <!-- Database Credentials needed by user lookup in
OAMFilter -->
            <property name="dbUsername" value="fwadmin" />
            <property name="dbPassword"
value="{password_for_above_user}" />
            <!-- Your application protected resources (relative to
applicationUrl) -->
            <property name="protectedMappingIncludes">
```

```
                <list>
                           <value>wem/fatwire/**value>wem/
fatwire/**>
                           <value>/faces/jspx/**value>/faces/
jspx/**>
<value>/ContentServer?[pagename=OpenMarket/Xcelerate/UIFramework/
LoginPage|OpenMarket/Xcelerate/UIFramework/ShowMainFrames|fatwire/
getAllUserGroups|fatwire/getAllSecurityConfigs|rest/asset,# </
value>
<value><Satellite?[pagename=fatwire/insitetemplating/request|
OpenMarket/Xcelerate/ControlPanel/Request|OpenMarket/Xcelerate/
ControlPanel/EditPanel|fatwire/wem/ui/Ping|fatwire/wem/sso/
validateMultiticket|OpenMarket/Xcelerate/UIFramework/
ShowPreviewFrames,#]
</value>
                           <value>Xcelerate/LoginPage.html</value>
```

5. Restart Sites server after the above changes.

6. Use a protected URL from the resource webgate to login to Sites. For example :
   `http://{OHS_Host_of_Resource_Webgate:OHS_Port}/{sites-context}/.`

> **Note:**
>
> Site Capture, Satellite Server and Visitor Services can be configured to the OAM in the same way.

12

Setting Up a CAS Cluster

You can set up a Central Authentication Server (CAS) cluster in the same WebLogic domain as Oracle WebCenter Sites, in a different WebLogic domain on the same machine, or for high availability, in a different WebLogic domain on a different machine.

The following topics describe how to set up a CAS cluster:

- Configuring the CAS Primary Cluster Node
  This topic describes how to set up the CAS application to function on a WebCenter Sites cluster both as a single instance and as a clustered application. If you are not clustering the CAS application, you can skip the steps required specifically for clustering CAS.

- Configuring the CAS Secondary Cluster Node(s)
  This topic describes how to set up one or more secondary CAS (Central Authentication Service) application cluster nodes.

Configuring the CAS Primary Cluster Node

This topic describes how to set up the CAS application to function on a WebCenter Sites cluster both as a single instance and as a clustered application. If you are not clustering the CAS application, you can skip the steps required specifically for clustering CAS.

Before completing the steps in this procedure, note the following items:

- An instance of WebCenter Sites with CAS, the primary cluster node, needs to be up and running.

- Never change the context root of the CAS application from its default value of `/cas`, even if the CAS application itself is relocated.

To set up the primary CAS cluster node:

1. Using the WebLogic Server Administration Console, create a new Managed Server for the primary CAS cluster node (for example, `cas_server1`).

   a. If CAS will be clustered, create and assign additional servers to the cluster as needed.

   b. Determine the load balancer's IP address and port becaause these values will be required to complete the setup.

   c. The initial configuration of CAS will be for only a single cluster member. Once WebCenter Sites is set up and running on a single server accessed through the load balancer, you can configure additional servers.

   d. (Optional) If you are deploying the CAS application on a WebLogic domain separate from the WebCenter Sites domain, do the following steps:

      i. Copy the contents of `DOMAIN_HOME/wcsites/bin/` to the same location in the CAS domain.

      ii. Copy the contents of `ORACLE_HOME`/`wcsites/wcsites_common/lib/` to the same location in the CAS domain.

2. Create a CAS `config` directory on the Managed Server you created in step 1. For example: `DOMAIN_HOME`/`wcsites/cas/config`.

    Subsequent steps will refer to this directory as `CAS_CONFIG_DIR`.

3. Move (do not copy) the following files and directories from `DOMAIN_HOME`/`wcsites/wcsites/config` on the Managed Server that is the primary WebCenter Sites cluster node to `CAS_CONFIG_DIR`:

- `cas.properties`

- `host.properties`

- `jbossTicketCacheReplicationConfig.xml`

- `customBeans.xml`

- `deployerConfigContext.xml`

- `fatwire_settings.properties`

- `fatwire_views.properties`

- `logging-config.xml`

- `cas-spring-configuration`

> **Note:**
>
> If the WebCenter Sites node you are copying from is part of a cluster, the `host.properties` and `jbossTicketCacheReplicationConfig.xml` files may be located under `DOMAIN_HOME`/`wcsites/wcsites/config`/`node-name` and need to be copied from there to `CAS_CONFIG_DIR`.

