Oracle® Retail Service Backbone

Installation Guide

Release 16.0.2

E99800-01

November 2018

ORACLE®

Oracle® Retail Service Backbone Installation Guide, Release 16.0.2

E99800-01

Primary Author: Gloreen Soans

reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

Send Us Your Comments

Oracle® Retail Service Backbone Installation Guide, Release 16.0.2.

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at **http://www.oracle.com**.

Preface

The Oracle® Retail Service Backbone Installation Guide contains the requirements and procedures that are necessary for the retailer to install Oracle Retail Service Backbone product.

Audience

The Installation Guide is written for the following audiences:

- Database administrators (DBA)
- System analysts and designers
- Integrators and implementation staff

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.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 16.0) or a later patch release (for example, 16.0.2). If you are installing the base release and additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is available on the following web site:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

(Data Model documents are not available through Oracle Technology Network. You can obtain these documents through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1
Introduction

This document is the installation guide for the Retail Service Backbone (RSB) product. Generally, an RSB installation contains the following components:

- An installation of RSB's Decorator Services on Java EE 5 compliant application server.
- (Optional) Installation of the Java Service Interface Tester tool (JSIT)

It is important to also follow all installation steps of the Oracle Retail Applications that are being connected to the RSB. Failure to follow these may result in a faulty RSB installation. See the installation guides for the relevant Oracle Retail applications for more information.

> **Note:** The instructions provided in this guide apply to a full installation of the RSB 16.0.2.

2

RSB Installation Master Checklist

RSB Installation Master Checklist

This list covers all of the sequential steps required to perform a full installation of the RSB using a command line installation.

Task	Notes
Install JDK 1.8	Prerequisite
Prepare the Oracle Database schemas that the RIB will use: ■ Install Repository Creation Utility (RCU) 12.2.1.3 ■ Create DB schema for OSB using RCU	Prerequisite
Prepare the Oracle WebLogic Servers for installation of the RSB Components: ■ Install Oracle Service Bus (OSB) on WebLogic ■ Configure OSB domain and ADF runtime (Oracle JRF-12.2.1.3) ■ Create Cluster	Prerequisite
Verify that the applications to which RSB will be integrating are configured appropriately	
Gather information for the installation (URLs, credentials, path information etc)	During the prerequisites steps, there is information that should be noted that will be used to configure the RSB during the installation process.
Install using the RSB command line tools.	

3

Technical Specifications

RSB has several dependencies on Oracle Retail Application installations, as well as on the Oracle WebLogic servers. This section covers these requirements.

Note: Oracle Retail assumes that the retailer has applied all required fixes for supported compatible technologies.

Requesting Infrastructure Software

If you are unable to find the necessary version of the required Oracle infrastructure software (database server, application server, WebLogic, etc.) on the Oracle Software Delivery Cloud, you should file a non-technical 'Contact Us' Service Request (SR) and request access to the media. For instructions on filing a non-technical SR, see My Oracle Support Note 1071023.1 - *Requesting Physical Shipment or Download URL for Software Media*.

Server Requirements

Supported On	Versions Supported
Database Server OS	OS certified with Oracle Database 12c Enterprise Edition. Options are: ■ Oracle Linux 6 or 7 for x86-64 (Actual hardware or Oracle virtual machine). ■ Red Hat Enterprise Linux 6 or 7 for x86-64 (actual hardware or Oracle virtual machine) ■ IBM AIX 7.1 (actual hardware or LPARs) ■ Solaris 11.x SPARC (actual hardware or logical domains) ■ HP-UX Itanium 11.31 Integrity (Actual hardware, HPVM, or vPars)

Database Server 12c	Oracle Database Enterprise Edition 12c (12.1.0.2) with the following specifications: **Components:** ■ Enterprise Edition ■ Examples CD (formerly the companion CD) **Oneoff Patches:** ■ 20846438: ORA-600 [KKPAPXFORMFKK2KEY_1] WITH LIST PARTITION ■ Patch 19623450: MISSING JAVA CLASSES AFTER UPGRADE TO JDK 7 ■ 20406840: PROC 12.1.0.2 THROWS ORA-600 [17998] WHEN PRECOMPILING BY 'OTHER' USER **Other Components:** ■ Perl interpreter 5.0 or later ■ X-Windows interface ■ JDK 1.7
Application Server OS	OS certified with Oracle Fusion Middleware 12c. Options are: ■ Oracle Linux 6 or 7 for x86-64 (Actual hardware or Oracle virtual machine). ■ Red Hat Enterprise Linux 6 or 7 for x86-64 (actual hardware or Oracle virtual machine) ■ IBM AIX 7.1 (actual hardware or LPARs) ■ Solaris 11.x SPARC (actual hardware or logical domains) ■ HP-UX Itanium 11.31 Integrity (Actual hardware, HPVM, or vPars)
Application Server	Oracle Fusion Middleware 12c (12.2.1.3) **Components:** ■ Oracle WebLogic Server 12c (12.2.1.3) ■ Java: JDK 1.8+ latest security updates 64 bit **Patches:** ■ Patch 22648025 : ILLEGALSTATEEXCEPTION WHEN INVOKING A WEBSERVICE/EJB IN WLS 12.2.1.3 (you need an Oracle support account to get it)
Minimum required JAVA version for all operating systems	JDK 1.8+ latest security updates 64 bit

Note: By default, JDK is at 1.6. After installing the 12.1.0.2 binary, apply patch 19623450. Follow the instructions on *Oracle Database Java Developer's Guide 12c Release 1* to upgrade JDK to 1.7. The Guide is available at:

http://docs.oracle.com/database/121/JJDEV/chone.htm#JJDEV01000.

Follow-through to complete the post-patch operation.

Important: If there is an existing WebLogic installation on the server, you must upgrade to WebLogic 12.2.1.3. All middleware components associated with WebLogic server should be upgraded to 12.2.1.3.

Back up the weblogic.policy file ($WLS_HOME/wlserver/server/lib) before upgrading your WebLogic server, because this file could be overwritten. Restore the weblogic.policy from backup file after the WebLogic upgrade is finished and the post patching installation steps are completed.

Additional Requirement for Retail Integration Console (RIC)

The RIC model and view components require ADF runtime to run properly. Verify that ADF runtime 12.2.1.3 or higher is available in the WebLogic Application Server (12.2.1.3) and applied to the domain where RIC will be installed.

Other Resources

For information about WebLogic Application Server 12.2.1.3, see the Oracle WebLogic Server Documentation Library.

- WebLogic Application Server 12c - Index
  http://docs.oracle.com/middleware/12212/cross/getstartedtasks.htm
- WebLogic Application Server 12c - Documents
  http://docs.oracle.com/middleware/12212/wls/index.html

Note: See also the Oracle Database Administrator's Guide 12c (12.2.1.3) and the Oracle WebLogic Application Server 12c (12.2.1.3) documentation.

Additional Requirement for Installing JSIT

JSIT requires WebLogic Application Server 12c (12.2.1.3). Before installing JSIT, verify that the WebLogic Application Server 12c (12.2.1.3) is available in your environment. For more information on installing JSIT, see Install JSIT.

Supported Oracle Retail Products

Retail Product	Version Supported
Oracle Retail Warehouse Management System (RWMS) 16.0.2	RIB 16.0.2
Oracle Retail Merchandising System (RMS) 16.0.2	RIB 16.0.2
Oracle Retail Price Management (RPM) 16.0.2	RIB 16.0.2
Oracle Retail Store Inventory Management (SIM) 16.0.2	RIB 16.0.2
Oracle Retail Advanced Inventory Planning (AIP) 16.0.3	RIB 16.0.2
Integration Gateway Services (IGS) 16.0.2	RSB 16.0.2

Oracle Retail Financial Integration (ORFI) 16.0.2	RSB 16.0.2
Oracle Retail Invoice Matching (ReIM) 16.0.2	RSB 16.0.2
Rib4OMS 16.0.2	RSB 16.0.2

The RSB and Oracle WebLogic Server Cluster

Oracle Service Bus (OSB) supports three types of topologies: Admin-only topology, Admin + Managed Server topology and Cluster topology. The first two topologies are non-clustered topologies which are not highly-available; therefore it is recommended that you use Cluster topology.

Clustering allows OSB to run on a group of servers that can be managed as a single unit. An OSB deployment can use clustering and load balancing to improve scalability by distributing the workload across nodes. A WebLogic server clustered domain consists of only one Admin Server, and one or more managed servers. The managed servers in an OSB domain can be grouped in a cluster. When OSB resources are configured, resources are targeted to the named cluster. The advantage of specifying a cluster as the target for resource deployment is that it makes it possible to dynamically increase capacity by adding Managed Servers to the cluster.

Singleton Resources

While most resources used by OSB are deployed homogeneously across the cluster, there are a few resources that must be pinned to a single Managed Server in order to operate correctly. The following table lists these components:

- Service Bus Cluster Singleton Marker Application
- Service Bus Domain Singleton Marker Application
- Service Bus Message Reporting Purger
- configwiz-jms service

Load balancing in an OSB cluster

Load balancing distributes the workload proportionately across all the servers in a cluster so that each server can run at full capacity. Web services (SOAP or XML over HTTP) can use HTTP load balancing. External load balancing can be accomplished through the WebLogic HttpClusterServlet, a WebServer plug-in or a hardware router. In the steps described in this document, it uses a HTTP proxy server which is a managed server in the same domain and is not a part of the cluster.

4

Preinstallation Tasks

Before you begin installation, check to be sure that you have the most recent version of this installation guide. Oracle Retail installation guides are available on the Oracle Technology Network.

Prepare WebLogic Application Server

Oracle Service Bus (OSB) supports 3 types of topologies: Admin-only, Admin + Managed Server and Cluster. The first two topologies are non-clustered topologies which are not high-available, therefore we recommend using Cluster topology and this document describes how to configure a sample cluster topology for RSB applications.

Steps for Configuring OSB Domain

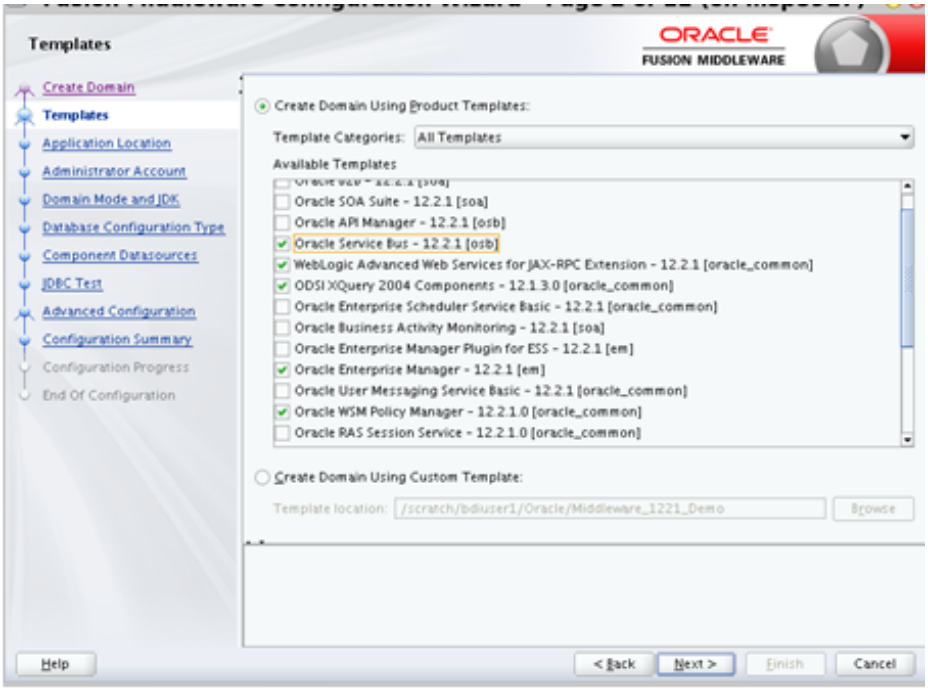
This section describes step-by-step process of creating and configuring an OSB domain using the configuration wizard. In this configuration, there are following servers:

- One Admin Server
- Three Managed Servers: *rsb_server1*, *rsb_server2* and *rsb_http_proxy*.
- Cluster: The cluster consists of rsb_server1 and rsb_server2 as managed servers. OSB features are deployed on this cluster. Also, rsb_server1 hosts the singleton resources of OSB.
- Managed server *rsb_http_proxy* acts as the proxy server of the cluster. It does not have OSB code installed on it.

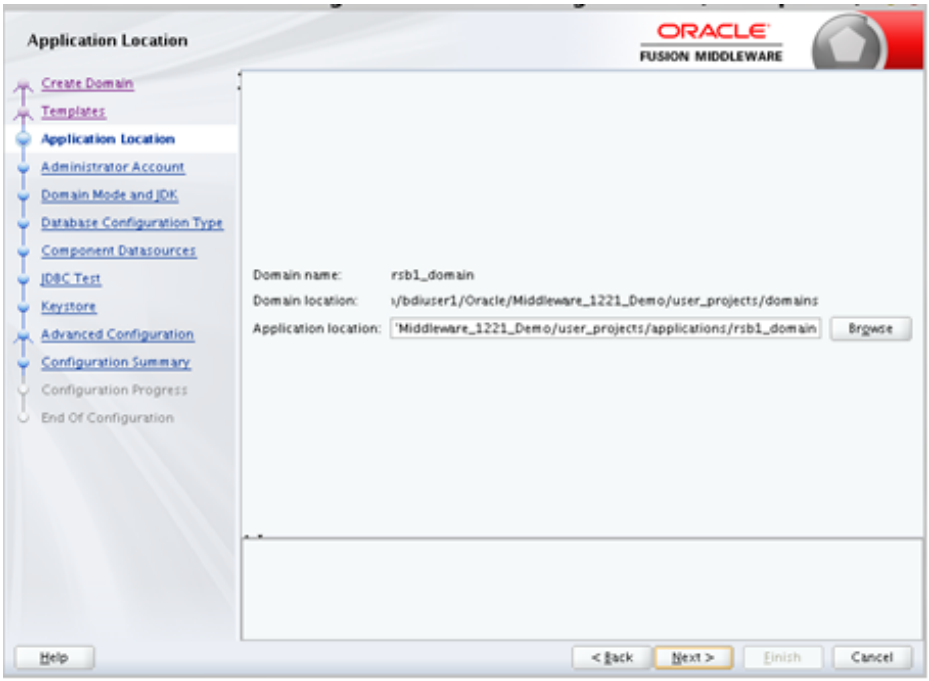
Perform the following steps to create a new WebLogic domain:

1. Run <WLS_HOME>/wlsserver/common/bin/config.sh.
2. Select **Create a new Domain**. Click **Next**.

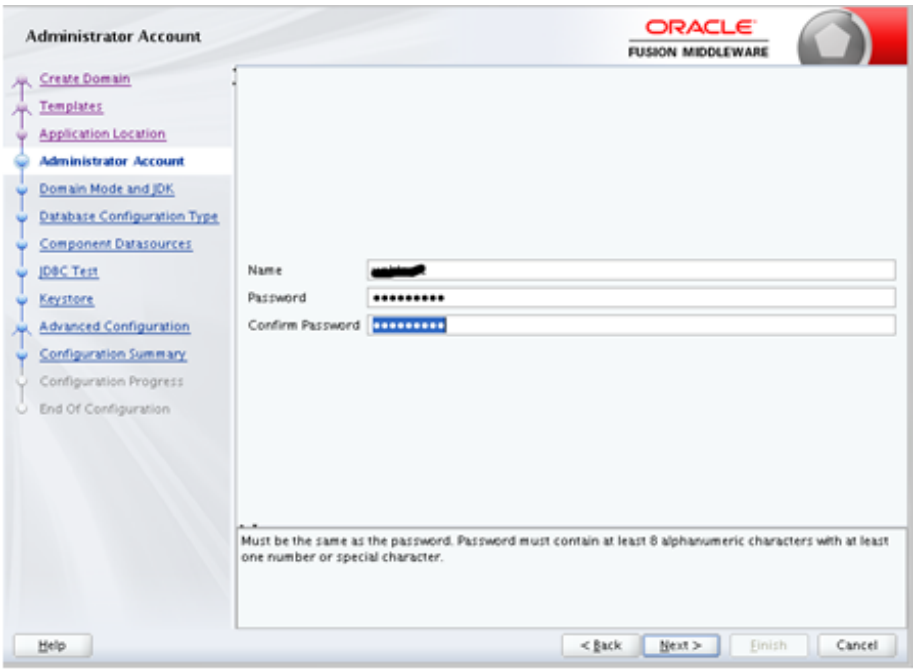
3. Select Oracle Service Bus -12.2.1.3 [osb] option as shown, this will select other required options for OSB like EM, OWSM, JRF etc. Click **Next**.



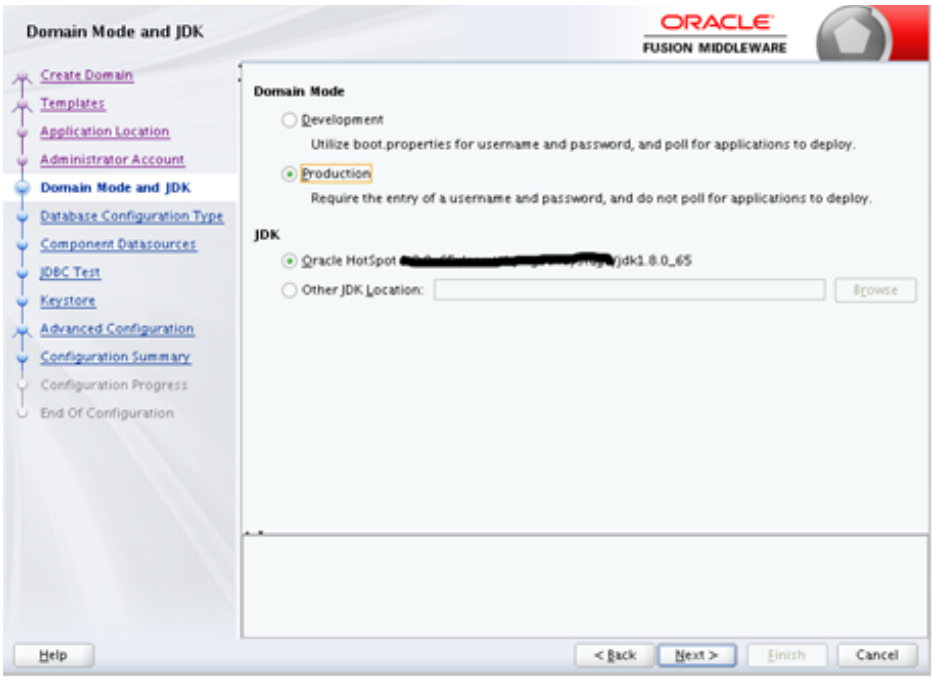
4. Select Application Location and click **Next**.



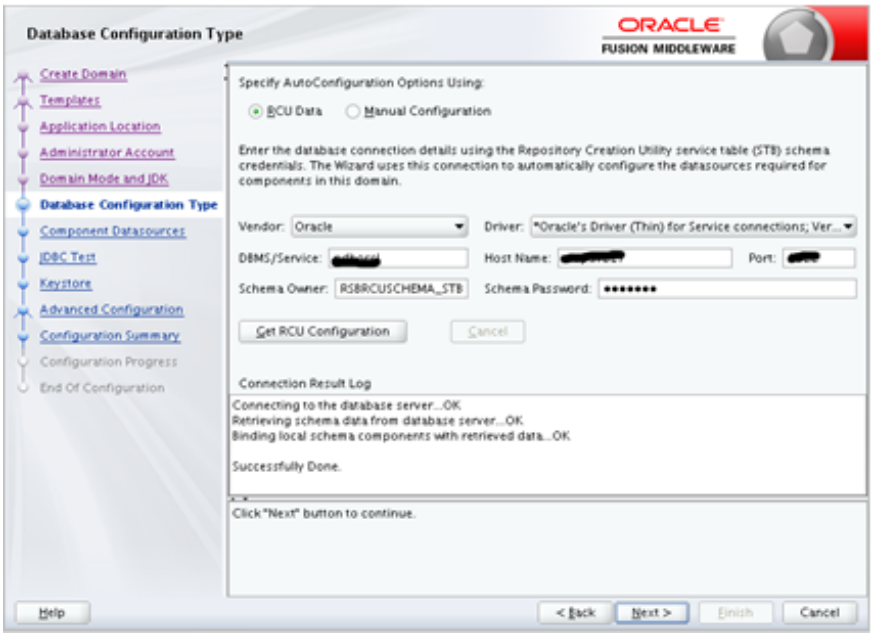
5. Enter **Name** (Username) and **User password** for the domain. Please note down the username and password. These are required again in the compilation phase of RSB.



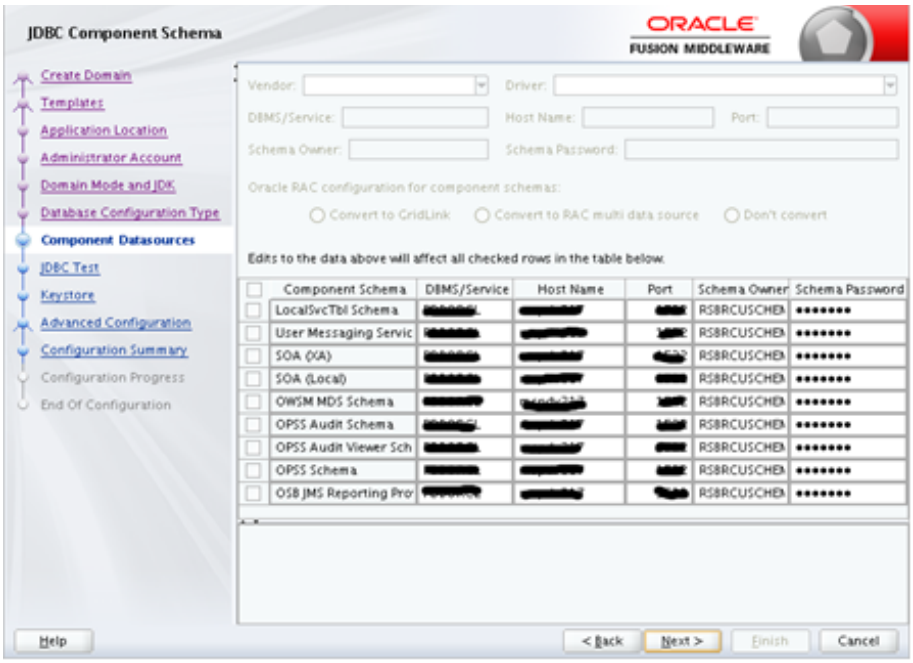
6. Select domain mode option as production and point to latest jdk location. Click **Next**.



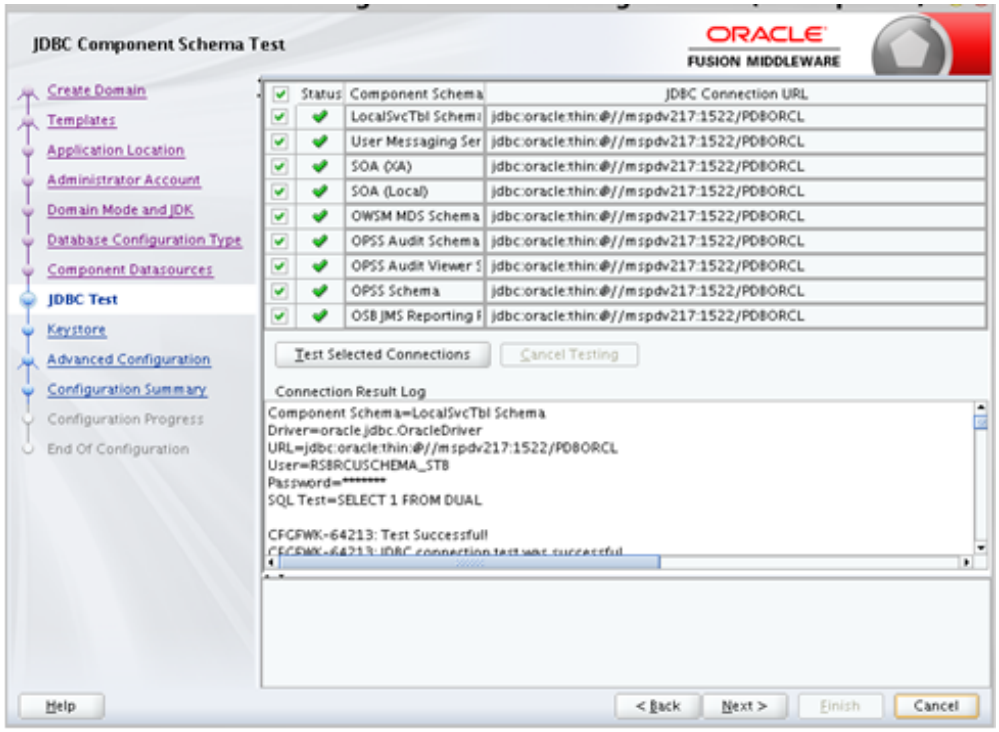
7. Select RCU Data option and enter database details like driver, hostname, service, port, schema owner and password. The schema must be created already using the RCU tool. Then click on Get RCU Configuration button to get the RCU data for RSB. If connection result logs are OK, then click Next.