4. Set the `host.name` parameter value in `cas_config_dir`/`host.properties` to the host name or IP address of the CAS host machine.

5. Modify `CAS_CONFIG_DIR`/`jbossTicketCacheReplicationConfig.xml` as follows:

- (Optional) If you are using IPv6 addressing, set `mcast_addr` value to a valid IPv6 multicast address. This value must be the same for each node in the cluster. For example, [ff0x:0:0:0:0:0:0:301].

- Set `bind_addr` to the host name or IP address of the CAS host machine.

- (Optional) If you are clustering the CAS application, set `ip_ttl` to a value appropriate for your environment. Oracle recommends `1` as a starting point. For a list of suggested values, see Setting Up a WebCenter Sites Cluster.

6. Set the `server.name` parameter value in `CAS_CONFIG_DIR`/`cas.properties` to the URL of the CAS host machine.

> **Note:**
>
> If you are clustering the CAS application, use the IP address and port of the load balancer.

7. Update the class path on the CAS application's Managed Server to include the full path to the `CAS_CONFIG_DIR` directory.

8. Deploy the `cas.war` application file to the CAS application's Managed Server.

9. On the primary WebCenter Sites cluster node, modify the following properties in the `WCSITES_CONFIG_DIR`/`wcs_properties.json` file, as described in the following table.

Properties	Description
`wcsites.cas.host`	Host name or IP address of the CAS application's Managed Server. Used for external connections.
`wcsites.cas.port`	Port of the CAS application's Managed Server. Used for external connections.
`wcsites.cas.internal.url`	URL (in `hostname:port` format) of the CAS application's Managed Server. Used internally.

10. Restart the primary WebCenter Sites cluster node Managed Server and the CAS application's Managed Server.

11. Log in to the Admin interface on the primary WebCenter Sites cluster node to confirm the new configuration.

12. (Optional) If you are clustering the CAS application, complete the steps in Configuring the CAS Secondary Cluster Node(s).

Configuring the CAS Secondary Cluster Node(s)

This topic describes how to set up one or more secondary CAS (Central Authentication Service) application cluster nodes.

Before completing the following steps, you must have completed the steps in Configuring the CAS Primary Cluster Node.

To set up each secondary CAS cluster node:

1. Create a Managed Server for each secondary CAS cluster node and assign it to the WebLogic cluster containing the primary CAS cluster node.

2. Shut down all CAS Managed Servers.

3. Create a CAS `config` directory (`CAS_CONFIG_DIR`) on the new Managed Server; for example, `DOMAIN_HOME`/wcsites/cas/config.

4. Copy the contents of the `CAS_CONFIG_DIR` directory from the primary CAS Managed Server to the new Managed Server, the secondary cluster node.

5. Set the `host.name` parameter value in `CAS_CONFIG_DIR`/host.properties to the host name or IP address of this secondary cluster node.

6. Update the `CAS_CONFIG_DIR`/jbossTicketCacheReplicationConfig.xml file as follows:

   • Set `bind_addr` to the host name or IP address of this secondary cluster node.

   • (Optional) If you are clustering the CAS application, set `ip_ttl` to a value appropriate for your environment. Oracle recommends `1` as a starting point. See Setting Up a WebCenter Sites Cluster for a list of suggested values.

7. Start the load balancer, if it is not already running.

8. Start the new Managed Server.

9. Log in to the WebCenter Sites Admin interface to ensure that the new server is functional.

After you have configured and tested all the secondary CAS cluster nodes, start the primary and all secondary CAS cluster nodes, and, optionally, restart the load balancer. Then log in to the WebCenter Sites Admin interface to confirm that the CAS cluster has been successfully configured.

> **Note:**
>
> If the cluster members are not all colocated in a Weblogic domain on the same machine, the `timeToLive` field must be changed from the default value of `0`. Set the `timeToLive` field based on the distribution of your clustered machines. A list of possible settings follows:
>
> | | |
> |---|---|
> | 1 | Multicast packets restricted to the same subnet (suggested cluster value if distribution unknown) |
> | 32 | Multicast packets restricted to the same site |
> | 64 | Multicast packets restricted to the same region |
> | 128 | Multicast packets restricted to the same continent |
> | 255 | Multicast packets unrestricted |

13
Setting Up a Cluster

For high availability, you can set up a WebCenter Sites cluster in a WebLogic domain with a primary cluster node on one machine and one or more secondary cluster nodes on the same or different machines. The first WebCenter Sites Managed Server you create is the primary node, and any additional WebCenter Sites Managed Servers in the same domain are secondary nodes.