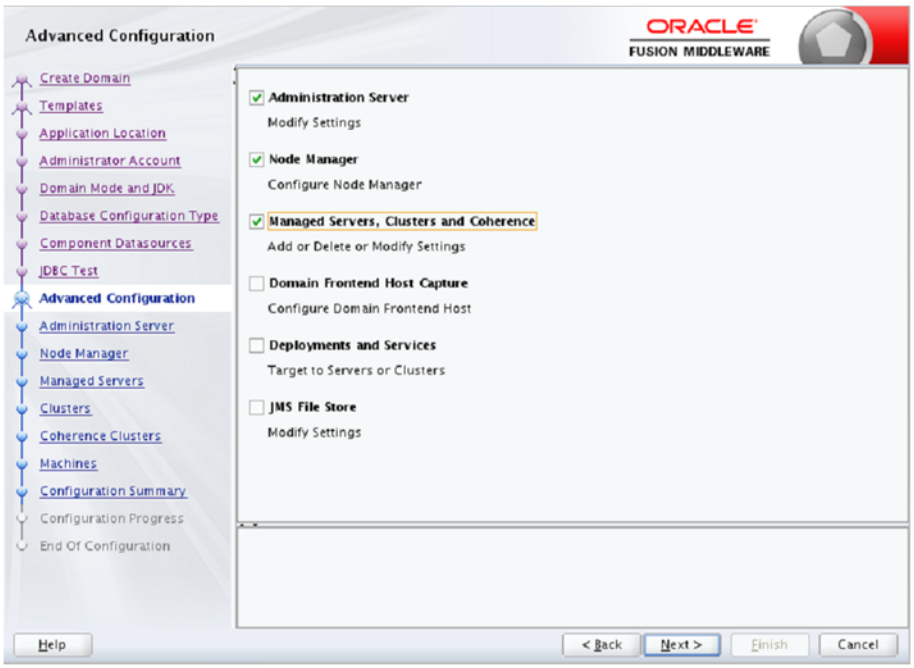
8. This screen shows all RCU schemas for RSB. Select all schemas by clicking on Component Schema Label and click **Next**.



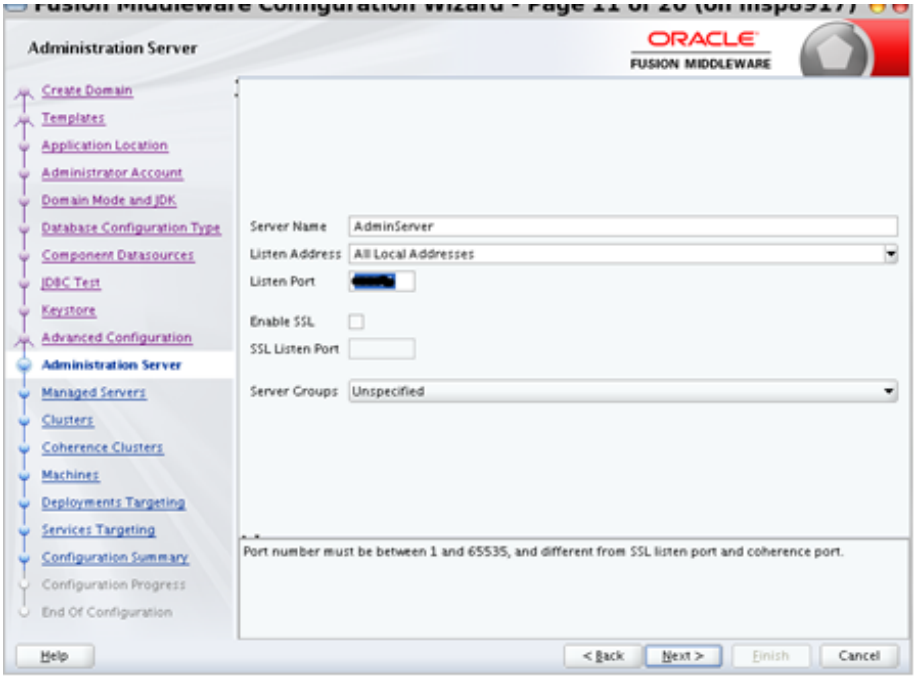
9. Here all the schemas will be tested and corresponding data sources will be created in domain. When all statuses are green, click **Next**.



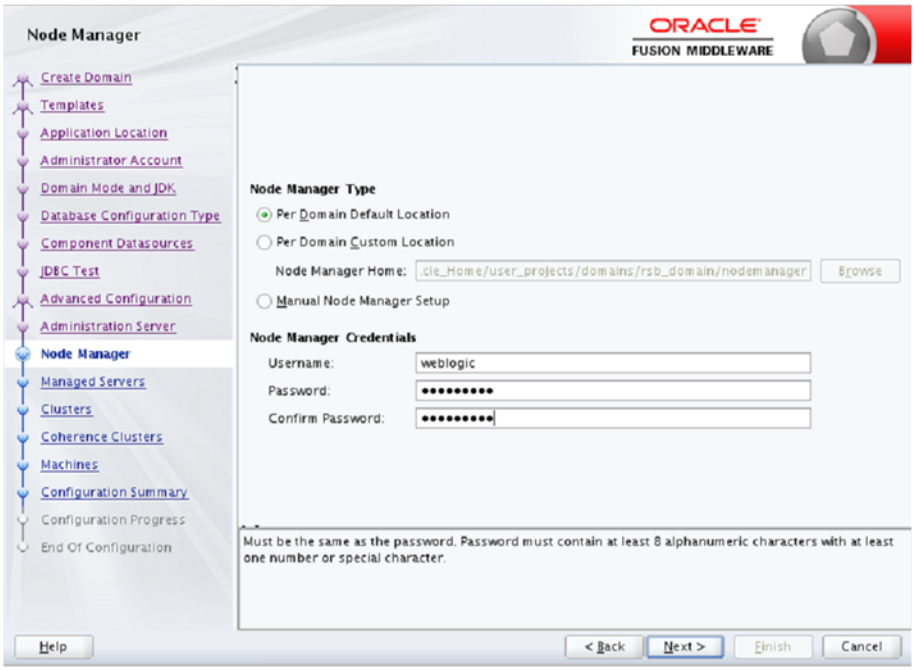
10. Select the options for creating AdminServer, Node Manager, Managed Servers and Cluster. Click **Next**.



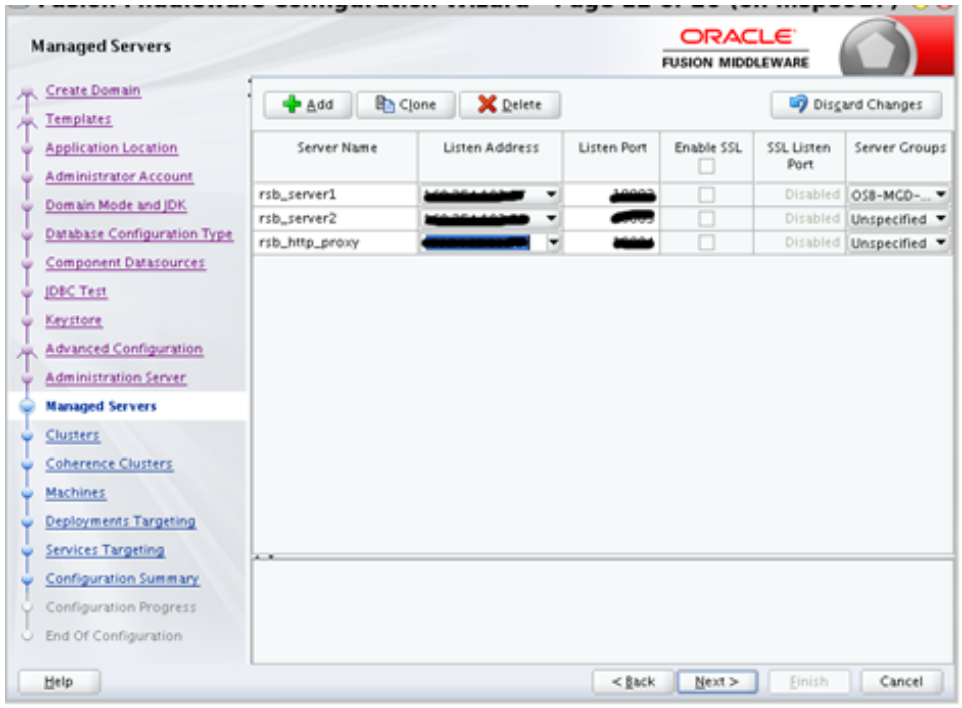
11. Enter Admin Server details, Listen address will be IP address and enter valid Listen port. If you are using SSL, you can enable SSL in this step and specify the SSL port.



12. Enter Node Manager details like select Per Domain Default Location and provide Node Manager Credentials same as weblogic credentials. Click **Next**.



13. Enter details of all managed servers. If you are using SSL, you can enable the SSL in this step and specify the SSL port. Click Next.

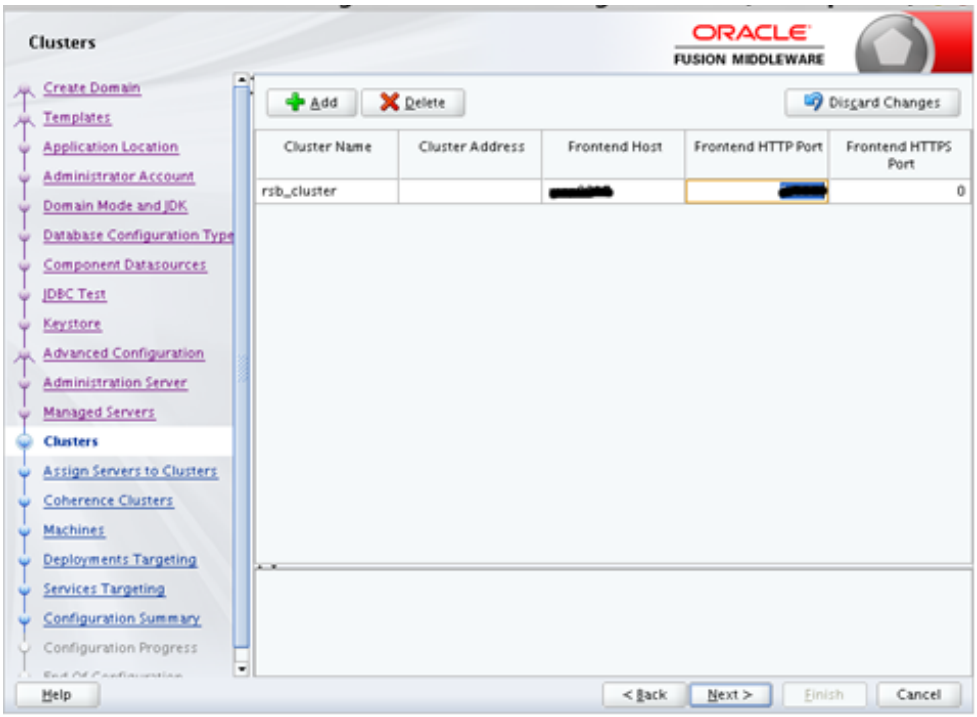


Note: Oracle recommends to disable SSLv3 in all products. We recommend to use TLSv1.2 protocol. WebLogic server can be configured to use TLSv1.2 protocol by adding the following line in the setDomainEnv.sh. Restart the server after making the change.

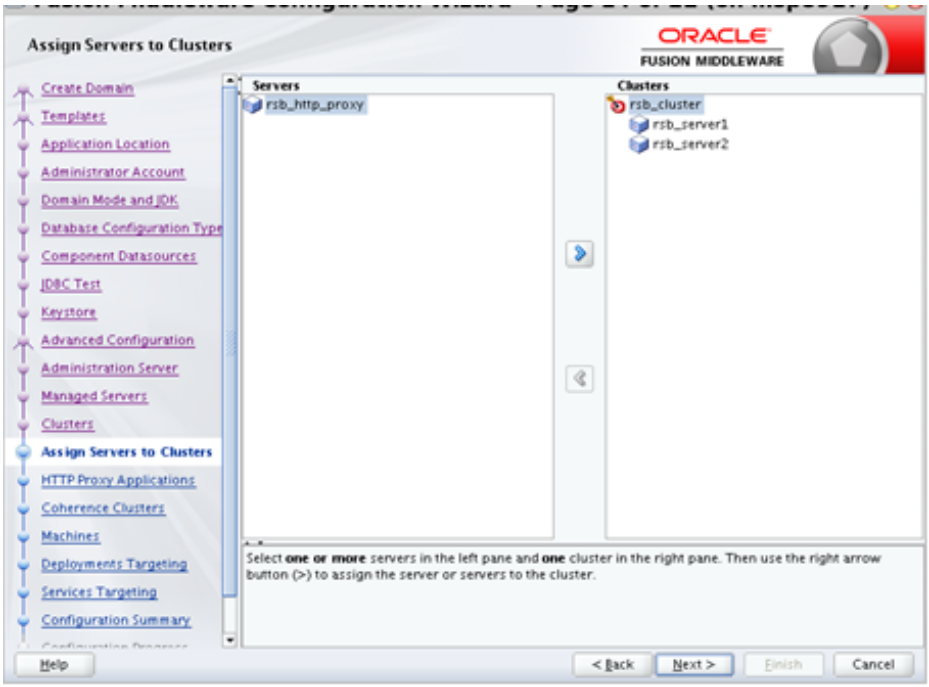
JAVA_OPTIONS=" $JAVA_OPTIONS
-DwebLogic.security.SSL.minimumProtocolVersion=TLSv1.2"

---

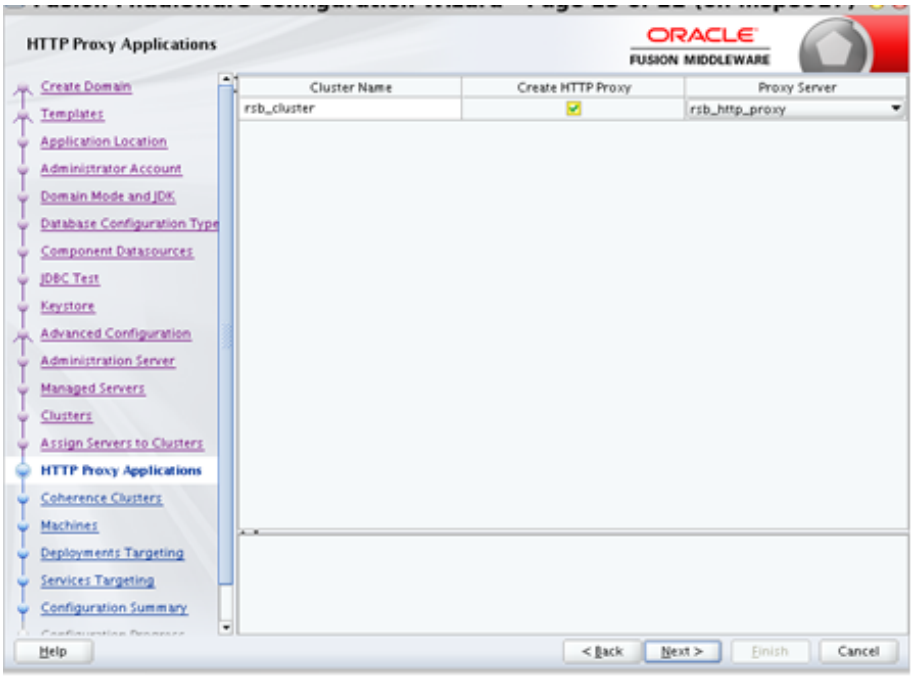
14. Enter the cluster name.



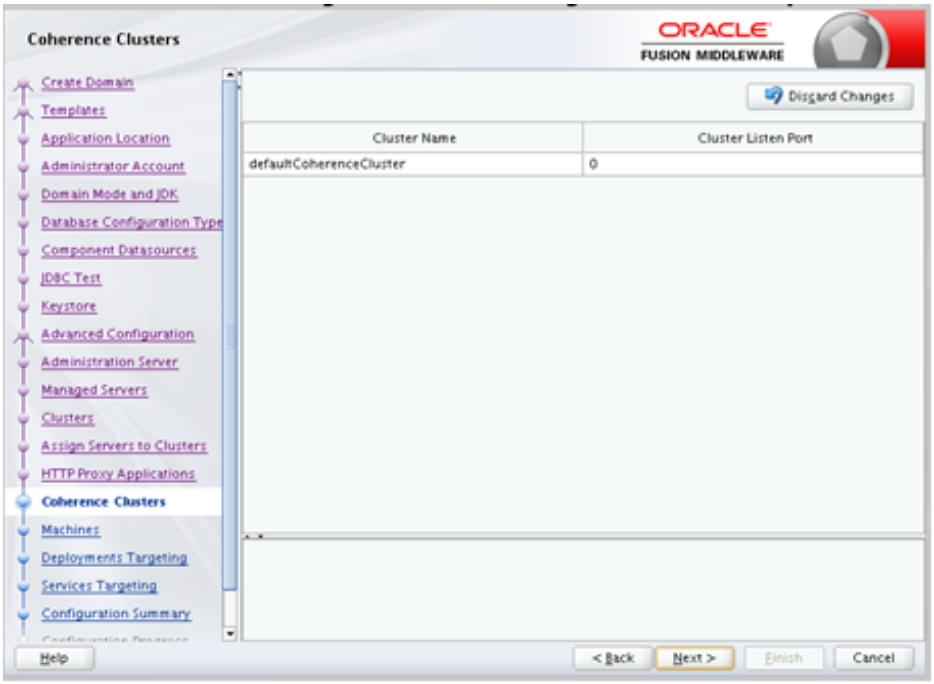
15. Add managed servers to the cluster. Notice that the proxy server, rsb_http_proxy, is not added to the cluster because we need that server as the HTTP proxy of the cluster.



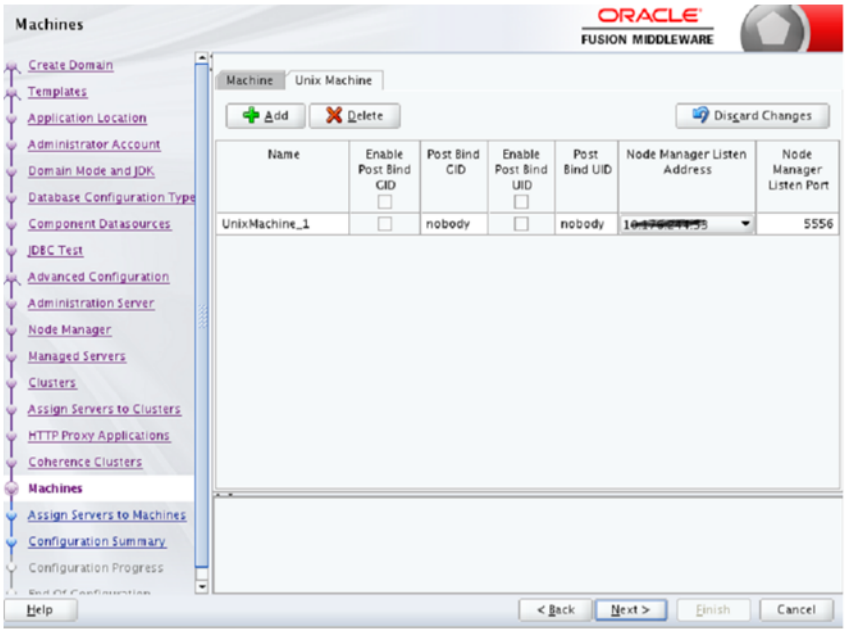
16. Enter HTTP Proxy details.



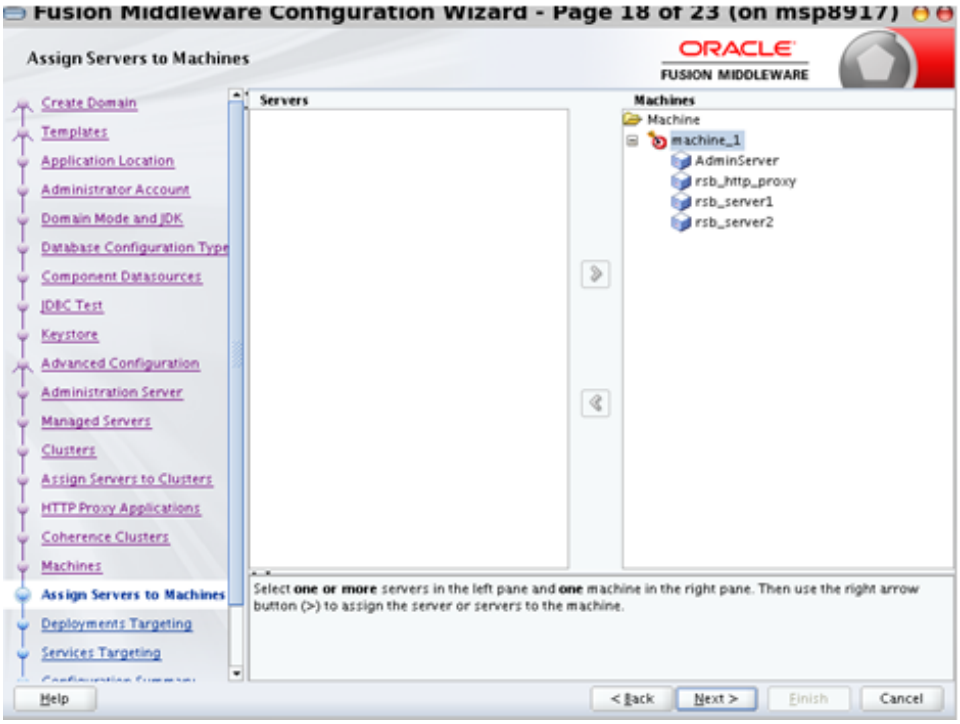
17. Do not modify coherence cluster details keep it as is and Click **Next**.



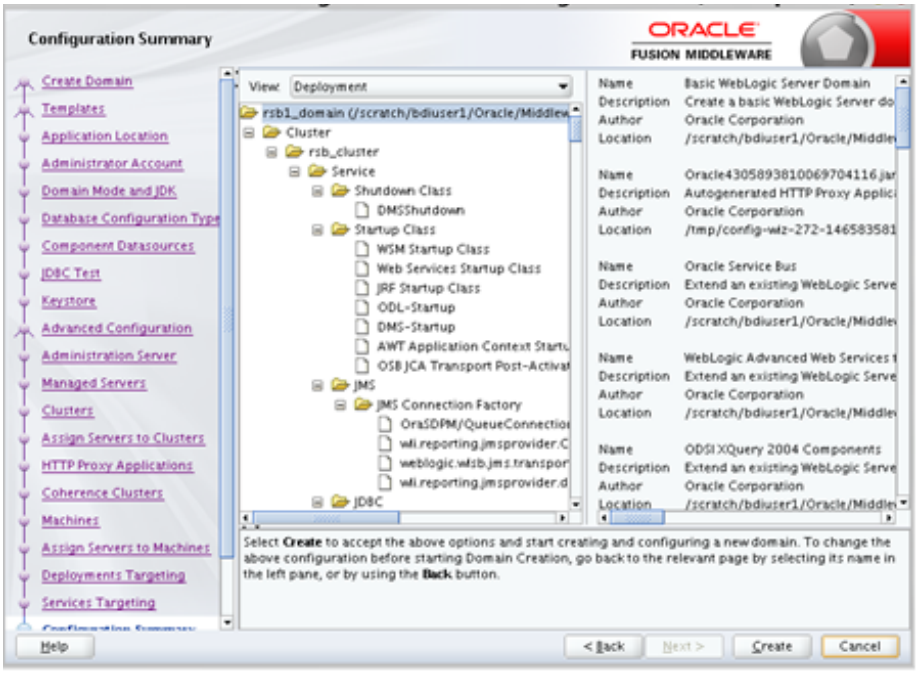
18. Configure Machine details. Click **Unix Machine** and specify the Name, Node Manager hostname and port. Click **Next**.