The following topics describe how to set up a WebCenter Sites cluster.

- Preparing to Set Up a WebCenter Sites Cluster
  Now that you have installed and configured a WebCenter Sites domain with Managed Servers, set up a load balancer, run the Configurator, set up an LDAP authentication provider, and configured CAS, you can set up a cluster of WebCenter Sites Managed Servers for the domain.

- Setting Up a WebCenter Sites Cluster
  After you create one or more WebCenter Sites cluster nodes as Managed Servers (`wcs_server1` and `wcs_server2`), you need to configure the nodes to set up the cluster.

Preparing to Set Up a WebCenter Sites Cluster

Now that you have installed and configured a WebCenter Sites domain with Managed Servers, set up a load balancer, run the Configurator, set up an LDAP authentication provider, and configured CAS, you can set up a cluster of WebCenter Sites Managed Servers for the domain.

Before setting up a WebCenter Sites cluster, ensure that the following tasks are done:

1. Install WebCenter Sites, as Installing the Oracle WebCenter Sites Software describes, and set up a WebLogic domain with at least one WebCenter Sites Managed Server, the primary node in a cluster, as Configuring the WebCenter Sites Domain describes.

   If you followed the instructions in Configuring the WebCenter Sites Domain, you would have a WebCenter Sites domain with one cluster and two Manager Servers to start setting up the cluster.

   To add secondary nodes, you can clone the primary node configuration through the WebLogic Server Administration Console, as Setting Up a WebCenter Sites Cluster describes. Or you can use the Fusion Middleware Configuration Wizard to extend the WebCenter Sites domain,

2. Set up a web tier and load balancer, and configure the primary cluster node to use the load balancer's IP address, as Creating a WebCenter Sites Web Tier describes.

   For more information about setting up a load balancer, see "Server Load Balancing in a High Availability Environment" and "Configure Load Balancer" in the *High Availability Guide*

3. Run the WebCenter Sites Configurator, as Configuring WebCenter Sites describes.

4. For authentication based on an external LDAP authentication provider or Oracle Access Manager, complete this integration before scaling out for a clustered environment. You can change the default identity store to an LDAP authentication provider with Oracle Access Manager, as Switching to Authentication Against an LDAP Directory describes. You also have the option of integrating WebCenter Sites with an external LDAP directory, as Switching to Authentication Against an LDAP Directory describes.

5. If you want to deploy the Centeral Authentication Service (CAS) on a separate server for High Availability, set up a CAS cluster prior to WebCenter Sites cluster configuration.

6. If the CAS application is to reside on a cluster node other than the primary, complete the steps in Configuring the CAS Primary Cluster Node.

7. For a traditional, file-based cluster, set up a new shared location, containing the `wcs_properties.json` file that all the different cluster nodes can point to.

> **Note:**
>
> This step is not required for a cluster that uses the NIO database-based file system. For more information, see Moving the Shared File System to a Database.

   a. In the WebCenter Sites shared storage directory (`sites-shared`), create a directory named `config`.

   b. Move the file `DOMAIN_HOME`/wcsites/wcsites/config/wcs_properties.json to the `sites-shared`/config directory. Do not copy the file.

   c. Update the `sites.config` system property on each cluster node to reference the shared directory where `wcs_properties.json` now resides.

> **Note:**
>
> The `sites.config` cannot used for sharedFS. For the directory sharedFS you need to create a new directory, often the directory `wcssites/wcssites/shared` is used. The configuration utility will fail when pointing the sharedFS to `sites.config` .

8. Shut down all WebCenter Sites Managed Servers in the cluster.

Setting Up a WebCenter Sites Cluster

After you create one or more WebCenter Sites cluster nodes as Managed Servers (`wcs_server1` and `wcs_server2`), you need to configure the nodes to set up the cluster.

First you configure the primary cluster node for WebCenter Sites. Then you can configure one or more secondary nodes to work with the primary node in a cluster. Do the following steps to complete configuration changes required for the primary node to work in a cluster configuration:

1. Register the primary cluster node:

    a. Start the WebCenter Sites Managed Server.

    b. Sign in to the WebCenter Sites Admin interface, select the **Admin** tab, expand **System Tools**, and click **Cluster Node Management**.

    c. Enter valid values for the following fields for `sites_server1`:

    Node name: The node name should be the Managed Server Name. For example: `sites_server1`.

    Host name: The host name or IP address of the node member is the actual listen address of the node, and *not* the load balancer.

    Port number: The port number of the node member is the actual port of the node, and *not* the load balancer's port.

    Batch Host name: The host name or IP address of the node member is the actual listen address of the node, and *not* the load balancer. In a clustered environment, only one batch host is supported. The property must be set on each cluster member to point to the dedicated host.

    Batch Port number: Note that if the port number is something other than `80`, you must also specify the port number.

    Are you installing over a secure connection? : Specify the protocol of the server on which the cluster member is running. Set `yes` for HTTPS and `no` for HTTP.

    d. Click **Add** to register the primary node.

    > **Note:**
    >
    > The primary node *must* be registered first.

2. In WebLogic Admin Console, follow this procedure to navigate to:

    a. **Standard Cluster Setup**: **Servers** >**sites-server** > **Server Start**.

    b. **Dynamic Cluster Setup**: **Clusters** > **Server Templates** > **wcsites-server-template** >**Server Start**.

    Add `-Dsites.node={serverName}` under **Arguments**.

3. In the `DOMAIN_HOME`/wcsites/wcsites/config directory, modify the following two files:

    • `host.properties`: Update the `host.name` property with a valid host name for this cluster node. The `host.name` value should be unique within the cluster.

    • `jbossTicketCacheReplicationConfig.xml`: Update the `bind_addr` property with a valid host or IP address for this cluster node.

4. If the cluster spans multiple physical servers, edit the `cas-cache.xml`, `cs-cache.xml`, `linked-cache.xml`, `ss-cache.xml`, and `jbossTicketCacheReplicationConfig.xml` files in the `DOMAIN_HOME`/wcsites/wcsites/config directory as follows.

    • (Optional) If you are using IPv6 addressing, set multicastGroupAddress value to a valid IPv6 multicast address. This value must be the same for each node in the cluster. For example: [ff0x:0:0:0:0:0:0:301].

- Set the `timeToLive` parameter in `cas-cache.xml`, `cs-cache.xml`, `linked-cache.xml`, and `ss-cache.xml` files to a value appropriate for your environment (typically `1`). Set the `ip_ttl` parameter in `jbossTicketCacheReplicationConfig.xml` file to a value appropriate for your environment (typically `1`). The `timeToLive` field must be changed from the default value of `0` if the cluster members are not all collocated on the same machine. This field must be set based on the distribution of your clustered machines, as the following table shows.

List	Description
1	Multicast packets restricted to the same subnet.
32	Multicast packets restricted to the same site.
64	Multicast packets restricted to the same geographical region.
128	Multicast packets restricted to the same continent.
255	No restriction.

> **Note:**
>
> Sometimes WebCenter Sites installation may be slow and take up to several hours because other installations may be using the same multicast port. Ensure that the ports used for this installation are different from other WebCenter Sites installations on the network. If your installation seems slow, change your multicast ports as a troubleshooting step.

- (Optional) Oracle recommends changing the `multicastGroupPort` value to a unique value greater than `2048`. Ensure that the multicast port used in `jbossTicketCacheReplicationConfig.xml` is the same on each node in the cluster but is different on other clusters running on the same network

5. If the CAS application is colocated on the same WebLogic domain as WebCenter Sites, complete the CAS cluster configuration steps in Configuring the CAS Primary Cluster Node..

6. Test the first node:

    a. Start theWebCenter Sites Managed Server for this node, or if it is already running, restart it (stop and start).

    b. Sign in to WebCenter Sites to ensure it is up and running.

7. To complete configuration changes required for `sites_server2` and any additional secondary nodes, ensure that the Managed Server is shut down, do the following steps, and then go back and repeat steps 2 through 6.

8. Add any additional nodes to the WebCenter Sites domain, through the WebLogic Server Administration Console (preferred), or by extending the domain through the Fusion Middleware Configuration Wizard.

    a. To add an additional node using the Administration Console, clone the existing primary node (such as `sites_server1`).

b. For `sites_server2` or any additional secondary node added using the Configuration Wizard (*DOMAIN_HOME*/wcsites/wcsites/config.sh), copy the `config` folder from the primary node (*DOMAIN_HOME*/wcsites/wcsites/config to replace the `config` folder created by the Configuration Wizard on the newly added node (*DOMAIN_HOME*/wcsites/wcsites/config).