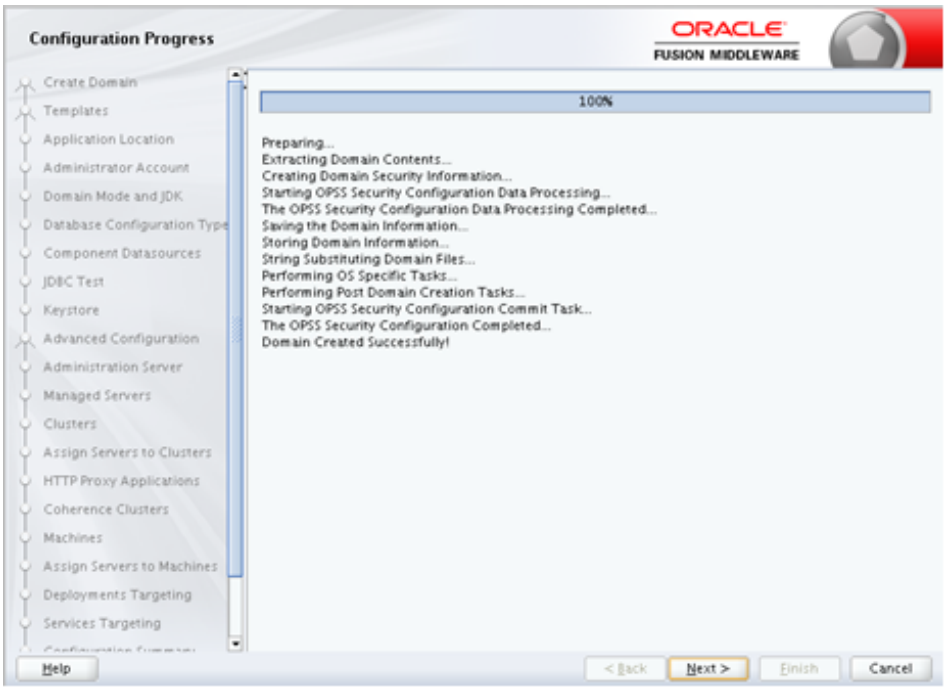
19. Add servers to the machine. Add all the servers.



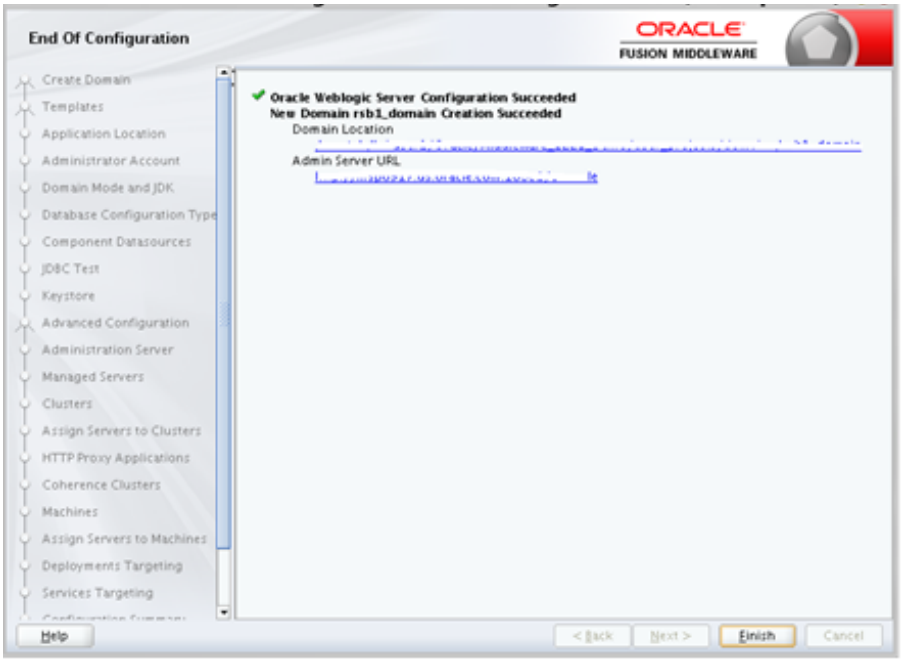
20. From the Configuration Summary page, click **Create**.



21. Domain creation confirmation page



22. The following screen appears after successful domain creation. Click **Finish**.



23. Grant required permission for WebLogic to access the credential store. Edit the <wlsHome>/wlserver/server/lib/weblogic.policy file and add the following permission, after replacing <domain-home> with the correct value.

    grant codeBase "file:<domain-home>/-" {

    permission java.security.AllPermission;

    permission oracle.security.jps.service.credstore.CredentialAccessPermission "credstoressp.credstore", "read,write,update,delete";

    permission oracle.security.jps.service.credstore.CredentialAccessPermission "credstoressp.credstore.*", "read,write,update,delete";

    };

24. Edit the DOMAIN-HOME/bin/setDomainEnv.sh to add the max and min memory requirement for the servers. It is recommended to use 2GB or more for max memory.

    USER_MEM_ARGS="-Xms1024m -Xmx2048m -XX:MaxPermSize=1024m"

25. If NodeManager is used to control the servers in the cluster, edit WL_HOME/common/nodemanager/nodemanager.properties file to change the StartScriptEnabled property to true and make sure the StartScriptName property is set to startWebLogic.sh. Below is a sample from the file:

    ```
    StartScriptName=startWebLogic.sh
    StartScriptEnabled=true
    ```

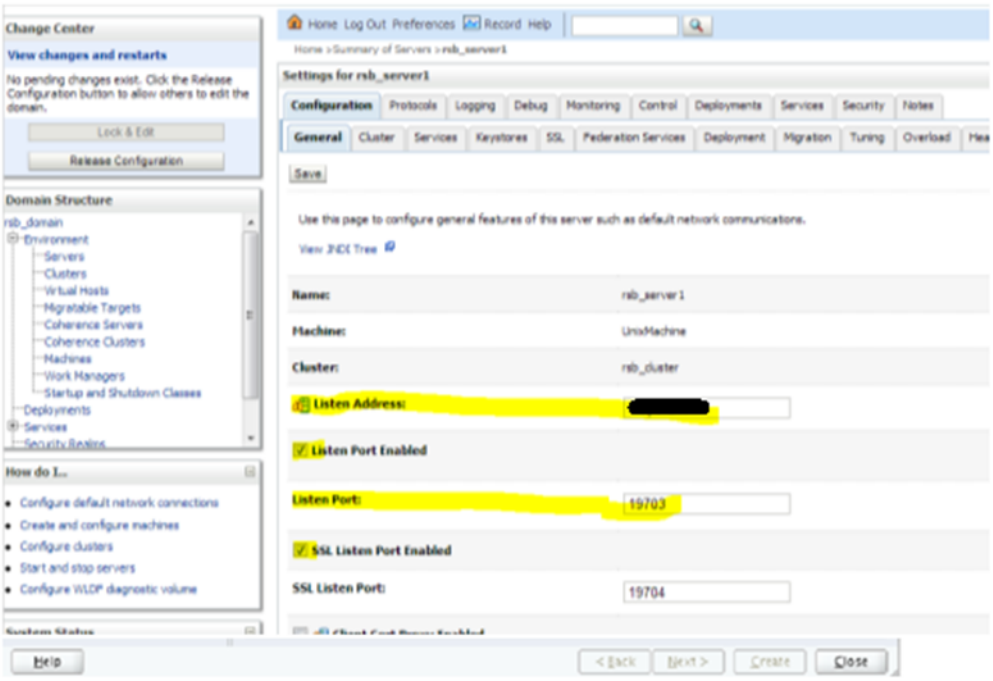
HTTPS Configuration for WebLogic Server

If you are using https (for Policy A), you will have to configure the following:

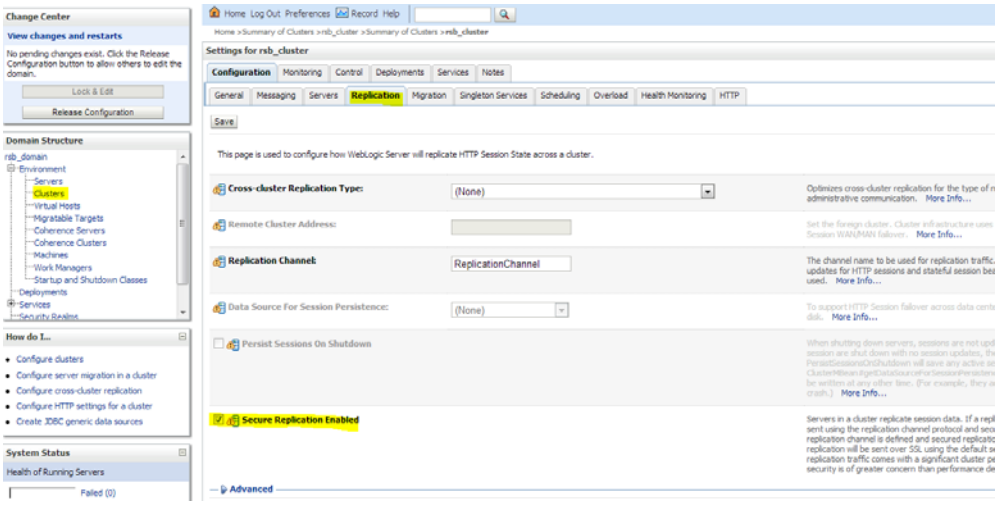
Note: For additional information on configuring Policy A or Policy B, see the *Oracle Retail Service Backbone Security Guide*.

---

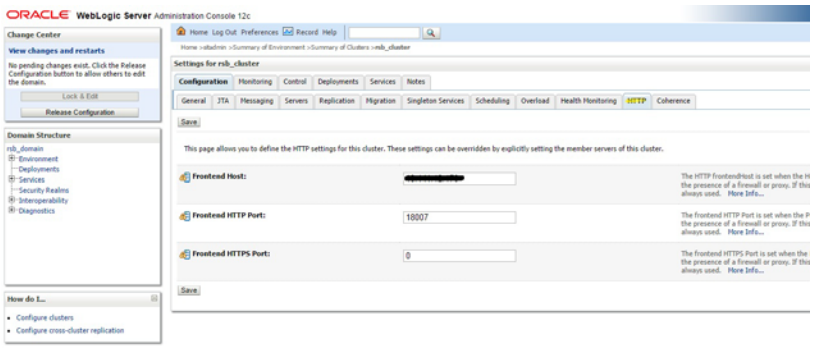
1. Enable https port for AdminServer, Http Proxy Server and all managed servers. Specify the **Listen Address**. The **Listen Address** must match the CN entry of the server certificate. Sometimes the CN entry of the server certificate is the fully qualified name (for example, rsbhost.example.com) instead of the short hostname (for example, rsbhost). If the entries do not match, the security configurations will not work.



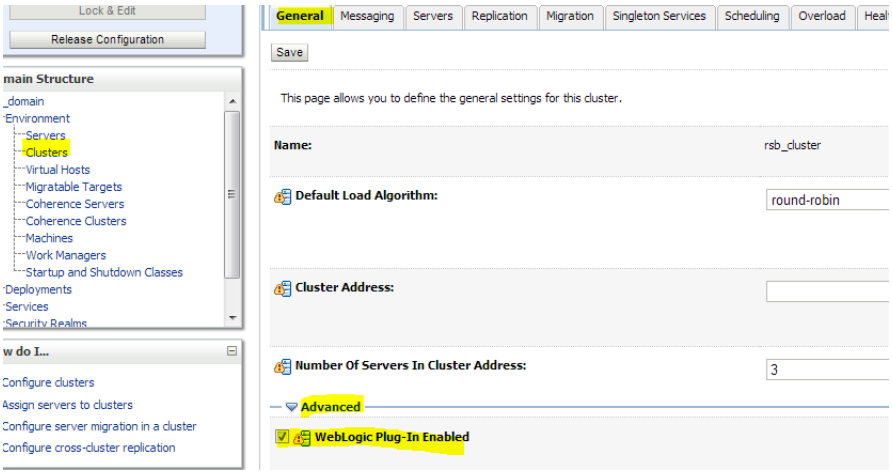
2. Enable secure replication. Enable the Secure Replication Enabled option available in **Environment** --> **Clusters** --> <cluster name> --> **Configuration** --> **Replication**



3. Set the Frontend Hostname for the cluster. This should match the CN entry of the certificate. **Environment** --> **Clusters** --> <cluster name> --> **Configuration** --> **HTTP**



4. Enable WebLogic plug-in. Check **WebLogic Plug-In Enabled** checkbox in **Environment** --> **Clusters** --> <cluster name> --> **Configuration** --> **General** --> **Advanced**. After the change, **Save, Activate Changes** and restart the Admin Server.



5

Database Installation Tasks

This chapter describes how to install the necessary database.

Repository Creation Utility

Many of the Oracle Fusion Middleware components require the existence of schemas in a database prior to installation. These schemas are created and loaded in your database using the Repository Creation Utility (RCU).

See Repository Creation Utility documentation for more information:

http://docs.oracle.com/middleware/12212/core/RCUUG/toc.htm

RCU is available with the Oracle Fusion Middleware Infrastructure distribution in 12c (12.2.1.3).

The repository for Oracle Service Bus (OSB) must be created using RCU tool. The repository must contain SOA Infrastructure (SOAINFRA) schema and all schemas under AS Common Schemas label.

While creating a schema using RCU tool, user must select/mention a prefix which is added to all the schemas created by RCU. In the following example, RCU tool is used to create a repository with SOA Infrastructure schema as <prefix>_SOAINFRA, Metadata Services schema as <prefix>_MDS etc.

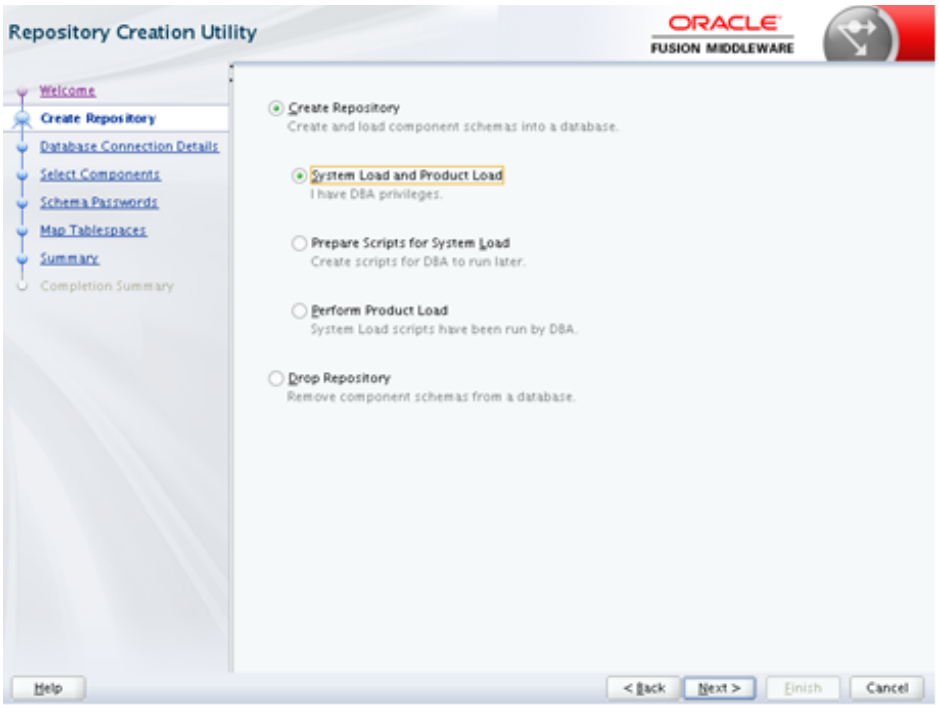
Steps for Creating Database Schema using RCU

1. Run rcu executable from *<wlsHome>/Oracle_Home/oracle_common/bin*

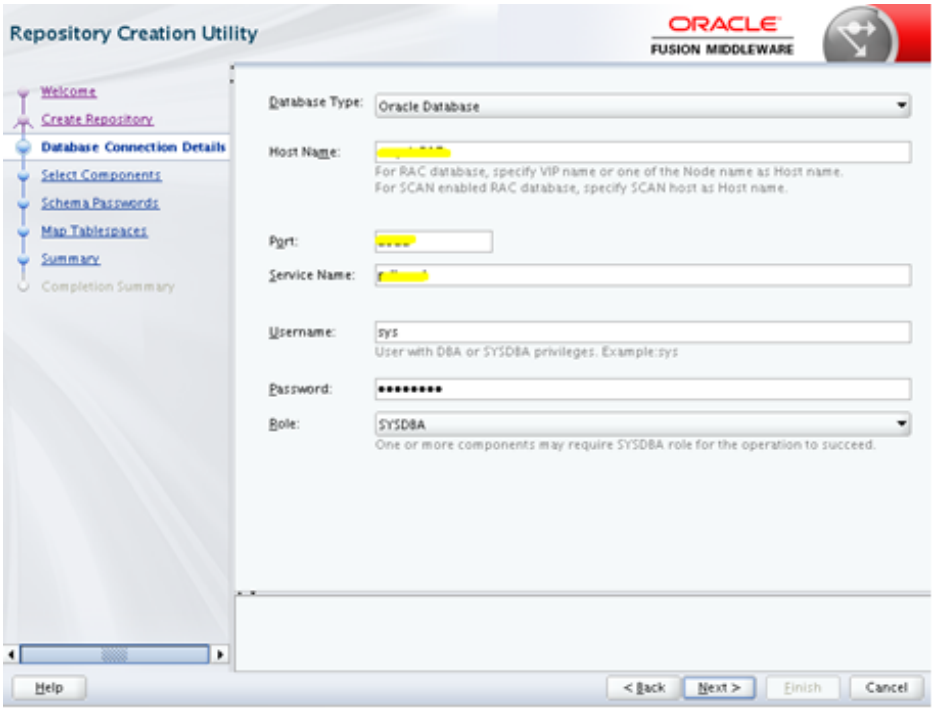
   ```
   cd <wlsHome>/Oracle_Home/oracle_common/bin
   rcu
   ```

   The Welcome page appears.

2. Click **Next** to continue.



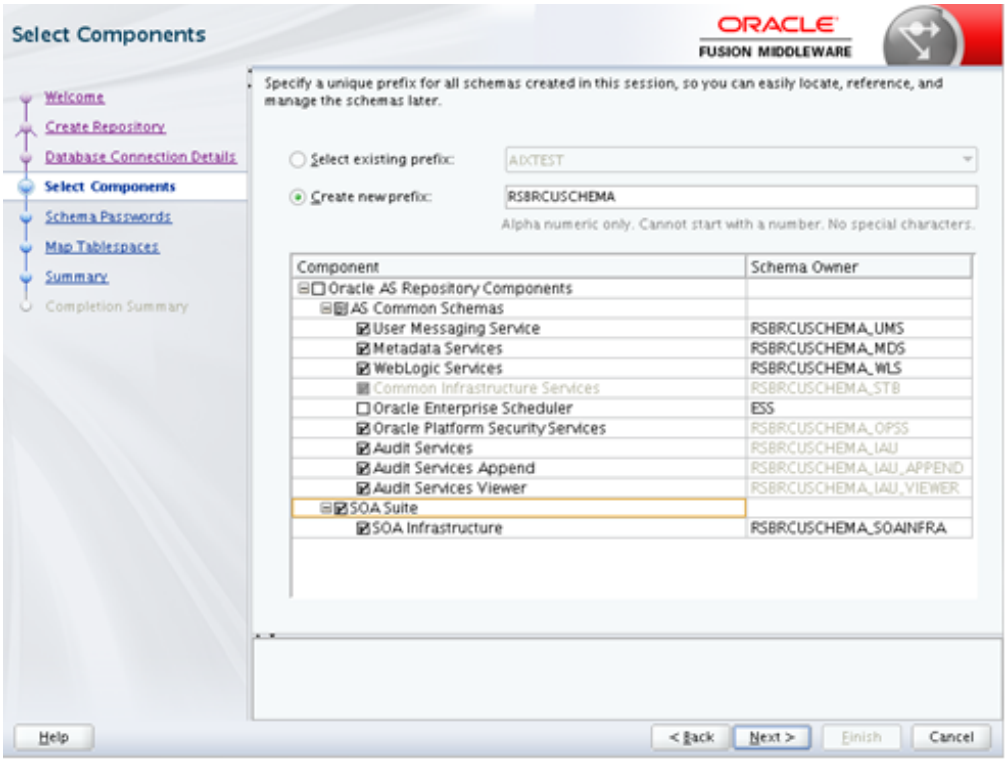
3. In Repository Creation Utility window, select Create Repository option and System Load and Product Load. Click **Next**.



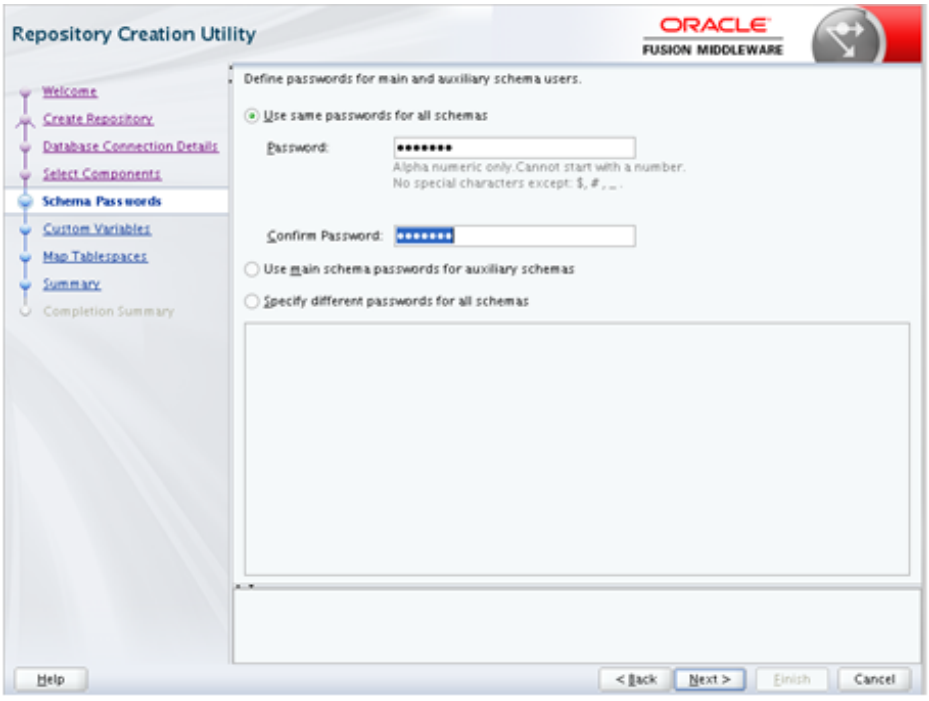
4. In Database Connection Details window, provide database details and click **Next**.