This ensures that the configuration files on the newly added node are properly configured.

9. Configure the `setStartupEnv.sh` script in the `<DOMAIN_HOME>/bin` folder:

a. Locate the first instance of *wcsites_server1* in a section that appears as follows:

```
if [ "${SERVER_NAME}" = "wcsites_server1" ] ; then
 STARTUP_GROUP="WCSITES-MGD-SVR"
 export STARTUP_GROUP
 fi
```

b. Copy the entire if statement and add one for every additional Sites server. For example:

```
if [ "${SERVER_NAME}" = "wcsites_server1" ] ; then
 STARTUP_GROUP="WCSITES-MGD-SVR"
 export STARTUP_GROUP
 fi
 if [ "${SERVER_NAME}" = "wcsites_server2" ] ; then
 STARTUP_GROUP="WCSITES-MGD-SVR"
 export STARTUP_GROUP
 fi
```

c. Save the file.

10. Complete the following steps related to the folder *DOMAIN_HOME*/wcsites/wcsites/config.

a. Ensure this directory has been copied to each cluster node and is available locally.

b. Ensure this directory is referenced in the Managed Server class path of each cluster node.

c. Ensure this directory does not contain the `wcs_properties.json` file.

11. Register the cluster node with WebCenter Sites:

a. Restart the Managed Server for this cluster node.

b. Sign in to the WebCenter Sites Admin interface, select the **Admin** tab, expand **System Tools**, and click **Cluster Node Management**.

c. In the screen that appears, choose **Add** from the drop-down list and provide values for the following parameters.

Name	Description
Node name	This **must** be the same as the value of `-Dsites.node` for this cluster node from step 3

Name	Description
Host name	The host name or IP address of this cluster node (**not** the load balancer).
Port number	The port number of this cluster node (**not** the load balancer).
Batch Host name	The host name or IP address of the node member, which is the actual listen address of the node, and **not** the load balancer. In a clustered environment, only one batch host is supported. Set this property on each cluster member to point to the dedicated host.
Batch Port number	The batch port number, which you must specify if it is something other than 80.
Are you installing over a secure connection?	Set to **Yes** if using SSL (HTTPS); otherwise set to **No**.

12. Restart the WebCenter Sites Managed Server running this cluster node.

13. Sign in to the WebCenter Sites Admin interface on this cluster node to confirm it is up and running. To view the cluster node configuration, click the **Admin** tab and navigate to **System Tools** > **System Information** > **Sites Info**.

14. (Optional) If you want to move the WebCenter Sites shared storage into a database, complete the steps in Moving the Shared File System to a Database.

For more information about clustering, see Advanced Administration: Expanding Your Environment in *Administering Oracle Fusion Middleware*.

14

Moving the Shared File System to a Database

WebCenter Sites can leverage a database to store its shared file system using the Java Nonblocking I/O (NIO) API. This eliminates the need for a network file share in a clustered environment and allows file locking to be handled by a Coherence cache.

> **✏ Note:**
>
> Although moving the shared file system to a database helps streamline the backup process, the movement adds an overhead of 5-10% in the overall performance. To improve performance and make the impact negligible, Oracle recommends you to tune the NIO cache parameters based on your architecture.

Out of the box, WebCenter Sites defaults to a disk-based shared file system (local or network). To move the shared file system to a database, complete the steps in this topic. Steps for reverting the process are also provided.

> **Note:**
>
> - Only the Oracle 11*g* and 12*c* databases are supported.
>
> - Oracle recommends storing files managed by WebCenter Sites (also referred to as shared files) in a database. This helps in configuring highly available deployments along with streamlining backup and restore processes for your environments. The database can be WebCenter Sites's own database or a separate database. Depending upon the needs of your site, you may need to plan for additional capacity or processing, or both.
>
> - If you are clustering WebCenter Sites, you must do the following steps before moving the shared file system:
>
>   1. Complete the steps in Setting Up a Cluster.
>
>   2. Add all cluster members to the Coherence Cluster:
>
>   a. In the WebLogic Server Administration Console, navigate to **Domain Name** > **Environment** > **Coherence Clusters**.
>
>   b. Select the default Coherence cluster, and then click the **Members** tab.
>
>   c. In the **Clusters** section, enable your WebCenter Sites cluster, and then enable the `All servers in the cluster` option.