   Database Type: Oracle Database

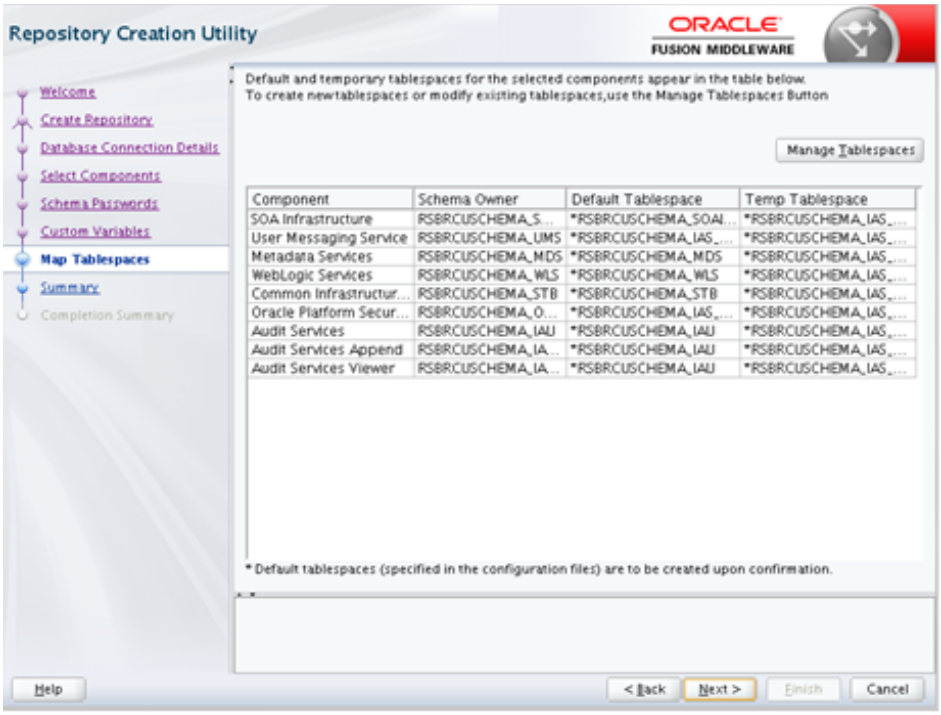
   Role: SYSDBA



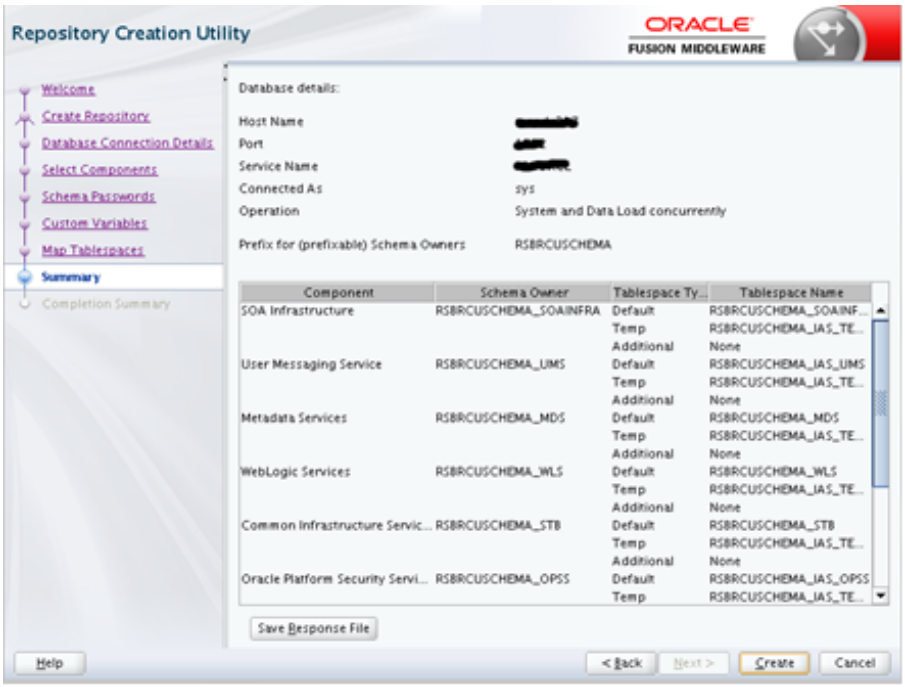
5. In Select Components window, provide a prefix (Select an existing prefix from drop down or give a new one). In Component box, select all options under AS Common Schemas and SOA Infrastructure as shown.



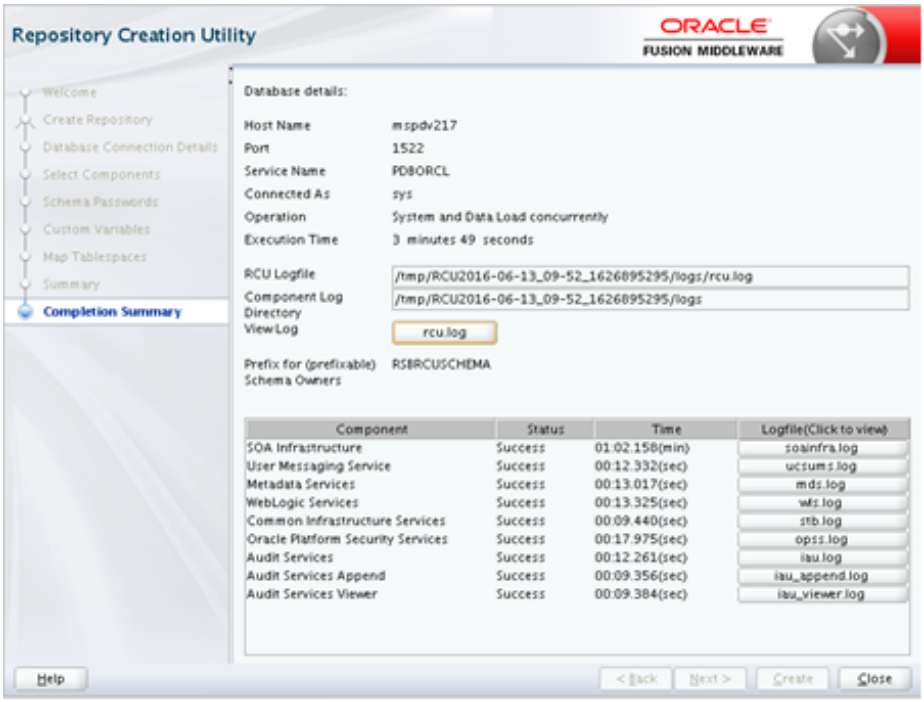
6. In Schema Passwords window, provide password and Click **Next**. Note down the schema name and passwords. These are needed during the domain creation time for configuring the OSB schemas and RSB compilation phase as credentials for sidb-jdbc-user-alias.



7. In Map Tablespaces window, check tablespace mapping details and click **Next**.



8. In Summary window, check database details and click **Create**.



9. In Completion Summary window, click **Close**.

6

RSB Installation

This chapter provides instructions for installing RSB. The complete installation of RSB can be broadly divided into four phases:

- Download
- Configuration
- Compilation
- Deployment

> **Note:** If there is an existing WebLogic installation on the server, you must upgrade to WebLogic 12.2.1.3. All middleware components associated with WebLogic server should be upgraded to 12.2.1.3.
>
> Back up the weblogic.policy file ($WLS_HOME/wlserver/server/lib) before upgrading your WebLogic server, because this file could be overwritten. Copy over the weblogic.policy backup file after the WebLogic upgrade is finished and the post patching installation steps are completed.

- Overview of RIC modes and installation of RIC in RSB only mode and DUAL mode.
  - RIC modes
  - Installation of RIC in different modes

Steps to Install RSB

The following sections describe the process of installing the RSB product.

Download

In this phase, you have to download all the necessary archive files.

1. Download `RsbKernel16.0.2.0ForAll16.x.xApps_eng_ga.zip` to a directory in Linux/Unix. The rsb-home will be created inside this directory. Extract the archive file.

   ```
   unzip RsbKernel16.0.2.0ForAll16.x.xApps_eng_ga.zip
   ```

2. Download all **`RsbAppServiceDecoratorPak<rsb_major_version>For<app><app_version>_eng_ga.zip`** to

rsb-home/download-home/all-app-service-decorator directory. Do not extract the files.

3. Download all **RsbServiceIntegrationFlowPak<rsb_major_version>For<service-name>_eng_ga.zip** to **rsb-home/download-home/all-functional-service-int-flow** directory. Do not extract the files.
4. Download the External and Sim Service Integration Paks. Due to constraints on file size, the External and Sim paks have been split up into the following zips:
   - RsbExt1.zip
   - RsbExt2.zip
   - RsbExt3.zip
   - RsbExt4.zip
   - RsbExt5.zip
   - RsbSim1.zip
   - RsbSim2.zip
   - RsbSim3.zip
   - RsbSim4.zip
5. Merge the RsbExt*.zip files into RsbServiceIntegrationPak16.0.2.0ForExternal16.0.2_eng_ga.zip:
   a. mkdir temp_work_area
   b. cd temp_work_area
   c. download all RsbExt?.zip
   d. cat RsbExt?.zip > whole.zip
   e. zip -FF whole.zip --out RsbServiceIntegrationPak16.0.2ForExternal16.0.2_eng_ga.zip
6. Merge the RsbSim*.zip files into RsbServiceIntegrationPak16.0.2ForSim16.0.2_eng_ga.zip:
   a. mkdir temp_work_area
   b. cd temp_work_area
   c. download all RsbSim?.zip
   d. cat RsbSim?.zip > whole.zip
   e. zip -FF whole.zip --out RsbServiceIntegrationPak16.0.2ForSim16.0.2_eng_ga.zip
7. Copy RsbServiceIntegrationPak16.0.2ForExternal16.0.2_eng_ga.zip and RsbServiceIntegrationPak16.0.2ForSim16.0.2_eng_ga.zip to rsb-home/download-home/all-functional-service-int-flow directory. Do not extract the files.
8. Set JAVA_HOME to a JDK 1.8 64 bit.

   For example:

   ```
   export JAVA_HOME=/usr/bin/java/1.8
   ```
9. Run rsb-home/download-home/bin/check-version-and-unpack.sh script.

`check-version-and-unpack.sh`
This will verify the versions of the kernel and downloaded decorators and extract them in respective folders.

Configuration

> **Note:** Please run the command ***uname -n*** and make sure that the output matches exactly with hostname of the machine. This is important since hostname is a part of the names of many internal configuration attributes.

1. Edit *rsb-home/deployment-home/conf/rsb-deployment-env-info.properties* to configure the following properties:
   - JAVA_HOME
   - rsb-deployment-env-info.service-provider-app-in-scope-for-integration
   - rsb-deployment-env-info.service-requester-app-in-scope-for-integration
   - rsb-osb-container.domain-name
   - rsb-osb-container.<domain-name>.home
   - rsb-osb-container.<domain-name>.cluster-name
   - rsb-osb-container.<domain-name>.<cluster-name>.http-url (Cluster port is the port of http proxy server)
   - rsb-osb-container.<domain-name>.admin-server-name
   - rsb-osb-container.<domain-name>.admin-server-http-url
   - rsb-osb-container.<domain-name>.admin-server-connection-url
   - rsb-osb-container.<domain-name>.<cluster-name>.managed-servers: It is a comma-separated list of managed servers in the cluster, excluding the http proxy managed server.
   - rsb-osb-container.<domain-name>.<cluster-name>.<managed-server>.managed-server-connection-url: Repeat this property for all the managed servers in the cluster.
   - service-infrastructure-db.jdbc-url
   - edge-app-container.<app>.connection-url: The host:port of the edge-application.
   - global.app-service-end-point-url-pattern: The pattern of edge service URLs. (**Note**: This is different if the service is hosted on glassfish Vs WebLogic 12c)
   - rib.home.path: It is an optional field, to be given only if a valid rib-home is present.

   Following table lists the various properties and their example values:

Property	Value (Illustration)
JAVA_HOME	/usr/java/jdk1.8.0_65
rsb-osb-container.domain-name	rsb_domain

rsb-osb-container.<domain>.home	rsb-osb-container.*rsb-domain*.home =/u00/rsb/Oracle/Middleware/user_ projects/do mains/rsb_domain
rsb-osb-container.<domain>.cluster-name	rsb-osb-container.*rsb_ domain*.cluster-name=rsb_cluster
rsb-osb-container.<domain>.<cluster name>.http-url (Cluster port is the port of http proxy server)	rsb-osb-container.*rsb_domain.rsb_ cluster*.http-url=http://*rsbhost*:7004
rsb-osb-container.<domain-name>.admin-server-name	rsb-osb-container.rsb_ domain.admin-server-name=AdminServer
rsb-osb-container.<domain>.admin-server-http-url	rsb-osb-container.*rsb_ domain*.admin-server-http-url=http://*rsbhost*:7001
rsb-osb-container.<domain>.admin-server-connection-url	rsb-osb-container.*rsb_ domain*.admin-server-connection-url=t3://*rsbhost*:7001
rsb-osb-container.<domain>.<cluster name>.managed-servers (Comma separated list of managed servers in the cluster, excluding the http proxy managed server)	rsb-osb-container.*rsb_domain.rsb_ cluster*.managed-servers=rsb_server1,rsb_ server2
rsb-osb-container.<domain>.<cluster name>.<managed server>.managed-server-connection-url (*Repeat this property for all the managed servers in the cluster*)	rsb-osb-container.*rsb_domain.rsb_cluster.rsb_ server1*.managed-server-connection-url=t3://*rsbhost*:7002
service-infrastructure-db.jdbc-url	jdbc:oracle:thin:@*rsbhost*:1521:rra1
edge-app-container.<app>.connection-url (the host:port of the edge application)	edge-app-container.*sim*.connection-url=t3://*rsbhost*:8080
global.app-service-end-point-url-pattern (The pattern of edge service URLs. Note: This is different if the service is hosted on glassfish Vs WebLogic)	http://<HTTP_HOSTNAME>:<HTTP_ PORT>/<SERVICE_ NAME>Service/<SERVICE_NAME>Bean
rib.home.path (optional)	rib1@*ribhost*:/u00/rib1/rib2/Rib1602ForAl l16xxApps/rib-home

Additional steps for Policy A configuration

If RSB is configured with Security Policy A, perform the following additional steps:

1. Property configuration in **`rsb-deployment-env-info.properties`**

   rsb-osb-container.<domain>.<cluster>.https-url: The property provides the HTTPS URL of the http proxy managed server.

2. Override the <decorator>.app-service-end-point-url to use **https** protocol and **SSL port.** This can be done at global level OR app level too, but it is recommended to test single service end to end with SSL first during initial stabilization

   Following table lists the various properties and their example values:

Property	**Value (Illustration)**

rsb-osb-container.rsb_domain.rsb_cluster.https-url	rsb-osb-container.*rsb_domain*.rsb_*cluster*.http-url=https://*rsbhost*:7104
<decorator>.app-service-end-point-url oms-AdvancedShipmentNotification-AppServiceDecorator.app-service-end-point-url	**https**://*rsbhost*:**7102**/AdvancedShipmentNotificationBean/AdvancedShipmentNotificationService

3. Set the port in edge-app-container.<app>.connection-url property to point https port or override protocol with https in property global.app-service-end-point-url-pattern to apply pattern at global level in case all the services are secured with policyA for an app, by default its http.

   The following table lists the various properties and their example values

Property	Value (Illustration)
edge-app-container.<app>.connection-url	t3://<hostname>:<httpsport>
edge-app-container.sim.connection-url	t3s://rsbhost:8102
global.app-service-end-point-url-pattern (The pattern of edge service URLs. Note: This is different if the service is hosted on glassfish Vs WebLogic)	http://<HTTP_HOSTNAME>:<HTTP_PORT>/<SERVICE_NAME>Bean/<SERVICE_NAME>Service https://<HTTP_HOSTNAME>:<HTTP_PORT>/<SERVICE_NAME>Bean/<SERVICE_NAME>Service

4. Security Configuration: Download edge app service WSDL files.

```
cd rsb-home/service-assembly-home/bin
download-app-service-wsdl.sh
```

5. Create Policy Mapping File: Create security policy mapping file.

```
generate-rsb-decorator-security-config.sh
```

Additional steps for Policy B configuration

If RSB is configured with Policy B, perform the following additional steps:

1. Security Configuration: Download edge app web service WSDL files.

```
cd rsb-home/service-assembly-home/bin
download-app-service-wsdl.sh
```

2. Create Policy Mapping File: Create security policy mapping file

```
generate-rsb-decorator-security-config.sh
```

3. Setup Security Credentials: Setup security credentials for Message Protection.

```
setup-message-protection-security-credentials.sh
```

Compilation

Setup security credentials and compile:

```
cd rsb-home/service-assembly-home/bin
rsb-compiler.sh-setup-security-credential
```

During the compilation step, credentials need to be provided for the following aliases.

- sidb-jdbc-user-alias
- admin-server-user-alias

Example:

Alias Name	Value (Illustration)
sidb-jdbc-user-alias	*<soainfra schema>*
admin-server-user-alias	*<weblogic user>*

The -setup-security-credential option creates or updates the wallet file in *deployment-home/conf/security* folder. The wallet file contains userids and passwords in encrypted form. However it is possible to decrypt the information programmatically by anyone who has access to this file. Hence it is a good idea to lock down this folder from unauthorized users. You may use the following command to remove read access to this folder:

```
chmod 700 rsb-home/deployment-home/conf/security
```

Note: If the security credentials are already setup for the above aliases (in a previous compilation attempt), compilation can be directly carried out as follows:

cd rsb-home/service-assembly-home/bin

```
rsb-compiler.sh
```

Deployment

1. Start Admin Server, Proxy Server and Managed servers:

   ```
   cd <domainHome>/bin
   startManagedWebLogic.sh
   <managed server>
   <AdminServer URL>
   ```
   For example:

   ```
   startManagedWebLogic.sh "qa_test_managedServer_1" "http://rsbhost:17001"
   ```
2. Prepare instrumentation configurations for WebLogic server.

   ```
   cd rsb-home/deployment-home/bin
   rsb-deployer.sh -prepare-wls
   ```
   If RSB is configured with Policy B, perform the following steps before proceeding further. For unsecured configuration or RSB configuration with Policy A, move directly to Step 3.

   a. Copy Script: Copy security scripts to RSB server

      ```
      cd rsb-home/integration-lib/rsb-tools/scripts
      scp generate-pki-certificate-keystore-for-osb.sh
      <user>@<host>:/<domainHome>/config/
      scp import-remote-server-public-key-certificate-into-keystore.sh
      <user>@<host>:/<domainHome>/config/
      scp export-server-public-key-certificate-from-keystore.sh
      <user>@<host>:/<domainHome>/config/
      ```
   b. Generate Certs and Key store: Generate private key, public key and key store for the RSB server (To be done in the RSB server).

      `<domainHome>/bin/setDomainEnv.sh` (This command must be run in the current shell. Prefix the command with a period and a space character)

      ```
      cd <domainHome>/config
      generate-pki-certificate-keystore-for-osb.sh
      ```

You will be asked for a keystore password and private key password. Please note the passwords. You will have to provide the same passwords in subsequent steps.

Note: If you are getting the certificate from a CA, do not run the above command. Instead, create a keystore with the name **<hostname>-keystore.jks** where hostname is the short hostname of the server (output of *hostname -s* command) and then import the certificate and key (public key and private key) to the key store. You may use the following command to import to the keystore.

For more information on RSB Policy Configuration, refer to the *Oracle Retail Service Backbone Security Guide*.

```
java utils.ImportPrivateKey -certfile <certificate file> -keyfile <private
key file> -keyfilepass <private key password> -keystore
<hostname>-keystore.jks -storepass <keystore password> -alias
<hostname>-public-private-key-alias -keypass <private key password>
```

c. Copy app server certificate(s)

Copy edge app certificate file(s) to *<domainHome>/config* of the RSB server. The file name must be *<remote-host>-certificate.der*

Note: See RSB Security Guide for instructions to export certificate from edge app server.

d. Import app server certificate(s):

Import all the edge app server public key certificates to RSB server's keystore. If the edge apps are deployed in different servers, import all the certificates to the keystore (To be done in the RSB server):

```
cd <domainHome>/config
import-remote-server-public-key-certificate-into-keystore.sh <app>
<remote-host>
```

For example:

```
import-remote-server-public-key-certificate-into-keystore.sh cm <hostname>
```

For the keystore password, provide the password you specified in the step b.

e. Configure RSB Server: Configure the RSB server to use the key store generate in the previous steps.

```
cd rsb-home/deployment-home/bin
configure-rsb-app-server-for-security-policy-b.sh
```

For the keystore password and private key password, provide the passwords you specified in the step ii.

f. Restart Servers: Restart Admin and Managed Servers

3. Deploy all the decorators using one of the methods below:

- Deploy one decorator at a time.

```
cd rsb-home/deployment-home/bin
rsb-deployer.sh -deploy-rsb-service <OSB Project jar>
```

For example, rsb-deployer.sh -deploy-rsb-service igs-ASNInPublishing-AppServiceDecorator.jar

- Deploy all the decorators of an app at a time.

```
cd rsb-home/deployment-home/bin
rsb-deployer.sh -deploy-all-rsb-service-for-app <appName>
```

For example, rsb-deployer.sh -deploy-all-rsb-service-for-app igs

- Deploy all the decorators of all apps in scope at a time.

```
cd rsb-home/deployment-home/bin
rsb-deployer.sh -deploy-all-rsb-service
```

4. Deploy rib4oms injector service

```
cd rsb-home/deployment-home/bin
rsb-deployer.sh -deploy-rsb-service
RibOmsToRsbOmsRouting-ServicesIntegrationFlow.jar
```

5. If RSB policy B is configured, perform the following step else jump to Step 6:

   Export Certificate: Copy the script from integration-lib. Export the certificate, so that it can be used by the service consumers. (To be done in the RSB server).

```
cd <wlsHome>/config

export-server-public-key-certificate-from-keystore.sh
```

6. Restrict access to the $RSB-HOME folder:

```
cd $RSB-HOME
chmod -R 700 .
```

7. Restart all the servers i.e. Admin Server, managed servers and proxy server.

Note: By default the maximum number of in-memory sessions for WebLogic web applications is unlimited. This setting can be misused by external attackers to create unlimited number of sessions by accessing the web application. In such cases it is possible that the WebLogic server run out of memory and eventually crash. So it is required to limit the number of sessions to a reasonable number (e.g., 100). The settings can be changed through the admin console of the WebLogic server. Follow the steps below to change this configuration setting:

1. Login to Admin Console.
2. Click **Deployments**.
3. Expand the rsb-admin-<version>.ear deployment. Click on the **rsb-admin** module.
4. Click **Configuration**.
5. Set Maximum in-memory Sessions to 100.
6. Save the changes. Activate the session, if needed.

How to Deploy and Configure RCE Decorators

RCE decorators have built-in transformation of messages that allows integration of micros Customer Engagement app with Retail Extension Modules (RXM) application. This section describes how to install RCE decorators using the rsb-home toolset.

For non-secured installations: (for implementation OR early test environments only)

Prerequisite: A valid rsb-home.

Installation Steps

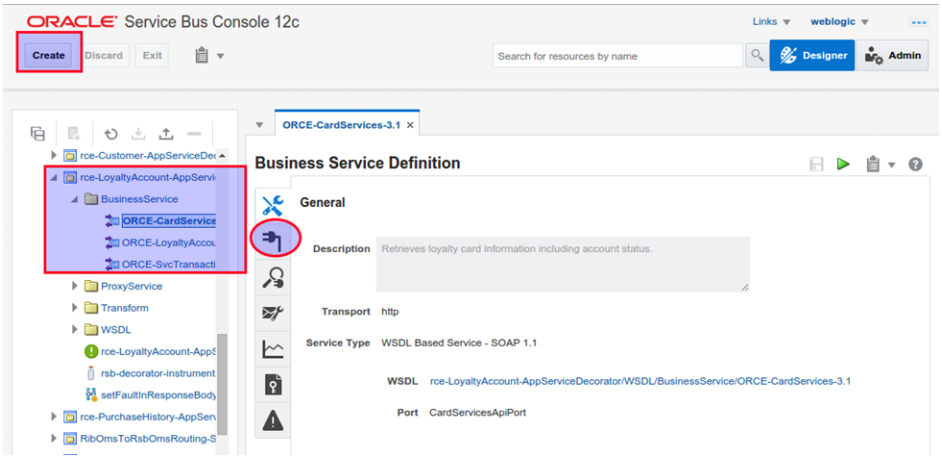
1. Download RsbAppServiceDecoratorPakWithTransform<$current_version>ForRce<$current_version>_eng_ga.zip into rsb-home/download-home/all-app-service-decorator

2. Delete the base decorator (with NO transformations) RsbAppServiceDecoratorPak<$current_version>ForRce<$current_version>_eng_ga.zip if that exists under rsb-home/download-home/all-app-service-decorator
3. Run all life cycle management scripts in rsb-home listed below
   - rsb-home/download-home/bin/check-version-and-unpack.sh
   - rsb-home/service-assembly-home/bin/download-app-service-wsdl.sh
   - rsb-home/service-assembly-home/bin/rsb-compiler.sh
   - rsb-home/deployment-home/bin/rsb-deployer.sh -deploy-all-rsb-service-for-app rce

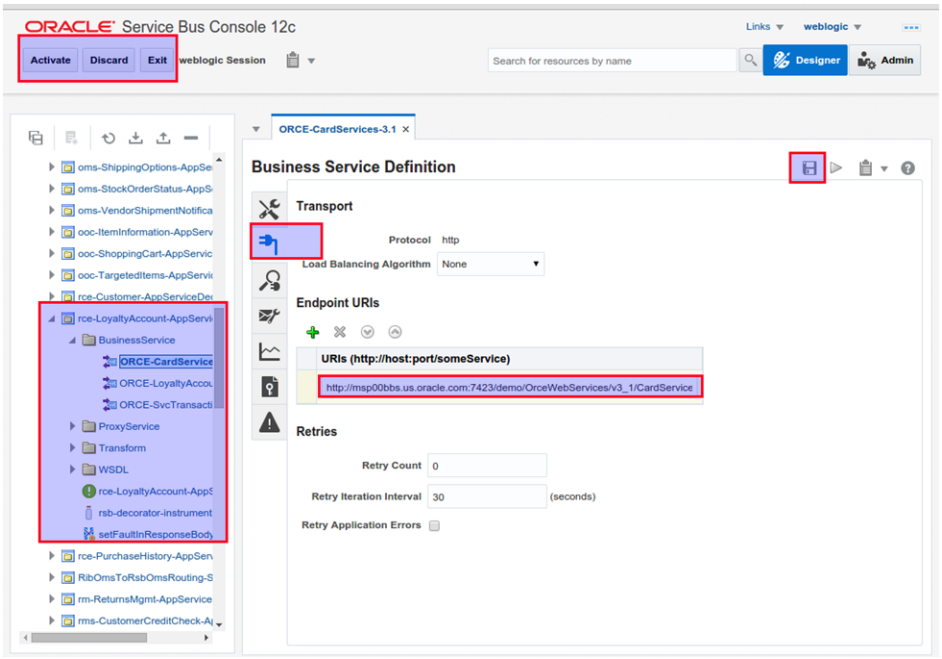
Post-Installation Steps

Some transformation enabled RCE decorators have multiple business service components inside a single decorator service. We need to manually update the end-point URL's for these decorators.

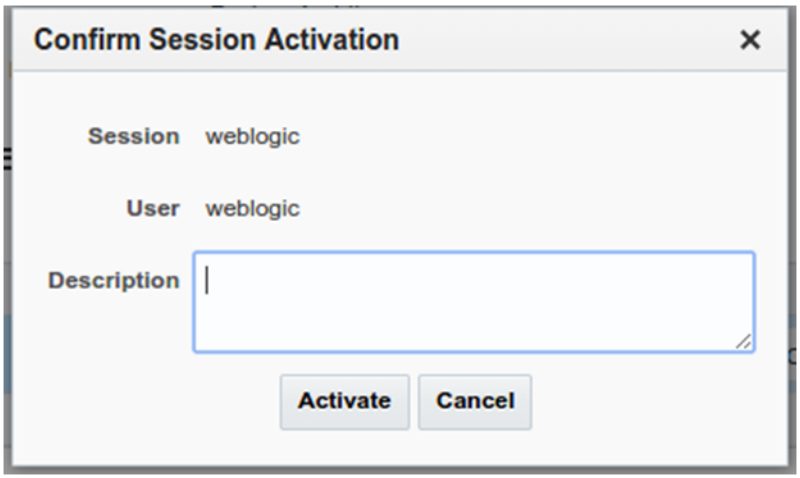
1. Login to SbConsole as Weblogic administrator
2. Identify the below decorators from navigation bar and perform steps 3 to for each of them.
   - rce-GiftList-AppServiceDecorator
   - rce-LoyaltyAccount-AppServiceDecorator
3. Create a Session, drill down to rce-LoyaltyAccount-AppServiceDecorator ORCE-CardServices Businesss Services as shown below



4. Go to Transport tab, Edit the End Point URL to be http://<HTTP_HOSTNAME>:<HTTP_PORT>/demo/OrceWebServices/v3_1/CardServicesApiService



5. Click on Save button then Activate the Session



6. Repeat steps 3 to 5 for ORCE-SvcTransactionServices in LoyaltyAccount decorator, with end point URL as in the Business Service to End Point URL mapping table.
7. Repeat steps 3 to 5 for ORCE-RegistryServices in GiftList decorator, with end point URL as in the Business Service to End Point URL mapping table.

Business Service to End Point URL Mapping

Decorator	Business Service	End point URL
rce-GiftList-AppServiceDecorator	ORCE-RegistryServices	<http_OR_https>://<HTTP_HOSTNAME>:<HTTP_PORT>/demo/OrceWebServices/v3_0/RegistryServicesApiService

Decorator	Business Service	End point URL
rce-LoyaltyAccount-AppServiceDecorator	ORCE-CardServices	<http_OR_https>://<HTTP_HOSTNAME>:<HTTP_PORT>/demo/OrceWebServices/v3_1/CardServicesApiService
rce-LoyaltyAccount-AppServiceDecorator	ORCE-SvcTransactionServices	<http_OR_https>://<HTTP_HOSTNAME>:<HTTP_PORT>/demo/OrceWebServices/v3_1/SvcTransactionServicesApiService

For Secured Installations (Policy-A)

For Policy-A services, there are a few required manual steps.

Prequisites

- A valid rsb-home, from where other secured decorator services have already been deployed. Remove rce from app-in-scope when installing other secured decorator services.
- SSL enabled WebLogic servers for RSB

Installation Steps

1. Download RsbAppServiceDecoratorPakWithTransform<$current_version>ForRce<$current_version>_eng_ga.zip into rsb-home/download-home/all-app-service-decorator
2. Delete the base decorator (with NO transformations) RsbAppServiceDecoratorPak<$current_version>ForRce<$current_version>_eng_ga.zip if that exists under rsb-home/download-home/all-app-service-decorator
3. Add rce back to app-in-scope list as service provider

   ```
   rsb-deployment-env-info.service-provider-app-in-scope-for-integration=rce
   rsb-deployment-env-info.service-requester-app-in-scope-for-integration=rxm
   ```
4. Run rsb-home/download-home/bin/check-version-and-unpack.sh
5. Do NOT run the generate-rsb-decorator-security-config.sh, instead find the file rsb-home/service-assembly-home/service-policy-config/output/decorator-service-proxy-security-policy/service-name-to-policy-id-map.properties

Note: This manual step is required because the edge app RCE uses a custom security policy (non-Policy-A) but RSB decorator needs to be secured with Policy-A. To handle this special case of mismatch in security policies between the decorator proxy service (Policy-A) and the edge-app service (custom security policy), we need to manually update the file.

service-name-to-policy-id-map.properties would exist if there were other secured decorators compiled previously, if the file does not exist the create a new file and copy the below configurations into that file.

```
service-provider.rce-CustomerService=owsm,policyA
service-provider.rce-Customer-AppServiceDecorator/ProxyService/Cust
omerAppServiceProxy=owsm,policyA
service-consumer.rce-Customer-AppServiceDecorator/ProxyService/Cust
omerAppServiceProxy=owsm,policyA
service-consumer.rce-Customer-AppServiceDecorator/BusinessService/C
ustomerAppServiceBiz=owsm,policyA
service-provider.rce-GiftListService=owsm,policyA
service-provider.rce-GiftList-AppServiceDecorator/ProxyService/Gift
ListAppServiceProxy=owsm,policyA
service-consumer.rce-GiftList-AppServiceDecorator/ProxyService/Gift
ListAppServiceProxy=owsm,policyA
service-consumer.rce-GiftList-AppServiceDecorator/BusinessService/G
iftListAppServiceBiz=owsm,policyA
service-provider.rce-LoyaltyAccountService=owsm,policyA
service-provider.rce-LoyaltyAccount-AppServiceDecorator/ProxyServic
e/LoyaltyAccountAppServiceProxy=owsm,policyA
service-consumer.rce-LoyaltyAccount-AppServiceDecorator/ProxyServic
e/LoyaltyAccountAppServiceProxy=owsm,policyA
service-consumer.rce-LoyaltyAccount-AppServiceDecorator/BusinessSer
vice/LoyaltyAccountAppServiceBiz=owsm,policyA
service-provider.rce-PurchaseHistoryService=owsm,policyA
service-provider.rce-PurchaseHistory-AppServiceDecorator/ProxyServi
ce/PurchaseHistoryAppServiceProxy=owsm,policyA
service-consumer.rce-PurchaseHistory-AppServiceDecorator/ProxyServi
ce/PurchaseHistoryAppServiceProxy=owsm,policyA
service-consumer.rce-PurchaseHistory-AppServiceDecorator/BusinessSe
rvice/PurchaseHistoryAppServiceBiz=owsm,policyA
```

6. Run rsb-home/service-assembly-home/bin/rsb-compiler.sh
7. Run rsb-home/deployment-home/bin/rsb-deployer.sh -deploy-all-rsb-service-for-app rce

Post-Installation Steps

1. Refer to Post-Installation steps and update all the Business service end point URL's with relevant URL's as described in the Business Service to End Point URL mapping table.
2. For Rce Decorators with security setup(proprietary in RCE and Policy-A in RSB), Weblogic requires an additional JAVA_OPTIONS. Locate setDomainEnv.sh file in the RSBDomain and add -Dcom.bea.wli.sb.transports.http.GetHttpAuthorizationHeaderAllowed=true

Note: This is required because RCE uses proprietary security headers that the client has to pass in and OSB/RSB has to copy and forward those proprietary headers in the SOAP call to AppService.

3. Restart the WebLogic servers.

RIC Modes

The following table shows different RIC modes:

Table 6–1

Supported Modes	Description	When to use?	Settings in the deployment file
RSB ONLY	RIC is configured to collect and display only RSB data.	If RSB is in-scope for your integration and not RIB.	"ribEnable":"false", "rsbEnable":"true", "ddiEnable":"true",
DUAL (RIB+RSB)	RIC is configured to collect and display both RIB and RSB data.	If both RIB and RSB are in-scope for your integration.	"ribEnable":"true", "rsbEnable":"true", "ddiEnable":"true",
RIB ONLY	RIC is configured to collect and display only RIB data.	If RIB is in-scope for your integration and not RSB.	"ribEnable":"true", "rsbEnable":"false", "ddiEnable":"true",

How to decide which mode should RIC run on?

Retailer's site specific integration topology must drive this decision. RIC can be installed in DUAL mode if you have a valid rib-home with jms-console and rsb-home on same machine. This configuration yields maximum visibility of Integration system and is our recommended mode. When only service oriented integration (RSB) is used then, one must configure RIC with RSB_ONLY mode.

DDI is enabled by default in all RIC modes, irrespective of the value of ddiEnable flag in the configuration file. The value of the properties ribEnable and rsbEnable in the ric configuration file ric-deployment-env-info.json inside ric-home/conf/ folder decides RIC mode.

Note: For more information, see the *Oracle Retail Integration Bus Implementation Guide* and the *RIC User Guide*.

Installation of RIC in different modes

After configuring RIC follow the installation steps according to the selected RIC mode.

RIB only Mode

RIC can be installed in RIB only mode to provide visibility into RIB.

Pre-requisites

1. RIB must be deployed.

2. JMS-Console must be deployed from rib-home/tools-home/.
3. rib-home must be accessible to ric-home, in other words both reside in the same file system.

RIC can be deployed in RIB_Only mode with the following steps:

1. Download RicKernel16.0.2ForAll16.x.xApps_eng_ga.zip to a location (for example - RIC-APP-BUILDER) on the computer which has your rib-home.
2. Edit the configuration file ric-deployment-env-info.json inside ric-home/conf/ folder.
3. Modify the MiddlewareServerDef and IntegrationProduct with information that is specific to your environment.
   - Set the value of ribEnable property in the configuration file to true.
   - Set the value of ribHome property in the configuration file to point to rib-home.
4. Set the value of RicAppServer fields to point to the environment where you want to deploy RIC.
5. Go to the ric-home/bin/ folder, run the compiler to update the RIC ear as follows:

   ```
   $ sh ric-app-compiler.sh -setup-credentials
   ```
   When prompted by the compiler, enter the user name and password for weblogic server and RIC admin user, the RIC admin user will be used to log in RIC.
6. From the same folder, run the deployer script to create the user and group and deploy RIC on your weblogic server as follows:

   ```
   $ sh ric-app-deployer.sh -deploy-ric-app
   ```
7. Restrict access to the $RIC-HOME folder:

   ```
   cd $RIC-HOME
   chmod -R 700 .
   ```
8. Restart the WebLogic server.

RSB only Mode

RIC can be installed in RSB only mode to provide RSB visibility if you have a valid rsb-home, with the following steps:

> **Note:** RIB is already installed then we recommend configuring DUAL mode, which will provide visibility into both RIB and RSB systems.

1. Download RicKernel16.0.2ForAll16.x.xApps_eng_ga.zip to a location (for example - RIC-APP-BUILDER) on the computer which has your rsb-home.
2. Edit the configuration file ric-deployment-env-info.json inside ric-home/conf/ folder.
3. Modify the DataSourceDef, MiddlewareServerDef and IntegrationProduct with information that is specific to your environment.
   - set the value of rsbEnable property in the configuration file to true.
   - set the value of rsbHome property in the configuration file to point to rsb-home.

- set the value of RicDataSource : jdbcUrl property same as service-infrastructure-db.jdbc-url property in rsb-home/deployment-home/conf/rsb-deployment-env-info.properties.
- set the value of RicAppServer fields to point to the environment where you want to deploy RIC.

> **Note:** RicDataSource and RsbDataSource should point to the same database schema.

4. Go to the ric-home/bin/ folder, run the compiler to update the RIC ear as follows:

```
$ sh ric-app-compiler.sh -setup-credentials
```

When prompted by the compiler, enter the user name and password for the WebLogic server, RicDataSource and RIC admin user, the RIC admin user will be used to log in RIC.

> **Note:** If the DISPLAY environment variable is set but no XWindow is running, the RIC compiler will fail. As a workaround, run this command before running compiling:
>
> ```
> unset DISPLAY
> ```

5. Run the deployer script to deploy RIC and create the user and group on your WebLogic server from the same folder as follows:

```
$ sh ric-app-deployer.sh -deploy-ric-app
```

6. Restrict access to the $RIC-HOME folder:

```
cd $RIC-HOME
chmod -R 700 .
```

7. Restart the WebLogic server.

DUAL Mode (RIB and RSB)

RIC can be installed in DUAL mode to provide visibility into both RIB and RSB.

Prerequisites

- RIB must be deployed.
- JMS-Console must be deployed from rib-home/tools-home/.
- RSB must be deployed.
- rib-home and rsb-home must be accessible to ric-home. rib-home and rsb-home (or copies of them) must reside in the same machine as ric-home.

RIC can be deployed in DUAL mode with the following steps:

1. Download RicKernel16.0.2ForAll16.x.xApps_eng_ga.zip to a location (for example - RIC-APP-BUILDER) on your computer which has your rib-home and rsb-home.
2. Edit the configuration file ric-deployment-env-info.json inside ric-home/conf/ folder.

> **Note:** Although users can deploy RIC in any domain, for dual mode it is recommended to deploy RIC in the RSB domain.

3. Modify the DataSourceDef, MiddlewareServerDef and IntegrationProduct with information that is specific to your environment.
   - set the value of ribEnable and rsbEnable property in the configuration file to true.
   - set the value of ribHome property in the configuration file to point to your rib-home.
   - set the value of rsbHome property in the configuration file to point to your rsb-home.
   - set the value of ddiHome property in the configuration file to point to rsb-home.
   - set the value of RicDataSource : jdbcUrl property same as service-infrastructure-db.jdbc-url property in rsb-home/deployment-home/conf/rsb-deployment-env-info.properties.
   - set the value of RicAppServer fields to point to the environment where you want to deploy RIC.

   Note: RicDataSource and RsbDataSource should point to the same database schema.

4. Go to the ric-home/bin/ folder, run the compiler to update the RIC ear as follows:

   ```
   $ sh ric-app-compiler.sh -setup-credentials
   ```

   When prompted by the compiler, enter the user name and password for the WebLogic server, RicDataSource and RIC admin user, the RIC admin user will be used to log in RIC.

   Note: If the DISPLAY environment variable is set but no XWindow is running, the RIC compiler will fail. As a workaround, run this command before running compiling:

   ```
   unset DISPLAY
   ```

5. Run the deployer script to deploy RIC and create the user and group on your WebLogic server from the same folder as follows:

   ```
   $ sh ric-app-deployer.sh -deploy-ric-app
   ```

6. Restrict access to the $RIC-HOME folder:

   ```
   cd $RIC-HOME
   chmod -R 700 .
   ```

7. Restart the WebLogic server.

7

Install JSIT

JSIT is a tool that can help to mock the behavior of retail applications. JSIT can be used to validate the installation of RSB, in the absence of edge applications. This is an optional step, only needed when one or more real oracle retail edge application is not ready at the time of RSB installation. Later, when the applications are ready, modify the service endpoints in the RSB configuration file (*rsb-deployment-env-info.properties*), recompile RSB and redeploy RSB decorators.

Download and Prepare SIT

1. Download and save javaee-service-interface-tester-<version>.ear in an install stage folder, which will be referred to here as SIT_JAVAEE_APP_HOME.
2. Download and save RSE generated JavaEE ejb-jar (<app>-service-ejb.jar) in SIT_JAVAEE_APP_HOME. <app> is the application name that hosts the application service. e.g., rms-service-ejb.jar. The <app>-service-ejb.jar can be found inside the RsbServiceIntegration Paks, for example:

   RsbServiceIntegrationPak16.0.2For<app>16.0.2_eng_ga.zip\<app>-app-service-contract\service-provider\generated-output\deployable-component\<app>_JavaEEServiceProvider.zip\<app>-service-ejb.jar

   Merge the two components:

   jar -uvf javaee-service-interface-tester-<version>.ear <app>-service-ejb.jar

   Note: Multiple applications can be hosted on JSIT.

   For example:

   jar uvf javaee-service-interface-tester-<version>.ear rms-service-ejb.jar ooc-service-ejb.jar oms-service-ejb.jar

Deploy javaee-service-interface-tester-<version>.ear to Glassfish

1. Open Glassfish (JavaEE 6) Application Service console.

   For example:

   http://localhost:4848/
2. Deploy javaee-service-interface-tester-<version>.ear.

   Your web browser --> Glassfish AdminConsole --> Application --> Deploy --> Browse to **javaee-service-interface-tester-<version>.ear**
3. Click **Deploy**.

Deploy SIT to WebLogic 12c

1. Open WebLogic 12c Console.
   a. Deploy javaee-service-interface-tester-<version>.ear.

      Your Web Browser --> WebLogic AdminConsole --> Deployments --> Deploy --> Browse to **javaee-service-interface-tester-<version>.ear**

   b. Click **Deploy**.

      Note: Please do not change the default application name. It should be kept as *javaee-service-interface-tester-<version>.ear*.

      If run into any DERB jar error, add derby.jar into weblogic startup classpath. To do this edit the commEnv.sh script in WLS and add the derby.jar to DERBY_CLIENT_CLASSPATH variable.

      For example, DERBY_CLIENT_CLASSPATH="${DERBY_HOME}/lib/derby.jar:${DERBY_HOME}/lib/derbyclient.jar"

      ---

   c. Create a new user for JSIT:

      - click on **Security Realms**

      - click on **myrealm**

      - click on **Users and Groups**

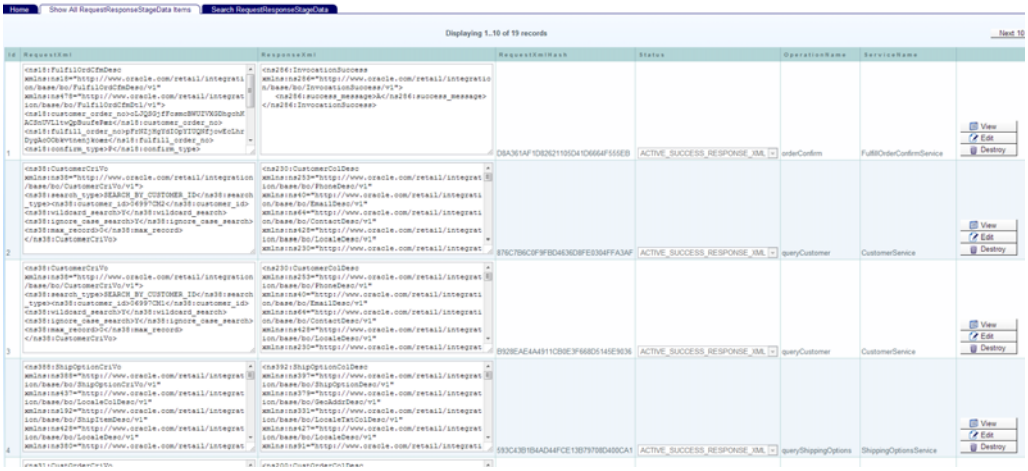
      - create a new group called "sitadmin"

      - create a new user. Add this new user to the sitadmin group.

   d. Bounce the managed server where JSIT is deployed.

Verify JSIT

JSIT Installation can be verified by browsing the URL **http://<hostname>:<port>/javaee-service-interface-tester-web**. You should be able to see the following screens if the installation is successful.


Home
Show All RequestResponseStageData Items
Search RequestResponseStageData
Displaying 1..10 of 19 records
Next 10
Id
RequestXml
ResponseXml
RequestXmlHash
Status
OperationName
ServiceName
ACTIVE_SUCCESS_RESPONSE_XML
orderConfirm
FulfillOrderConfirmService
queryCustomer
CustomerService
queryShippingOptions
ShippingOptionsService
View
Edit
Destroy

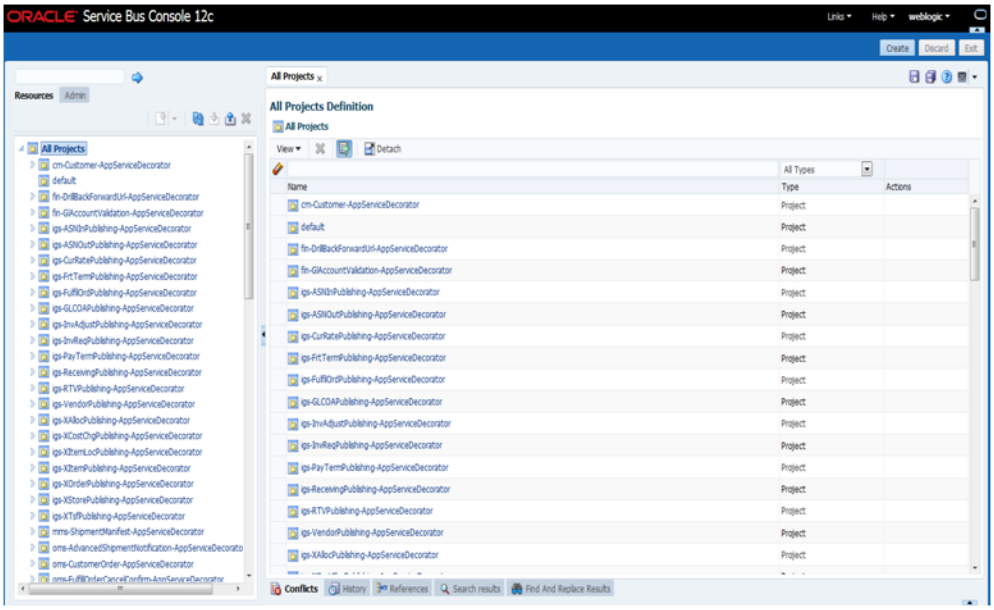
8

Post Installation Tasks

Verification using Oracle Service Bus Console

Once Deployement process is completed and decorators deployed can also be verified using weblogic test client Oracle Service Bus (OSB) console.

Open the link: http://hostname:port/sbconsole, where hostname and port are of weblogic Admin Server. All decorators are visible on Resources tab of Oracle Service Bus (OSB) Console.