>
> - Ensure that the primary node of the cluster has been set up and registered as a cluster node as Setting Up a WebCenter Sites Cluster describes.
>
> - The default data source name is `wcsitesDS`. If you want to use a different data source name, you must set the `databaseConnector` bean in *sites_config_dir*/NIOSharedServices.xml to the new name before completing the following steps.
>
>   > **Note:**
>   >
>   > The *sites_config_dir* is *DOMAIN_HOME*/wcsites/wcsites/config/.
>
> - If you have already setup a traditional, file-based cluster, the `wcs_properties.json` would have been moved to the `sites-shared/config` directory as part of the cluster setup. In that case, make note of the following:
>
>   – Move the `wcs_properties.json` file back to the `sites_config_dir`.
>
>   – If subsequently you wish to revert from database back to disk storage, then after having run the NIO Conversion utility with revert option, copy the `wcs_properties.json` file back to the `sites-shared/config` directory.
>
> - If you want to store the WebCenter Sites shared file system in the WebCenter Sites repository database, increase the tablespace size for the *prefix*_TS_WCSITES and *prefix*_TS_TMP_WCSITES tablespaces.

- If you want to store the WebCenter Sites shared file system in a database other than the WebCenter Sites repository database, do the following steps:

  1. Create a new database with the same permissions as the WebCenter Sites repository database with the following commands:
     - CREATE SEQUENCE
     - CREATE SESSION
     - CREATE TABLE
     - CREATE TRIGGER
     - CREATE VIEW
     - UNLIMITED TABLESPACE

  2. Create a new data source pointing to the new database, and deploy the new data source as a JDBC data source on the Managed Servers running WebCenter Sites.

  3. Set the `databaseConnector` bean in `sites_config_dir/NIOSharedServices.xml` to the new data source name.

To move the WebCenter Sites shared file system from disk to a database (either the WebCenter Sites repository, or a different database), do the following steps:

1. Shut down all Managed Servers running WebCenter Sites.

2. Back up `sites_config_dir`. In case of any failures, you can roll back changes made to the `config` folder.

3. Make note of the location of the WebCenter Sites shared directory.

   You can look it up the location in the `sites_config_dir/wcs_properties.json` file by searching for "`wcsites.shared`".

4. Set the `databaseConnector` and `sitesDatabaseConnector` beans in `sites_config_dir/NIOConversionServices.xml` to the appropriate database connection URL or URLs.

   The beans will be different only if you plan to store the WebCenter Sites shared file system table (`WCS_SHAREDFILESYSTEM`) in a database separate from the primary WebCenter Sites database.

5. Open a command prompt and change to `ORACLE_HOME/wcsites/webcentersites/sites-home/bin/`.

6. Run the conversion script: .

   a. `./nioconversion.sh sites-home_directory sites_config_directory sites_shared_directory convert|revert|sharefs|dbasefs database_driver_file`

   b. `sharefs/dbasefs` options convert a disk resident file system into a database resident file system and reverts a database resident file system back to disk resident. This includes all files that exist in the database file system not on the local file system.

   This script is on a UNIX operating system. On a Windows operating system, use the `nioconversion.bat` command, with the same options.

The following table describes the options of this script.

Properties	Description
convert or revert	Converts the shared file system to database storage, or reverts it back to disk storage.
sites-home_directory	Full path to the sites-home directory. By default, this is *ORACLE_HOME*/wcsites/webcentersites/sites-home.
sites_config_directory	Full path to the WebCenter Sites sites_config_directory, with no trailing slash. By default, this is *DOMAIN_HOME*/wcsites/wcsites/config.
sites_shared_directory	Full path of the WebCenter Sites shared file system directory (wcs_shared).
database_driver_file	Full path and name of the database driver file used for connecting to the target database.
silent (optional)	This flag minimizes messages to the console.
sharefs	Changes all configured dbasefs file specifications to sharefs.
dbasefs	Changes all configured sharefs file specifications to dbasefs.

UNIX example: `nioconversion.sh /mySites/sites-home /mySites/config /mySites/sites-shared convert /lib/ojdbc6.jar`

Windows example: `nioconversion.bat C:\mySites\sites-home C:\mySites\config C:\mySites\sites-shared convert C:\lib\ojdbc6.jar silent`

> **Note:**
>
> - The last two arguments are provided to switch between database only (dbasefs) or cache and database (sharefs) operation. These are intended for performance analysis. By default, the converted system will operate with sharefs.