Verification using Retail Integration Console

Once the deployment process is completed and all the servers are restarted, verify the success by accessing the Retail Integration Console (RIC)

Open the link: *http://hostname:port/rsb-admin*, where hostname and port are specific to the RIC deployment server.

Check if all the tabs are opening without error.

Common Issues

- -bash: sqlplus command not found

  Solution: sqlplus command should be run on machine where Oracle database is installed.

  Set Oracle Database Home directory path in a variable say ORACLE_HOME and export ORACLE_HOME/bin in the classpath. To add entries into path perform the following steps:

  ```
  ORACLE_HOME= /u00/oracle/app/oracle/product/12.1/dbhome_1

  export ORACLE_HOME

  PATH=$PATH:$ORACLE_HOME/bin

  export PATH
  ```

- Decorators not getting deployed in unsecured environment.

  Solution: OWSM is required even in non-secure deployment. Make sure that OWSM is configured for WebLogic domain where decorators are being deployed. User must make sure that Oracle Service Bus OWSM Extension is selected while WebLogic domain is created/extended.

- Admin app was showing the error *"Could not initialize class au.awt.GraphicsEnvironment*" or web browser stuck in refresh loop after logging in.

  Solution: Issue can be resolved by setting the variable *java.awt.headless* to true.

  (-Djava.awt.headless=true)

A

Appendix: RSB Installation Checklist

Notations

- wlsHome - The home directory of WebLogic. e.g., /u00/rsb/Oracle/Middleware/Oracle_Home
- domainHome - The home directory of the domain. e.g., /u00/rsb/Oracle/Middleware/Oracle_Home/user_projects/domains/rsb_domain
- app - the application acronym. e.g., sim, rms
- HIGHLIGHTED STEPS ARE ADDITIONAL STEPS REQUIRED FOR SECURITY. INSTALLATION WILL WORK WITHOUT ENABLING THE SECURITY
- [PolicyA] - These instructions are specific to security policy A configuration
- [PolicyB] - These instructions are specific to security policy B configuration

Prerequisites

Task	Notes	Command	Example
1. [PolicyA][PolicyB] Security Prerequisite: Secure Edge App Services	RSB supports security. However, primary lifecycle steps work with/without enabling security	Refer to the document *RSB Security Guide* for securing app services	
2. Download and stage all third-party software			
3. Install JDK	Version 1.8		
4. Install WebLogic	Version 12.2.1.3		
5. Install Oracle DB server	12c		
6. Install OSB on WebLogic	Version 12.2.1.3		
7. Install RCU	Version 12.2.1.3 The repository for OSB must be created with this tool		

8. Create DB schema for OSB	Use Repository Creation Utility (RCU)	<wlsHome>/oracle_common/bin/rcu	Create schema name: RSB_SOAINFRA -Under SOA Infrastructure in RCU [PolicyA][PolicyB]Create schema name: RSB_MDS - Under Metadata Services in RCU (OWSM domain requires MDS schema)
9. Configure OSB domain [PolicyA][Policy B] Create OWSM domain Create a cluster	Choose OSB (Oracle Service Bus - 12.2.1.3.0). This will select all other required templates ADF (Oracle JRF - 12.2.1.3.0) Create AdminServer Create 1 managed server for Http Proxy Create 2 managed servers	**cd <wlsHome>/wlserver/common/bin config.sh**	rsb_domain (See *RSB Deployment Architecture.doc* in References for detailed instructions) rsb_cluster AdminServer rsb_server1 rsb_server2 [PolicyA] Note: Enable SSL for all the managed servers during creation. This can be done post creation too using WebLogic Console. **Environment** --> **Servers** --> Click on <M.Server> --> Check "**SSL Listen Port Enabled**" --> Specify the port number --> **Save** --> Activate Session
10. Install RIB (optional)	A valid RIB home is required for the deployment of RSB, if RIB is enabled.		

Recommended Port Numbers for WebLogic Servers

Each WLS Domain has a unique number in the thousands place value. It starts from 7, increments of 1	SSL or non SSL is designated by the hundredth place value	Admin Server - Tenth and Unit place value is always 01	Managed Server - covers unit and tenth place value, starting from 2 increment of 1	Example
7XXX - first domain in a machine, 8XXX - second domain in a machine, 9XXX, 10XXX, 11XXX	X0XX for non-SSL X1XX for SSL	X001 - for non SSL	X0X2, X0X3, X0X4,...X0X9,X010, X011 - for non SSL	7001 7101

X101 - for SSL	X1X2, X1X3, X1X4,...X1X9,X110, X111 - for SSL

Prepare WebLogic Server for RSB deployment

Task	Notes	Command	Example

1. Grant WebLogic permission to access credential wallet	Edit *weblogic.policy* and add the permission to access credential wallet.	**cd <wlsHome>/wlserver/server/lib**
		vi weblogic.policy
			grant codeBase "file:/u00/rsb/Oracle/Middleware/user_projects/domains/rsb_domain/-" {
			permission java.security.AllPermission;
			permission oracle.security.jps.service.credstore.CredentialAccessPermission "credstoressp.credstore", "read,write,update,delete";
			permission oracle.security.jps.service.credstore.CredentialAccessPermission "credstoressp.credstore.*", "read,write,update,delete";
			};

2. JVM heap size (Optional)	Set maximum and minimum heap size	**cd <domainHome>/bin** **vi setDomainEnv.sh**	USER_MEM_ARGS="-Xms1024m -Xmx2048m -XX:MaxPermSize=1024m"

Download

Task	Notes	Command/Example
1. Download RSB Kernel	Download *RsbKernel16.0.2ForAll16.x.xApps_eng_ga.zip* to a directory in Linux/Unix. The rsb-home will be created inside this directory. Extract the archive file.	

2. Download Decorators	Download all *RsbAppServiceDecoratorPak<rsb_major_version>For<app><app_version>_eng_ga.zip* to rsb-home/download-home/all-app-service-decorator/ directory. Do not extract the files.	
3. Download Service Flows	Download all *RsbServiceIntegrationFlowPak< rsb_major_version >For<service-name>_eng_ga.zip* to *rsb-home/download-home/all-functional-service-int-flow* directory. Do not extract the files.	
4. Set JAVA_HOME	Set JAVA_HOME to a JDK 1.8+ 64 bit with latest security updates.	**export JAVA_HOME=/usr/bin/java/1.8.0_65**
5. Check version and unpack	Run the check version and unpack script	**cd rsb-home/download-home/bin check-version-and-unpack.sh**
6. Create tablespaces with names 'RETAIL_DATA' and 'RETAIL_INDEX'	The rsb-deployer.sh script expects permanent Tablespace with correct names created as a prerequisite and will use these Tablespaces to create RSB_SOAINFRA database objects.	

Configure

Edit *rsb-home/deployment-home/conf/rsb-deployment-env-info.properties* to configure following properties:

Property	Example Value
JAVA_HOME	/usr/java/jdk1.8.0_65
rsb-osb-container.domain-name	rsb_domain
rsb-osb-container.<domain>.home	rsb-osb-container.*rsb-domain*.home =/u00/rib1/Oracle/Middleware/user_projects/domains/rsb_domain

rsb-osb-container.<domain>.cluster-name	rsb-osb-container.*rsb_domain*.cluster-name=rsb_cluster
rsb-osb-container.<domain>.<cluster name>.http-url (Cluster port is the port of http proxy server)	rsb-osb-container.*rsb_domain.rsb_cluster*.http-url=http://*rsbhost*:7004
[PolicyA] rsb-osb-container.rsb_domain.rsb_cluster.https-url (Provide the HTTPS URL of the http proxy managed server)	rsb-osb-container.*rsb_domain.rsb_cluster*.http-url=https://*rsbhost*:7104
rsb-osb-container.<domain>.admin-server-http-url	rsb-osb-container.*rsb_domain*.admin-server-http-url=http://*rsbhost*:7001
rsb-osb-container.<domain>.admin-server-connection-url	rsb-osb-container.*rsb_domain*.admin-server-connection-url=t3://*rsbhost*:7001
rsb-osb-container.<domain>.<cluster name>.managed-servers (Comma separated list of managed servers in the cluster, excluding the http proxy managed server)	rsb-osb-container.*rsb_domain.rsb_cluster*.managed-servers=rsb_server1,rsb_server2
rsb-osb-container.<domain>.<cluster name>.<managed server>.managed-server-connection-url (Repeat this property for all the managed servers in the cluster)	rsb-osb-container.*rsb_domain.rsb_cluster.rsb_server1*.managed-server-connection-url=t3://*rsbhost*:7002
service-infrastructure-db.jdbc-url	jdbc:oracle:thin:@*dbhost*:1521:rra1
edge-app-container.<app>.connection-url (the host:port of the edge application)	edge-app-container.*sim*.connection-url=t3://*edgeapphost*:8080

global.app-service-end-point-url-pattern (The pattern of edge service URLs. Note: This is different if the service is hosted on glassfish Vs WebLogic)	http://<HTTP_HOSTNAME>:<HTTP_PORT>/<SERVICE_NAME>Service/<SERVICE_NAME>Bean
rib.home.path (optional)	rib1@*ribhost*:/u00/rib1/rib2/Rib1602ForAll16xxApps/rib-home

Compile

Task	Notes	Command
1. [Policy A] [PolicyB] Security Configuration	Download edge app service WSDLs	**cd rsb-home/service-assembly-home/bin/ download-app-service-wsdl.sh**
2. [PolicyA] [PolicyB] Create Policy Mapping file	Create security policy mapping file	**generate-rsb-decorator-security-config.sh**
3. [PolicyB] Setup Credentials	Setup security credentials for Message Protection	**setup-message-protection-security-credentials.sh**
4. Setup credentials and compile	Setup the user IDs and passwords in the wallet file ■ admin-server-user-alias ■ sidb-jdbc-user-alias	**cd rsb-home/service-assembly-home/bin/ rsb-compiler.sh -setup-security-credential**
5. Compile Note: If step 4 is executed, skip this step.	Compile the configurations	**cd rsb-home/service-assembly-home/bin/ rsb-compiler.sh**

Deploy

Task	Notes	Command
1. Start the servers	Start Admin Server, Proxy Server, Managed Servers	**cd <domainHome>/bin startWeblogic.sh startManagedWebLogic.sh <managed server>**
2. Prepare WLS	Prepare instrumentation configurations for WebLogic server	**cd rsb-home/deployment-home/bin rsb-deployer.sh -prepare-wls**

3. Restart Servers	Restart all the servers (Admin + Managed servers)	
4. [PolicyB] Copy script	Copy security scripts to RSB server	**cd rsb-home/integration-lib/rsb-tools/scripts** **scp generate-pki-certificate-keystore-for-osb.sh <user>@<host>:/<domainHome>/config/** **scp import-remote-server-public-key-certificate-into-keystore.sh <user>@<host>:/<domainHome>/config/** **scp export-server-public-key-certificate-from-keystore.sh <user>@<host>:/<domainHome>/config/**
5. [PolicyB] Generate Certs and Key store	Generate private key, public key and key store for the RSB server (To be done in the RSB server) **Note**: If you are using CA certificates, do not generate certificates. Instead import the certificates to the keystore.	**. <domainHome>/bin/setDomainEnv.sh** **cd <domainHome>/config** **generate-pki-certificate-keystore-for-osb.sh**
6. [PolicyB] Copy app server certificate(s)	Go to <wlsHome>/config of the **remote** edge app server and export the public key certificate. Copy the certificate file to < wlsHome >/config of the RSB server. The file name must be <remote-host>-certificate.der	Follow RSB Security Guide for instructions to export certificate

7. [PolicyB] Import app server certificate(s)	Import all the edge app server public key certificates to RSB server's key store. If the edge apps are deployed in different servers, import all the certificates to the keystore (To be done in the RSB server)	**cd <domainHome>/config** **import-remote-server-public-key-certificate-into-keystore.sh <app> <remote-host>** e.g., **import-remote-server-public-key-certificate-into-keystore.sh cm *<hostname>***
8. [PolicyB] Configure RSB Serve	Configure the RSB server to use the key store generate in the previous steps	**cd rsb-home/deployment-home/bin** **configure-rsb-app-server-for-security-policy-b.sh**
9. [PolicyB] Restart	Restart Admin and Managed Servers	
10. Deploy Decorator	Deploy all the decorators	**cd rsb-home/deployment-home/bin** **rsb-deployer.sh -deploy-all-rsb-service**
11. Deploy Injector	Deploy rib4oms injector service	**cd rsb-home/deployment-home/bin** **rsb-deployer.sh -deploy-rsb-service RibOmsToRsbOmsRouting-ServicesIntegrationFlow.jar**
12. [PolicyB] Export OSB certificate	Copy the script from integration-lib Export the certificate, so that it can be used by the service consumers. (To be done in the RSB server)	**cd <wlsHome>/config** **export-server-public-key-certificate-from-keystore.sh**
13. Restart	Restart all the servers (Admin + Managed servers)	

B

Appendix: How to Secure Application Service (including JSIT)

Depending on the security configuration chosen for each application (i.e., Policy A or Policy B) various security related configuration changes need to be made in the application side. This must be done prior to the installation of RSB. If the security on the application side is done after RSB installation, some of the steps of RSB deployment will have to redone after the security configuration change in the edge app server. The details steps on how to secure edge app services is given in the RSB Security guide.

Note: For more information, see *RSB Security Guide*.

C

External LDAP Configuration

WebLogic ships with a default internal Light-weight Directory Access Protocol (LDAP) authentication provider. In an environment where a couple of domains exist, an administrator can set up users and groups in an internal LDAP provider and use these parameters during login and authentication. Alternatively, in an environment that contains multiple domains, managing/maintaining users and groups can be a difficult task. Oracle recommends that you use a centralized LDAP server to manage/maintain the users and groups.

This chapter describes the steps you should take to configure the Oracle Internet Directory (OID) and the Active Directory (AD) LDAP based authentication provider in WebLogic.

Introducing the Oracle Internet Directory (OID)

An online directory is a specialized database that stores and retrieves collections of information about objects. The information can represent any resources that require management, for example:

- Employee names, titles, and security credentials
- Information about partners
- Information about shared resources such as conference rooms and printers

The information in the directory is available to different clients, such as single sign-on solutions, e-mail clients, and database applications. Clients communicate with a directory server by means of the LDAP. The Oracle Internet Directory is an LDAP directory that uses an Oracle database for storage.

Introducing the Microsoft Active Directory (AD)

An Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems.

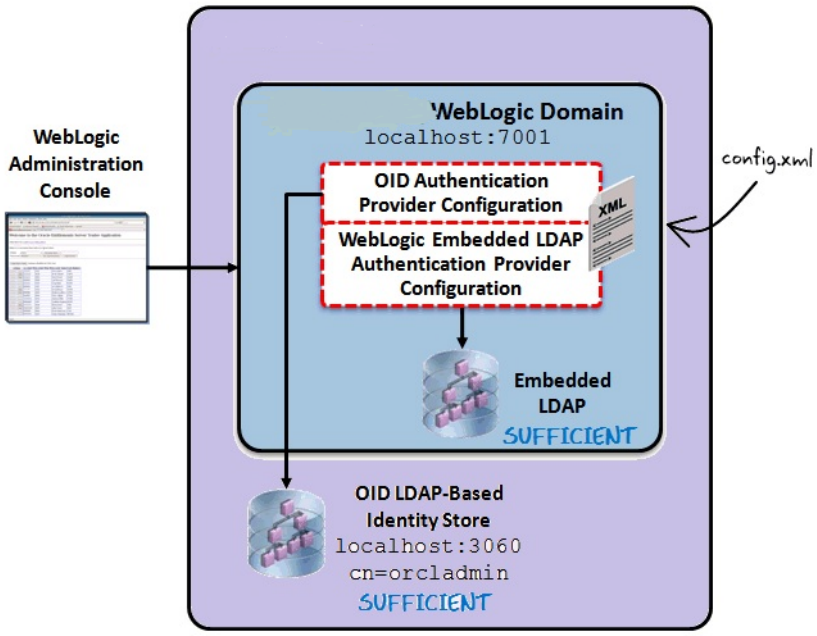
Active Directory is a special-purpose database — it is not a registry replacement. The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates. Active Directory data is hierarchical, replicated, and extensible. Because it is replicated, you do not want to store dynamic data, such as corporate stock prices or CPU performance.

In Windows 2000, Active Directory has three partitions. These are also known as naming contexts: do-main, schema, and configuration. The domain partition contains users, groups, contacts, computers, organizational units, and many other object types. Because Active Directory is extensible, you can also add your own classes and/or

attributes. The schema partition contains classes and attributes definitions. The configuration partition includes configuration data for services, partitions, and sites.

Architecture Overview

The architecture diagram describes the configuration of an OID and AD LDAP-based authentication provider used by applications deployed in an WebLogic server environment.



The diagram displays a sample environment and consists of the following:

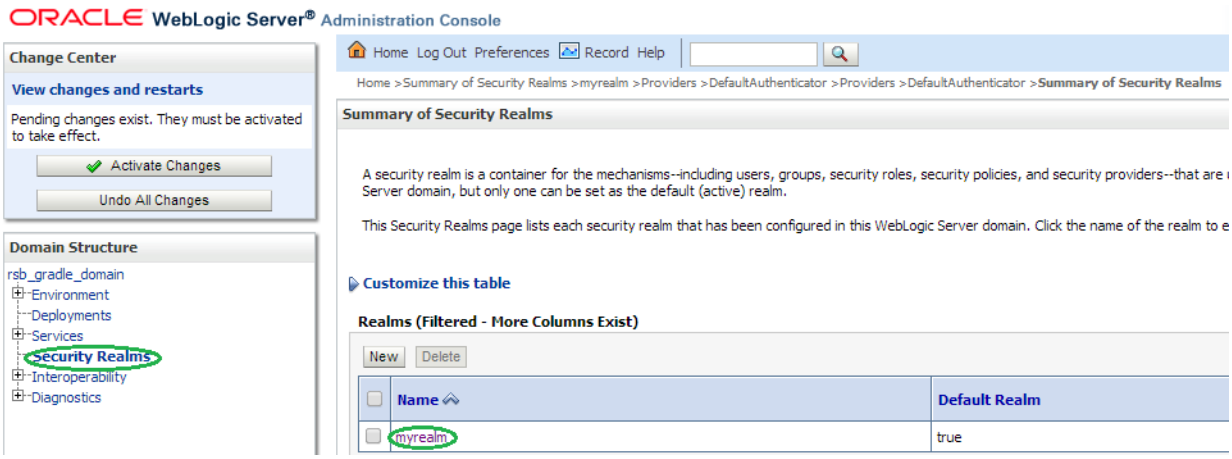
- The WebLogic Server running on port 7001
- The WebLogic Administration Console used to configure authentication providers
- The WebLogic Embedded LDAP server with a control flag setting of SUFFICIENT
- An OID LDAP-based identity store running on port 3060 with a control flag setting of SUFFI-CIENT
- The WebLogic config.xml that stores the authentication provider configuration

By default, the WebLogic server uses a security realm with the name “myrealm” that uses an embedded LDAP server (two default users WebLogic & OracleSystemUser) that acts as data store for Authentication, Authorization, Credential Mapping and Role Mapping Provider.

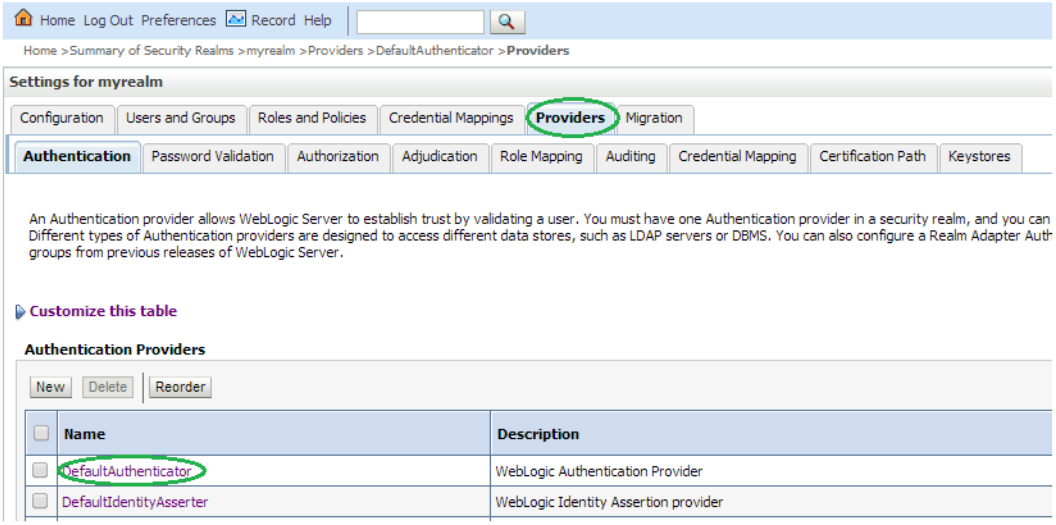
Configuring the Oracle Internet Directory (OID) as an Authentication Provider in WebLogic

To configure the OID as an authentication provider in WebLogic, take the following steps:

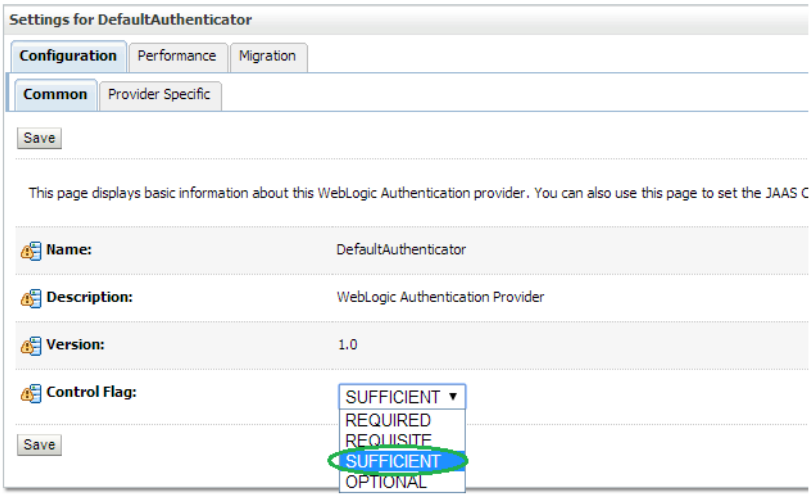
1. Login to **WebLogic Console -> Security Realm -> myrealm**.



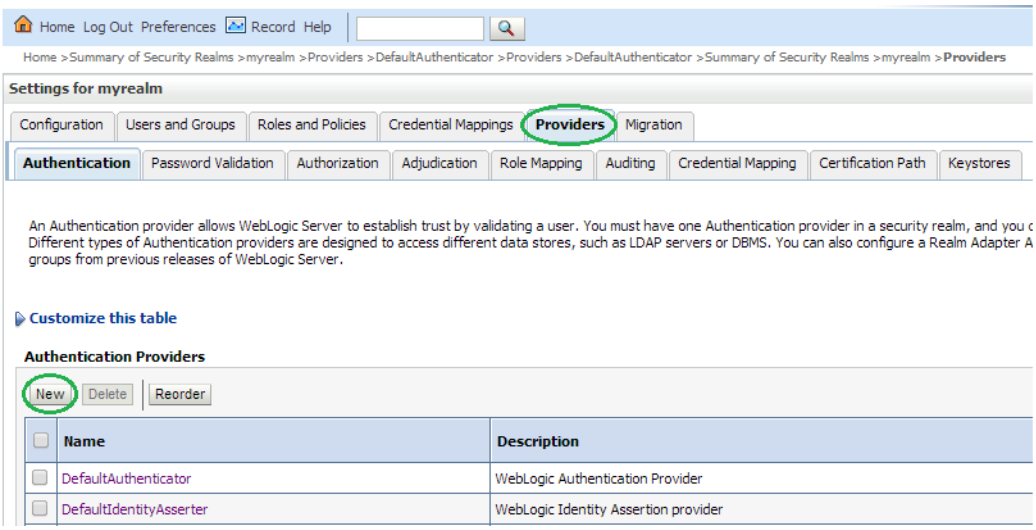
2. Select tab **Providers -> Authentication -> Default Provider (DefaultAuthenticator)**.