>
> - Do not supply symbolically linked paths to the conversion utility, or the conversion will fail. Supply full hard paths only. If you have symbolic links, you must use the actual value stored in wcs_properties.json:wcsites.shared as a parameter when running the utility

7. When prompted, enter the credentials for WebCenter Sites and the shared file system database (if you are not storing the shared file system in the WebCenter Sites repository database), and wait for the conversion process to complete.

   The passwords will be different only if you plan to store the WebCenter Sites shared file system table (WCS_SHAREDFILESYSTEM) in a database separate from the primary WebCenter Sites database.

The program will replicate the shared file system into the database and update all configuration files (`ini`/`json`/`database` tables) to reference the file system in the database.

The log file for the utility is called `sites.utilities.log`. It is created in the directory from which this utility is run.

8. Locate the old shared file system directory on the disk and rename it (do not yet delete it).

9. Start the WebCenter Sites Managed Servers and sign in to the Admin interface to verify that the new configuration is fully functional.

10. Confirm that the old shared file system directory on disk was not re-created after WebCenter Sites started up. If the directory was re-created, check for any custom code that might still be referencing it.

11. If the old shared file system directory on disk was not re-created after WebCenter Sites started up, back up the directory and then delete it and its contents.

> **Note:**
>
> If you store the WebCenter Sites shared file system in a database other than the WebCenter Sites repository database, logging in to the Admin interface takes a few extra minutes the first time.

15

Switching from Test Mode to Production Mode

After you install and configure an Oracle WebCenter Sites domain in a Fusion Middleware test environment, you can switch WebCenter Sites (and its component applications) to an equivalent production environment.

To switch one or more instances of WebCenter Sites or its component applications from test mode to production mode:

1. For more information standard test-to-production procedure, see Moving from a Test to a Production Environment in *Administering Oracle Fusion Middleware*.

2. Do the additional steps in the following sections for WebCenter Sites and for each of its components that you are moving to production mode.

Additional Steps for Moving WebCenter Sites from Test to Production

To finish moving Oracle WebCenter Sites from a test environment to a production environment:

1. Replace the WebCenter Sites `config` folder with the one available in the WebCenter Sites binaries: *ORACLE_HOME*`/wcsites/webcentersites/sites-home/template`

2. Start the Administration Server and Managed Servers on the target machine.

3. Run the bootstrap process to complete the WebCenter Sites configuration.

Additional Steps for Moving Site Capture from Test to Production

To finish moving Oracle WebCenter Sites: Site Capture from a test environment to a production environment:

1. Replace the Site Capture `config` folder with the one available in the Site Capture binaries: *ORACLE_HOME*`/wcsites/sitecapture/template`

2. Run the Configurator process to complete the Site Capture configuration.

3. Start the Administration Server and Managed Servers on the target machine.

Additional Steps for Moving Visitor Services from Test to Production

To finish moving Oracle WebCenter Sites: Visitor Services from a test environment to a production environment:

1. Replace the WebCenter Sites `config` folder with the one available in the WebCenter Sites binaries: *ORACLE_HOME*`/wcsites/webcentersites/sites-home/template`

2. Start the Administration Server and WebCenter Sites Managed Server on the target machine.

3. Run the bootstrap process to complete the WebCenter Sites configuration.

4. Replace the Visitor Services `config` folder with the one available in the Visitor Services binaries: *ORACLE_HOME*/wcsites/visitorservices/template

5. Start the Visitor Services Managed Server on the target machine.

6. Run the bootstrap process to complete the Visitor Services configuration.

Additional Steps for Moving Satellite Server from Test to Production

To finish moving Oracle WebCenter Sites: Satellite Server from a test environment to a production environment:

1. Replace the Satellite Server `config` folder with the one available in the Satellite Server binaries: *ORACLE_HOME*/wcsites/satelliteserver/template

2. Run the Configurator process to complete the Satellite Server configuration.

3. Start the Administration Server and Managed Servers on the target machine.

Part III

Uninstalling Oracle WebCenter Sites

Use the steps in this section to uninstall Oracle WebCenter Sites.

- Uninstalling or Reinstalling Oracle WebCenter Sites
  Follow the instructions in this section to uninstall or reinstall Oracle WebCenter Sites.

ORACLE®

16

Uninstalling or Reinstalling Oracle WebCenter Sites

Follow the instructions in this section to uninstall or reinstall Oracle WebCenter Sites.

> **Note:**
>
> This task applies only to *standalone* Oracle WebCenter Sites. You cannot uninstall Oracle WebCenter Sites when it is collocated in a WebLogic Server domain, as partial deconfiguration of a configured domain is not supported.

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 16-1   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 Stopping Oracle Fusion Middleware.
Remove your database schemas	Run Repository Creation Utility to remove your database schemas.	See Removing Your Database Schemas.
Remove the software	Run the product uninstaller to remove Oracle Fusion Middleware Infrastructure. Note that if your Oracle home contains multiple products, you must run the uninstaller multiple times, once for each product.	See Uninstalling the Software.
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 Removing the Oracle Home Directory Manually.
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 Removing the Domain and Application Data.

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 *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 *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 *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 *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.

> **Note:**
>
> This task applies only to *standalone* Oracle WebCenter Sites. You cannot uninstall Oracle WebCenter Sites when it is collocated in a WebLogic Server domain, as partial deconfiguration of a configured domain is not supported.

If you want to uninstall the product in a silent (command-line) mode, see Running the Oracle Universal Installer for Silent Uninstallation in *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 **WebCenter Sites 12.2.1.3.0** 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 Sites 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 *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 16-2, click **Help** on the screen.

Table 16-2   Uninstall Wizard Screens and Descriptions

Screen	Description
Welcome	Introduces you to the product Uninstall Wizard.
Uninstall Summary	Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory.
	If you want to save these options to a response file, click **Save Response File** 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 Running the Oracle Universal Installer for Silent Uninstall in *Installing Software with the Oracle Universal Installer*.
	Click **Deinstall**, to begin removing the software.
Uninstall Progress	Shows the uninstallation progress.
Uninstall Complete	Appears when the uninstallation is complete. Review the information on this screen, then click **Finish** 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/wcs_domain`, enter the following command:

   `cd /home/Oracle/config/domains`

   `rm -rf wcs_domain`

   On a Windows operating system, if your Domain home directory is `C:\Oracle\Config\domains\wcs_domain`, use a file manager window and navigate to the `C:\Oracle\Config\domains` directory. Right-click on the `wcs_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/wcs_domain`, enter the following commands:

   `cd /home/Oracle/config/applications`

   `rm -rf wcs_domain`

   On a Windows operating system, if your Application home directory is `C:\Oracle\Config\applications\wcs_domain`, use a file manager window and navigate to the `C:\Oracle\Config\applications` directory. Right-click on the `wcs_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 `wcs_domain`, find the following line and remove it:

   `<domain location="/home/Oracle/config/domains/wcs_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

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_131 that carries security enhancements and bug fixes. From 12*c* (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.

When you upgrade Oracle Identity Manager in an integrated environment, you may encounter the OPSS processing error. The following exception is seen when you run reconfig.sh command to reconfigure the Oracle Identity Manager domain:

```
SEVERE [93] com.oracle.cie.domain.progress.AbstractProgressGenerator -
Error occurred in
phase {OPSS Processing} execution.
java.lang.IllegalStateException: SecurityContext: Domain Name:
IAMGovernanceDomain
JDBC URL: opss-audit-DBDS:jdbc:oracle:thin:@//<hostname>:<port>/
<service>
JDBC URL: opss-data-source:jdbc:oracle:thin:@//<hostname>:<port>/
<service>
Caused by: java.security.InvalidKeyException: Illegal key size
at javax.crypto.Cipher.checkCryptoPerm(Cipher.java:1039)
at javax.crypto.Cipher.implInit(Cipher.java:805)
at javax.crypto.Cipher.chooseProvider(Cipher.java:864)
at javax.crypto.Cipher.init(Cipher.java:1396)
at javax.crypto.Cipher.init(Cipher.java:1327)
```

To resolve this issue:

1. Install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files from the following location: Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 Download.

2. Copy the local_policy.jar and the US_export_policy.jar files to the location `JAVA_HOME/jre/lib/security/`. If the files already exist in the destination folder, overwrite them.

- 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:

1. 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.

2. 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

> **✎ Note:**
>
> - If you change the value of JAVA_HOME for the Node Manager in the `setNMJavaHome.sh|cmd` file, then the Oracle BI system components that you has started using the Node Manager will automatically use the new JAVA_HOME that you specify in the `setNMJavaHome.sh|cmd` file.
>
> - Observe caution while updating the `setDomainEnv.sh|cmd` file. Any incorrect updates may undo the manual operations, such as scale-out, upgrade, or extending the domain, that were performed on the domain.