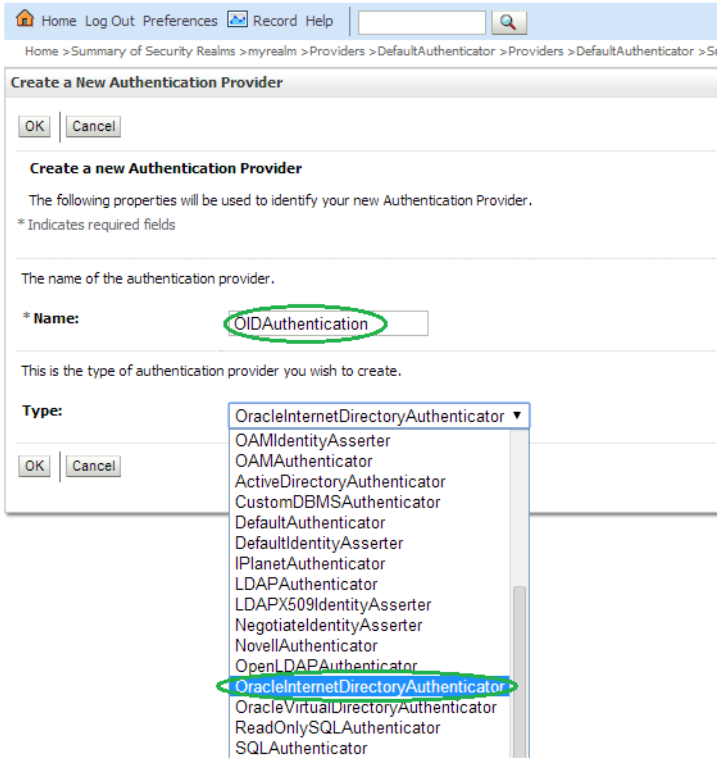
3. Change the **Control Flag** (JAAS Flag) parameter from REQUIRED to SUFFICIENT and click **Save**.



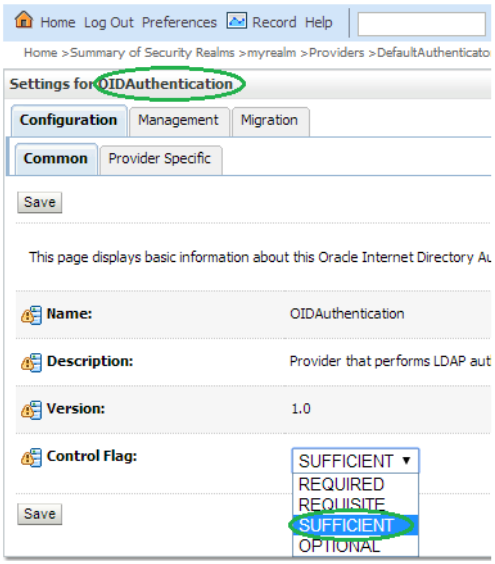
4. Click **New** to add a new Authentication Provider.



5. Enter OIDAuthentication as the **Name** of the new provider. Select OracleInternetDirectoryAuthenticator as **Type** and then click **OK**.



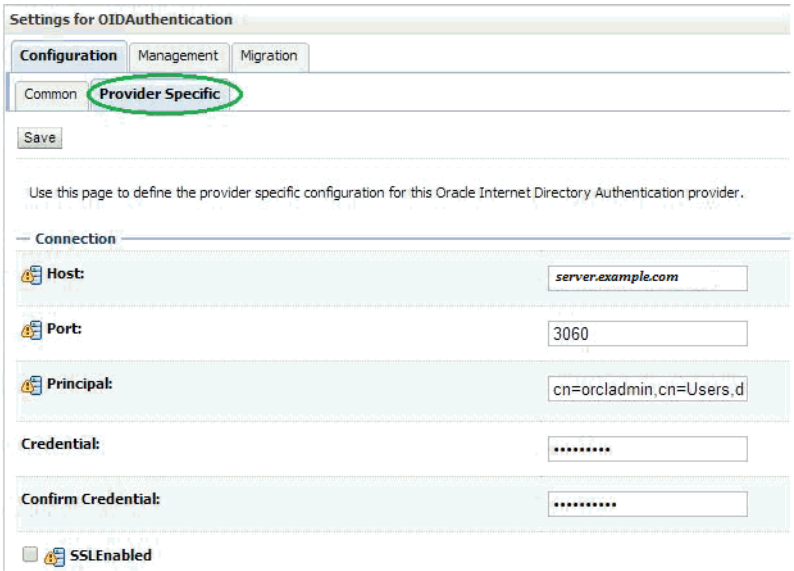
6. Change the **Control Flag** to SUFFICIENT for the OIDAuthentication Provider added and click **Save**.



7. Select the **Provider Specific** tab and enter your OID server details.

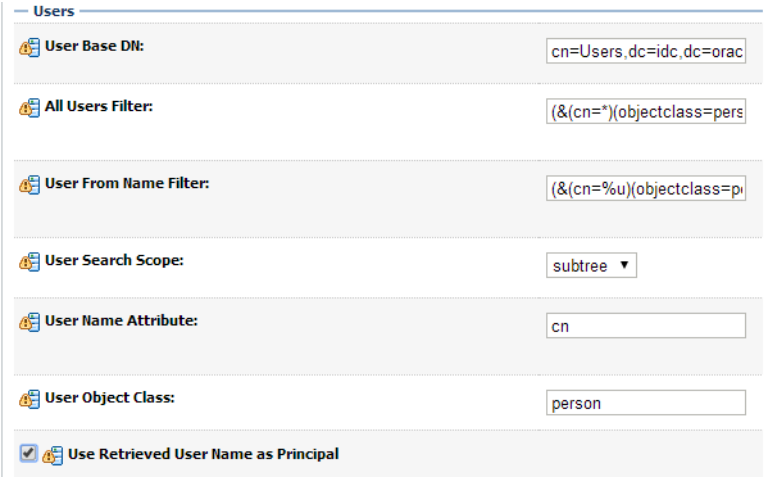
   a. The first section contains the Connection settings for the OID server. Use the appropriate values based on where the OID is hosted and the credentials:

Name	Value	Purpose
Host:	server.example.com	The OID host name
Port:	3060	The standard OID listening port
Principal:	cn=orcladmin,cn=Users,dc=idc,dc=oracle,dc=com	The LDAP user that logs into OID on behalf of your authentication provider
Credentials:		Password for the principal user
Confirm Credentials:		Confirmation of the password
SSL Enabled:	Unchecked	Enables or disables SSL connectivity



b. The second section contains the Users settings for the OID provider. Use appropriate values:

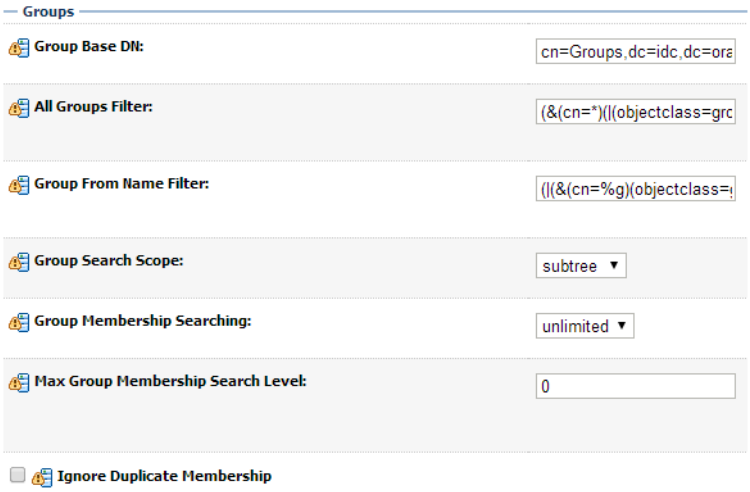
Name	Value	Purpose
User Base DN:	cn=Users,dc=idc,dc=oracle,dc=com	The root (base DN) of the LDAP tree where searches are performed for user data
All Users Filter:	(&(cn=*)(objectclass=person)) -- Leave as default	The LDAP search filter that is used to show all the users below the User Base DN
User From Name Filter:	(&(cn=%u)(objectclass=person)) -- Leave as default	The LDAP search filter used to find the LDAP user by name
User Search Scope:	Leave as default	Specifies how deep in the LDAP tree to search for users
User Name Attribute:	Leave as default	The attribute of the LDAP user that specifies the user name
User Object Class:	Leave as default	The LDAP object class that stores users
Use Retrieved User Name as Principal:	Checked	Specifies if the user name retrieved from the LDAP directory will be used as the Principal in the Subject



c. The third section contains the Groups settings for the OID provider. Use appropriate values:

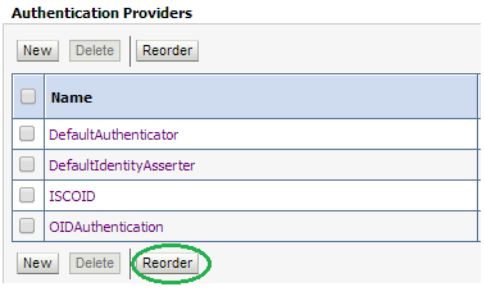
Name	Value	Purpose
Group Base DN:	cn=Groups,dc=idc,dc=oracle,dc=com	The root (base DN) of the LDAP tree where searches are per-formed for group data
All Groups Filter:	(&(cn=*)(|(objectclass=groupofUniqueNames)(objectclass=orcldynamicgroup))) -- Leave as default	The LDAP search filter that is used to show all the groups below the Group Base DN
Group From Name Filter:	(|(&(cn=%g)(objectclass=groupofUniqueNames))(&(cn=%g)(objectclass=orcldynamicgroup))) -- Leave as default	The LDAP search filter used to find the LDAP group by name

Name	Value	Purpose
Group Search Scope:	Leave as default	Specifies how deep in the LDAP tree to search for groups
Group Member-ship Searching:	Leave as default	Specifies whether group searches into nested groups are limited or unlimited
Max Group Member-ship Search Level:	Leave as default	Specifies how many levels of group membership can be searched. This setting is only valid if GroupMembershipSearching is set to limited
Ignore Duplicate Membership:	Unchecked	Determines whether duplicates members are ignored when adding groups.

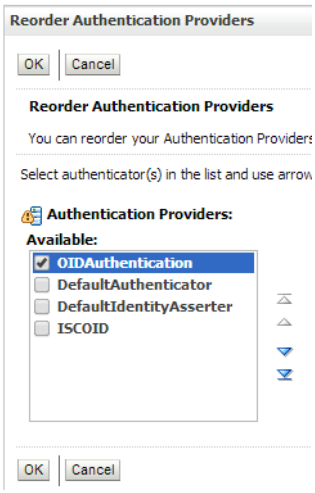


d. Click **Save**.

8. Click **Reorder** to change the order of your configured authentication providers. In order to ensure that the new OID authenticator is recognized as authentication provider, you must reorder your list of authentication providers so that the OID authentication provider is first in the list.



9. Select the OIDAuthentication and use the arrows on the right to move it into the first position. Click **OK**.



Verifying the Oracle Internet Directory (OID) Configuration

To verify the OID configuration, take the following steps:

1. Restart the WebLogic Server for your changes to take effect.
2. Using the WebLogic Administration Console, select **Security Realms > myrealm > Users and Groups** tab. The Users sub-tab should be selected by default. The circled users are created in OID and can verify the Provider – OIDAuthentication provider.

3. Click the **Groups** tab to see the list of groups the server can see. The highlighted groups are created in OID and can verify the Provider – OIDAuthentication provider.

Using LDIF Scripts to Configure Users and Groups for OID

LDIF scripts can be used to import users and groups into OID. Two sample scripts are supplied below. The scripts contain users and groups for multiple Oracle Retail integration products. You must review and edit the scripts to match your deployment topology and in-scope applications.

Integration-oid-create-groups.ldif

dn: cn=BdiJobAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiJobAdminGroup

description: BDI Job Admin is a group of individuals who can start the job, view the runtime statistics of the job , stop the job and edit the configuration.

displayname: BDI Job Administrator

#businessCategory: TBD

uniquemember: cn=bdirmsjobadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=bdirxmjobadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=bdisimjobadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiJobOperatorGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiJobOperatorGroup

description: BDI Job Operator is a group of individuals who can start the job , view the runtime statistics of the job , stop the job but cannot edit the configuration.

displayname: BDI Job Operator

#businessCategory: TBD

uniquemember: cn=bdirmsjoboperator,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=bdirxmjoboperator,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=bdisimjoboperator,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiJobMonitorGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiJobMonitorGroup

description: BDI Job Monitor is a group of individuals who can view the runtime statistics of the job.

displayname: BDI Job Monitor

#businessCategory: TBD

uniquemember: cn=bdirmsjobmonitor,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=bdirxmjobmonitor,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=bdisimjobmonitor,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiProcessAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiProcessAdminGroup

description: BDI process admin is a group of individuals who can start the process , view the runtime statistics of the process , stop the process and edit the process flows.

displayname: BDI Process Administrator

#businessCategory: TBD

uniquemember: cn=bdiprocessadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiProcessOperatorGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiProcessOperatorGroup

description: BDI process opeartor is a group of individuals who can start the process , view the runtime statistics of the process , stop the process but cannot edit the process flows.

displayname: BDI Process Opeartor

#businessCategory: TBD

uniquemember: cn=bdiprocessoperator,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiProcessMonitorGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiProcessMonitorGroup

description: BDI process Monitor is a group of individuals who can view the runtime statistics of the process.

displayname: BDI Process Monitor

#businessCategory: TBD

niquemember: cn=bdiprocessmonitor,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiSchedulerAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiSchedulerAdminGroup

description: BDI scheduler admin is a group of individuals who can start/stop the schedule , view the summary of scheduled runs metrics and schedule details.Also create, edit, delete/disable the schedules.

displayname: BDI Scheduler Administrator

#businessCategory: TBD

uniquemember: cn=bdischeduleradmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiSchedulerOperatorGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiSchedulerOperatorGroup

description: BDI scheduler Operator is a group of individuals who can start/stop the schedule , view the summary of scheduled runs metrics and schedule details.

displayname: BDI Scheduler Operator

#businessCategory: TBD

uniquemember: cn=bdischeduleroperator,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BdiSchedulerMonitorGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: BdiSchedulerMonitorGroup

description: BDI scheduler monitor is a group of individuals who can view the summary of scheduled runs metrics and schedule details.

displayname: BDI Scheduler Monitor

#businessCategory: TBD

uniquemember: cn=bdischedulermonitor,cn=users,dc=us,dc=oracle,dc=com

dn: cn=agAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: agAdminGroup

description: ArtifactGenerator Administrator is a group of individuals who can generate artifacts used in the integration products like OracleObject, JavaBeans.

displayname: ArtifactGenerator Administrator

#businessCategory: TBD

uniquemember: cn=agadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=JmsConsoleAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: JmsConsoleAdminGroup

description: JMS Console Administrator is a group of individuals who can perform various administrator task on jmsconsole like publishing message on topic, browsing messages on topic.

displayname: JMS Console Administrator

#businessCategory: TBD

uniquemember: cn=jmsconsoleadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=ribAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: ribAdminGroup

description: RIB Administrator is a group of individuals who can administrator rib-admin-gui. View the adapters state, start/stop adapters, view logs,set the log levels for adapters.

displayname: RIB Administrator

#businessCategory: TBD

uniquemember: cn=ribrmsadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribsimadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribrwmsadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribaipadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribomsadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribrxmadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribtafradmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribrfmadmin,cn=users,dc=us,dc=oracle,dc=com

uniquemember: cn=ribrpmadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=IntegrationGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: IntegrationGroup

description: IntegrationGroup is a group of individuals who can invoke rib interface api inject and publish.

displayname: Integration Group

#businessCategory: TBD

uniquemember: cn=integrationuser,cn=users,dc=us,dc=oracle,dc=com

dn: cn=RihaAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: RihaAdminGroup

description: Riha Admin Group is a group of individuals who can administer rib hospital. Can flush the messages stuck in rib error hospital, can retry the messages,view the messages in error hospital and can edit.

displayname: Riha Administrator

#businessCategory: TBD

uniquemember: cn=rihaadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=RicAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: RicAdminGroup

description: Ric Admin Group is a group of individuals who can administer rib runtime statistics , rsb runtime statistics.

displayname: Ric Administrator

#businessCategory: TBD

uniquemember: cn=ricadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=rseAdminGroup,cn=groups,dc=us,dc=oracle,dc=com

objectclass: groupOfUniqueNames

objectclass: orclGroup

objectclass: top

cn: rseAdminGroup

description: Rse Admin Group is a group of individuals who can generate webservice provider , consumer.

displayname: RSE Administrator
#businessCategory: TBD
uniquemember: cn=rseadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=RfiAdminGroup,cn=groups,dc=us,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: orclGroup
objectclass: top
cn: RfiAdminGroup
description: RFI Admin
displayname: RFI Administrator
#businessCategory: TBD
uniquemember: cn=rfiadmin,cn=users,dc=us,dc=oracle,dc=com

Integration-oid-create-users.ldif

dn: cn=bdirmsjobadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdirmsjobadmin
orclsamaccountname: bdirmsjobadmin
sn: bdirmsjobadmin
uid: bdirmsjobadmin
givenname: bdirmsjobadmin
displayname: bdirmsjobadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdirmsjobadmin@example.com

postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdirxmjobadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdirxmjobadmin
orclsamaccountname: bdirxmjobadmin
sn: bdirxmjobadmin
uid: bdirxmjobadmin
givenname: bdirxmjobadmin
displayname: bdirxmjobadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdirxmjobadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdisimjobadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Admin' role.
objectclass: inetOrgPerson

objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdisimjobadmin
orclsamaccountname: bdisimjobadmin
sn: bdisimjobadmin
uid: bdisimjobadmin
givenname: bdisimjobadmin
displayname: bdisimjobadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdisimjobadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdirmsjoboperator, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Operator' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdirmsjoboperator
orclsamaccountname: bdirmsjoboperator
sn: bdirmsjoboperator

uid: bdirmsjoboperator
givenname: bdirmsjoboperator
displayname: bdirmsjoboperator
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdirmsjoboperator@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdirxmjoboperator, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Operator' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdirxmjoboperator
orclsamaccountname: bdirxmjoboperator
sn: bdirxmjoboperator
uid: bdirxmjoboperator
givenname: bdirxmjoboperator
displayname: bdirxmjoboperator
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:

mail: bdirxmjoboperator@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdisimjoboperator, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Operator' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdisimjoboperator
orclsamaccountname: bdisimjoboperator
sn: bdisimjoboperator
uid: bdisimjoboperator
givenname: bdisimjoboperator
displayname: bdisimjoboperator
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdisimjoboperator@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdirmsjobmonitor, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Monitor' role.

objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdirmsjobmonitor
orclsamaccountname: bdirmsjobmonitor
sn: bdirmsjobmonitor
uid: bdirmsjobmonitor
givenname: bdirmsjobmonitor
displayname: bdirmsjobmonitor
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdirmsjobmonitor@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdirxmjobmonitor, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Monitor' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdirxmjobmonitor
orclsamaccountname: bdirxmjobmonitor

sn: bdirxmjobmonitor
uid: bdirxmjobmonitor
givenname: bdirxmjobmonitor
displayname: bdirxmjobmonitor
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdirxmjobmonitor@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdisimjobmonitor, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Job Monitor' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdisimjobmonitor
orclsamaccountname: bdisimjobmonitor
sn: bdisimjobmonitor
uid: bdisimjobmonitor
givenname: bdisimjobmonitor
displayname: bdisimjobmonitor
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:

facsimileTelephoneNumber:
mail: bdisimjobmonitor@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdiprocessadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Process Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdiprocessadmin
orclsamaccountname: bdiprocessadmin
sn: bdiprocessadmin
uid: bdiprocessadmin
givenname: bdiprocessadmin
displayname: bdiprocessadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdiprocessadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdiprocessoperator, cn=Users,dc=us,dc=oracle,dc=com

description: A user for the 'BDI Process Operator' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdiprocessoperator
orclsamaccountname: bdiprocessoperator
sn: bdiprocessoperator
uid: bdiprocessoperator
givenname: bdiprocessoperator
displayname: bdiprocessoperator
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdiprocessoperator@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdiprocessmonitor, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Process Monitor' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdiprocessmonitor

orclsamaccountname: bdiprocessmonitor
sn: bdiprocessmonitor
uid: bdiprocessmonitor
givenname: bdiprocessmonitor
displayname: bdiprocessmonitor
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdiprocessmonitor@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdischeduleradmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'BDI Scheduler Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdischeduleradmin
orclsamaccountname: bdischeduleradmin
sn: bdischeduleradmin
uid: bdischeduleradmin
givenname: bdischeduleradmin
displayname: bdischeduleradmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:

telephoneNumber:
facsimileTelephoneNumber:
mail: bdischeduleradmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdischeduleroperator, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'Bdi Scheduler Operator' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdischeduleroperator
orclsamaccountname: bdischeduleroperator
sn: bdischeduleroperator
uid: bdischeduleroperator
givenname: bdischeduleroperator
displayname: bdischeduleroperator
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdischeduleroperator@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=bdischedulermonitor, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'Bdi Scheduler Monitor' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: bdischedulermonitor
orclsamaccountname: bdischedulermonitor
sn: bdischedulermonitor
uid: bdischedulermonitor
givenname: bdischedulermonitor
displayname: bdischedulermonitor
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: bdischedulermonitor@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=agadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'AG Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson

cn: agadmin
orclsamaccountname: agadmin
sn: agadmin
uid: agadmin
givenname: agadmin
displayname: agadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: agadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=jmsconsoleadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'JMS Console Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: jmsconsoleadmin
orclsamaccountname: jmsconsoleadmin
sn: jmsconsoleadmin
uid: jmsconsoleadmin
givenname: jmsconsoleadmin
displayname: jmsconsoleadmin
userpassword: <update your password here>
employeeNumber:
middleName:

orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: jmsconsoleadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribrmsadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribrmsadmin
orclsamaccountname: ribrmsadmin
sn: ribrmsadmin
uid: ribrmsadmin
givenname: ribrmsadmin
displayname: ribrmsadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribrmsadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribrpmadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribrpmadmin
orclsamaccountname: ribrpmadmin
sn: ribrpmadmin
uid: ribrpmadmin
givenname: ribrpmadmin
displayname: ribrpmadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribrpmadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribrxmadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2

objectclass: orclIDXPerson
cn: ribrxmadmin
orclsamaccountname: ribrxmadmin
sn: ribrxmadmin
uid: ribrxmadmin
givenname: ribrxmadmin
displayname: ribrxmadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribrxmadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribrwmsadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribrwmsadmin
orclsamaccountname: ribrwmsadmin
sn: ribrwmsadmin
uid: ribrwmsadmin
givenname: ribrwmsadmin
displayname: ribrwmsadmin
userpassword: <update your password here>
employeeNumber:

middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribrwmsadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribomsadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribomsadmin
orclsamaccountname: ribomsadmin
sn: ribomsadmin
uid: ribomsadmin
givenname: ribomsadmin
displayname: ribomsadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribomsadmin@example.com
postalAddress:
street:
postalCode:
title:

employeeType:

dn: cn=ribtafradmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribtafradmin
orclsamaccountname: ribtafradmin
sn: ribtafradmin
uid: ribtafradmin
givenname: ribtafradmin
displayname: ribtafradmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribtafradmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribaipadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser

objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribaipadmin
orclsamaccountname: ribaipadmin
sn: ribaipadmin
uid: ribaipadmin
givenname: ribaipadmin
displayname: ribaipadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribaipadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribsimadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribsimadmin
orclsamaccountname: ribsimadmin
sn: ribsimadmin
uid: ribsimadmin
givenname: ribsimadmin
displayname: ribsimadmin
userpassword: <update your password here>

employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribsimadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=ribrfmadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIB Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ribrfmadmin
orclsamaccountname: ribrfmadmin
sn: ribrfmadmin
uid: ribrfmadmin
givenname: ribrfmadmin
displayname: ribrfmadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ribrfmadmin@example.com
postalAddress:
street:
postalCode:

title:
employeeType:

dn: cn=integrationuser, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'Integration' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: integrationuser
orclsamaccountname: integrationuser
sn: integrationuser
uid: integrationuser
givenname: integrationuser
displayname: integrationuser
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: integrationuser@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=rihaadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIHA Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top

objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: rihaadmin
orclsamaccountname: rihaadmin
sn: rihaadmin
uid: rihaadmin
givenname: rihaadmin
displayname: rihaadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: rihaadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

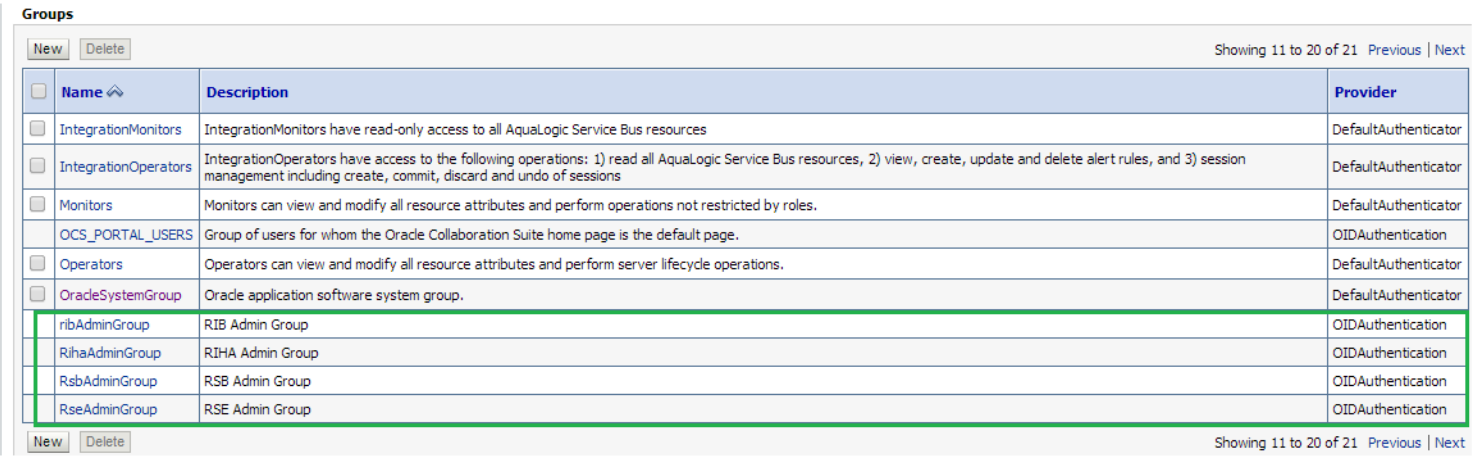
dn: cn=ricadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RIC Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: ricadmin
orclsamaccountname: ricadmin
sn: ricadmin
uid: ricadmin
givenname: ricadmin
displayname: ricadmin

userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: ricadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:

dn: cn=rseadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RSE Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: rseadmin
orclsamaccountname: rseadmin
sn: rseadmin
uid: rseadmin
givenname: rseadmin
displayname: rseadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: rseadmin@example.com
postalAddress:
street:

postalCode:
title:
employeeType:

dn: cn=rfiadmin, cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'RFI Admin' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPerson
cn: rfiadmin
orclsamaccountname: rfiadmin
sn: rfiadmin
uid: rfiadmin
givenname: rfiadmin
displayname: rfiadmin
userpassword: <update your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: rfiadmin@example.com
postalAddress:
street:
postalCode:
title:
employeeType:



Groups

New Delete — Showing 11 to 20 of 21 Previous | Next

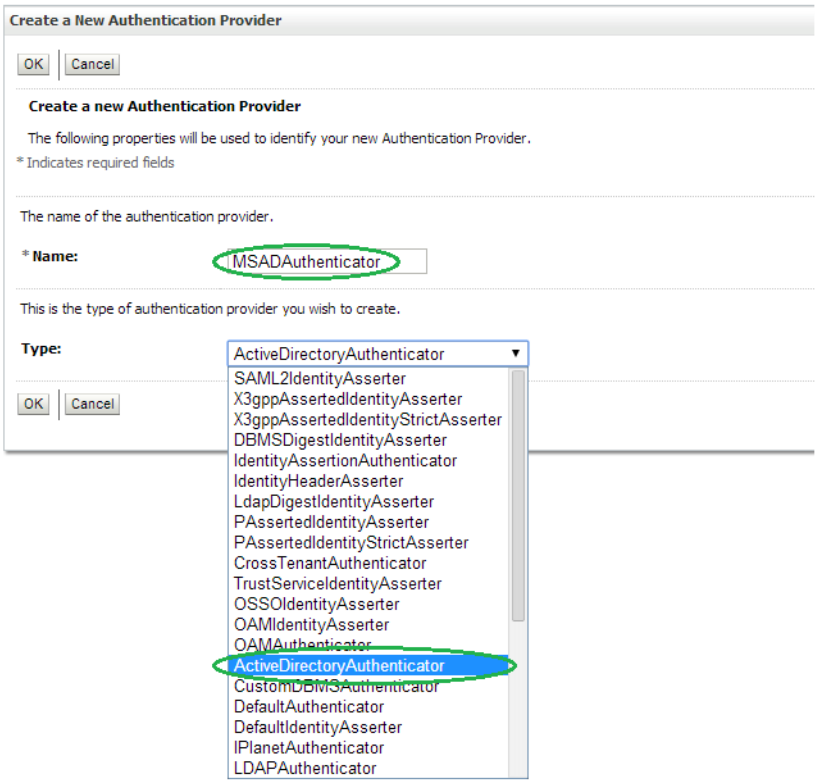
Name	Description	Provider
IntegrationMonitors	IntegrationMonitors have read-only access to all AquaLogic Service Bus resources	DefaultAuthenticator
IntegrationOperators	IntegrationOperators have access to the following operations: 1) read all AquaLogic Service Bus resources, 2) view, create, update and delete alert rules, and 3) session management including create, commit, discard and undo of sessions	DefaultAuthenticator
Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
OCS_PORTAL_USERS	Group of users for whom the Oracle Collaboration Suite home page is the default page.	OIDAuthentication
Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator
OracleSystemGroup	Oracle application software system group.	DefaultAuthenticator
ribAdminGroup	RIB Admin Group	OIDAuthentication
RihaAdminGroup	RIHA Admin Group	OIDAuthentication
RsbAdminGroup	RSB Admin Group	OIDAuthentication
RseAdminGroup	RSE Admin Group	OIDAuthentication

New Delete — Showing 11 to 20 of 21 Previous | Next

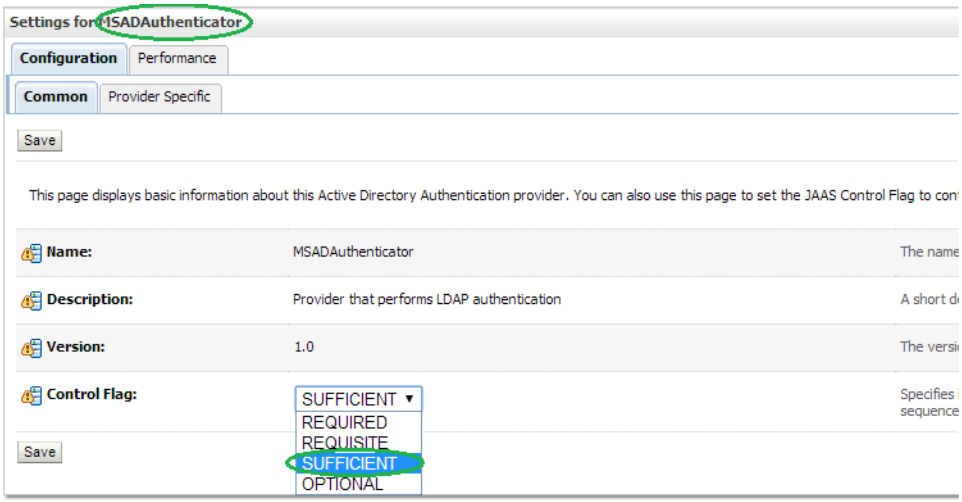
Configuring Active Directory (AD) as an Authentication Provider in WebLogic

To configure the AD as an authentication provider in WebLogic, take the following steps:

1. Login to **WebLogic Console -> Security Realm -> myrealm**.
2. Select tab **Providers -> Authentication -> Default Provider (DefaultAuthenticator)**.
3. Change the **Control Flag** (JAAS Flag) from REQUIRED to SUFFICIENT and click **Save**.
4. Click **New** to add a new Authentication Provider.
5. Enter MSADAuthenticator as the **Name**. Select ActiveDirectoryAuthenticator as the **Type** and click **OK**.



6. Change the **Control Flag** to SUFFICIENT for the MSADAuthenticator Provider added and click **Save**.

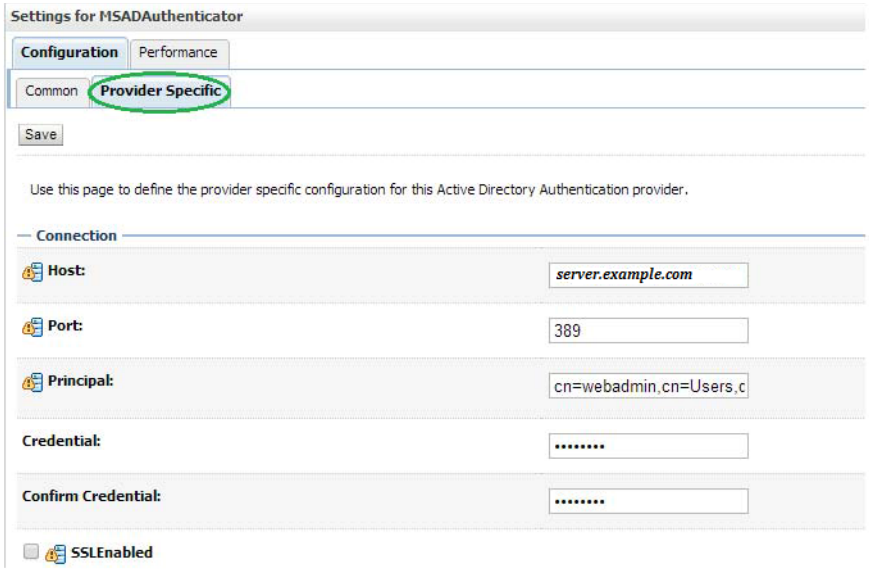


7. Select **Provider Specific** tab and enter the Active Directory (AD) server details.

   a. The first section contains the Connection settings for the AD server. Use appropriate values based on where AD is hosted and the credentials:

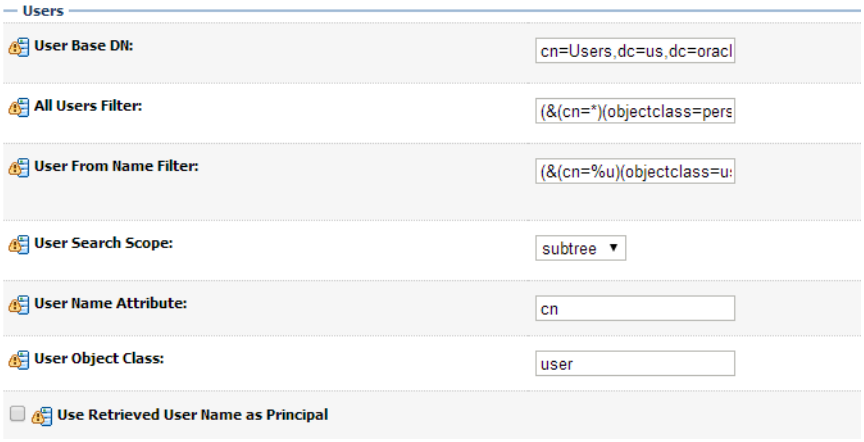
Name	Value	Purpose
Host:	server.example.com	The AD host name
Port:	389	The standard AD listening port

Name	Value	Purpose
Principal:	cn=webadmin,cn=Users, dc=us,dc=oracle,dc=com	The LDAP user that logs into AD on behalf of your authentication provider
Credentials:		Password for the principal user
Confirm Credentials:		Confirmation of the password
SSL Enabled:	Unchecked	Enables or disables SSL connectivity



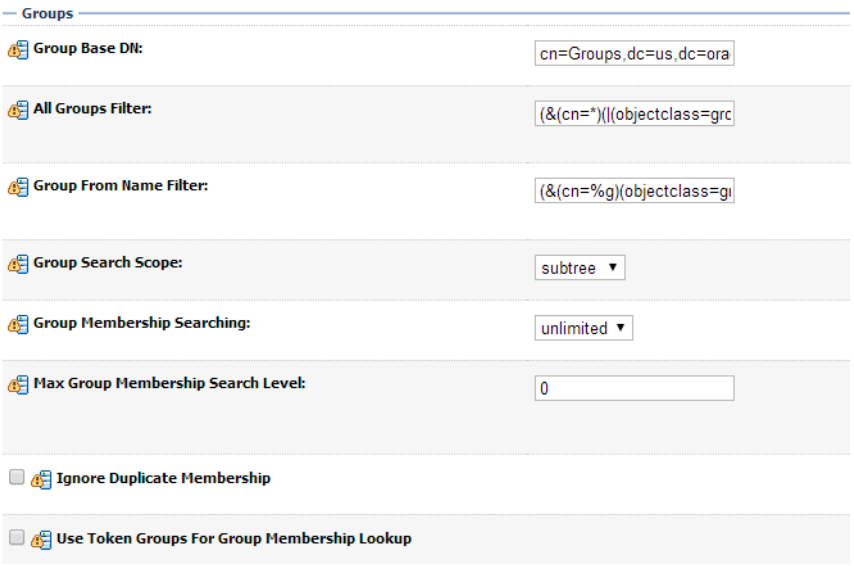
b. The second section contains the Users settings for the AD provider. Use appropriate values:

Name	Value	Purpose
User Base DN:	cn=Users,dc=us,dc=oracle,dc=com	The root (base DN) of the LDAP tree where searches are performed for user data
All Users Filter:	(&(cn=*)(objectclass=person))	The LDAP search filter that is used to show all the users below the User Base DN
User From Name Filter:	(&(cn=%u)(objectclass=user))	The LDAP search filter used to find the LDAP user by name
User Search Scope:	Leave as default	Specifies how deep in the LDAP tree to search for users
User Name Attribute:	Leave as default	The attribute of the LDAP user that specifies the user name
User Object Class:	Leave as default	The LDAP object class that stores users
Use Retrieved User Name as Principal:	Unchecked	Specifies if the user name retrieved from the LDAP directory will be used as the Principal in the Subject



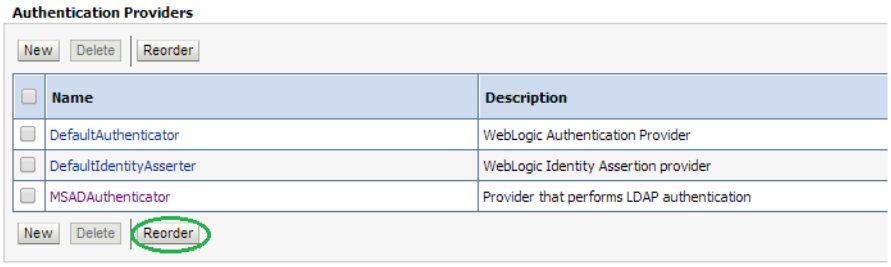
c. The third section contains the Groups settings for the AD provider. Use appropriate values:

Name	Value	Purpose
Group Base DN:	cn=Groups,dc=us,dc=oracle,dc=com	The root (base DN) of the LDAP tree where searches are performed for group data
All Groups Filter:	(&(cn=*)(|(objectclass=group)))	The LDAP search filter that is used to show all the groups below the Group Base DN
Group From Name Filter:	(&(cn=%g)(objectclass=group))	The LDAP search filter used to find the LDAP group by name
Group Search Scope:	Leave as default	Specifies how deep in the LDAP tree to search for groups
Group Member-ship Searching:	Leave as default	Specifies whether group searches into nested groups are limited or unlimited
Max Group Membership Search Level:	Leave as default	Specifies how many levels of group membership can be searched. This setting is only valid if GroupMembershipSearching is set to limited
Ignore Duplicate Membership:	Unchecked	Determines whether duplicates members are ignored when adding groups.

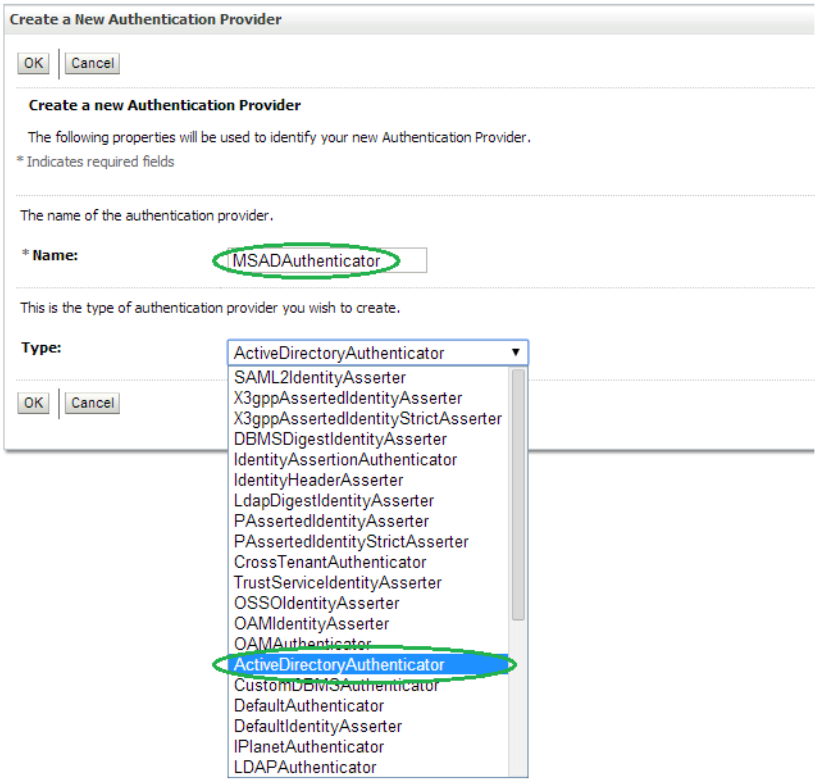


d. Click **Save**.

8. Click **Reorder** to change the order of your configured authentication providers. In order to ensure that MSAD authenticator is recognized as authentication provider, you must reorder your list of authentication providers so that the MSAD authentication provider is first in the list.

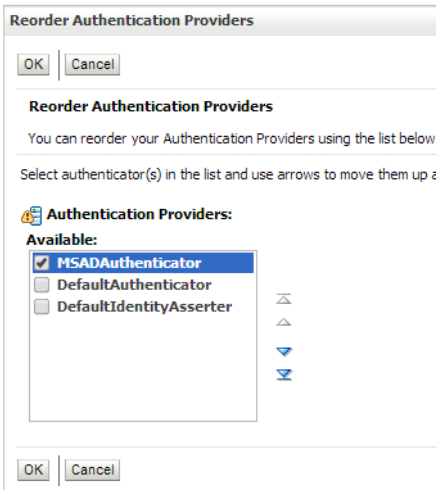


9. Select the MSADAuthenticator and use the arrows on the right to move it into the first position. Click **OK**.



10. Click **Reorder** to change the order of your configured authentication providers. In order to ensure that MSAD authenticator is recognized as authentication provider, you must reorder your list of authentication providers so that the MSAD authentication provider is first in the list.

11. Select the MSADAuthenticator and use the arrows on the right to move it into the first position. Click OK.



Verifying the Active Directory (AD) Configuration

To verify the AD configuration, take the following steps:

1. Restart the WebLogic Server for your changes to take effect.
2. Using the WebLogic Administration Console, select S**ecurity Realms > myrealm > Users and Groups** tab. The Users sub-tab should be selected by default. The circled users are created in AD and can verify the Provider – MSADAuthenticator provider.

Users

New | Delete | Showing 1 to 18 of 18 Previous | Next

Name	Description	Provider
Administrator	Built-in account for administering the computer/domain	MSADAuthenticator
agadmin	ag admin	MSADAuthenticator
agadmin	agadmin	DefaultAuthenticator
devsrvsppt	Oracle Sys Admin Account	MSADAuthenticator
Guest	Built-in account for guest access to the computer/domain	MSADAuthenticator
jsituser	jsit user	MSADAuthenticator
krbtgt	Key Distribution Center Service Account	MSADAuthenticator
logUser		MSADAuthenticator
OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
ribadmin	rib admin	MSADAuthenticator
rihauser	riha user	MSADAuthenticator
rmsuser		DefaultAuthenticator
rsbadmin	rsb admin	MSADAuthenticator
rsbuser	rsb user	MSADAuthenticator
rseadmin	rse admin	MSADAuthenticator
user		MSADAuthenticator
webadmin		MSADAuthenticator
weblogic	This user is the default administrator.	DefaultAuthenticator

New | Delete | Showing 1 to 18 of 18 Previous | Next

3. Click the **Groups** tab to see the list of groups the server can see. The highlighted groups are created in AD and can verify the Provider – MSADAuthenticator provider.

Groups

New Delete

Showing 1 to 16 of 16 Previous | Next

Name	Description	Provider
AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
agAdminGroup	ag Admin Group	MSADAuthenticator
agAdminGroup	agAdminGroup	DefaultAuthenticator
AppTesters	AppTesters group.	DefaultAuthenticator
CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
logUserGroup		MSADAuthenticator
Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator
OracleSystemGroup	Oracle application software system group.	DefaultAuthenticator
ribAdminGroup	Rib Admin Group	MSADAuthenticator
RihaAdminGroup	Riha admin group	DefaultAuthenticator
RsbAdminGroup	Rsb Admin Group	MSADAuthenticator
rseAdminGroup	rse Admin Group	MSADAuthenticator
rseAdminGroup		DefaultAuthenticator

New Delete

Showing 1 to 16 of 16 Previous | Next

D

Appendix: Installation Order

This section provides a guideline for the order in which the Oracle Retail applications should be installed. If a retailer has chosen to use only some of the applications, the order is still valid, less the applications not being installed.

Note: The installation order is not meant to imply integration between products.

Enterprise Installation Order

1. Oracle Retail Merchandising System (RMS), Oracle Retail Trade Management (RTM)
2. Oracle Retail Sales Audit (ReSA)
3. Oracle Retail Extract, Transform, Load (RETL)
4. Oracle Retail Warehouse Management System (RWMS)
5. Oracle Retail Invoice Matching (ReIM)
6. Oracle Retail Price Management (RPM)
7. Oracle Retail Allocation
8. Oracle Retail Mobile Merchandising (ORMM)
9. Oracle Retail Customer Engagement (ORCE)
10. Oracle Retail Xstore Office
11. Oracle Retail Xstore Point-of-Service, including Xstore Point-of-Service for Grocery, and including Xstore Mobile
12. Oracle Retail Xstore Environment
13. Oracle Retail EFTLink
14. Oracle Retail Store Inventory Management (SIM), including Mobile SIM
15. Oracle Retail Predictive Application Server (RPAS)
16. Oracle Retail Predictive Application Server Batch Script Architecture (RPAS BSA)
17. Oracle Retail Demand Forecasting (RDF)
18. Oracle Retail Category Management Planning and Optimization/Macro Space Optimization (CMPO/MSO)
19. Oracle Retail Replenishment Optimization (RO)

20. Oracle Retail Regular Price Optimization (RPO)
21. Oracle Retail Merchandise Financial Planning (MFP)
22. Oracle Retail Size Profile Optimization (SPO)
23. Oracle Retail Assortment Planning (AP)
24. Oracle Retail Item Planning (IP)
25. Oracle Retail Item Planning Configured for COE (IP COE)
26. Oracle Retail Advanced Inventory Planning (AIP)
27. Oracle Retail Integration Bus (RIB)
28. Oracle Retail Services Backbone (RSB)
29. Oracle Retail Financial Integration (ORFI)
30. Oracle Retail Bulk Data Integration (BDI)
31. Oracle Retail Integration Console (RIC)
32. Oracle Commerce Retail Extension Module (ORXM)
33. Oracle Retail Data Extractor for Merchandising
34. Oracle Retail Clearance Optimization Engine (COE)
35. Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)
36. Oracle Retail Insights, including Retail Merchandising Insights (previously Retail Merchandising Analytics) and Retail Customer Insights (previously Retail Customer Analytics)
37. Oracle Retail Order Broker