Oracle® Health Sciences Network

Installation Guide

Release 2.0.0.0

E65879-01

September 2015

Oracle Health Sciences Network Installation Guide, Release 2.0.0.0

E65879-01

Contents

Preface

Oracle Health Sciences Network (HSN) is a new SaaS services offering for both healthcare providers and pharmaceutical customer organizations. It brings together multiple customer organizations under a single cloud-based and Oracle-hosted business network, thus allowing them to exchange information and/or business services using HSN applications such as Protocol Validator and Patient Recruiter (PVPR).

HSN consists of two components: Patient Validator and Patient Recruiter (PVPR), and Platform.

Audience

This document is intended for users (having knowledge of WebLogic server administration and database administration) who want to install HSN applications.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

- *Oracle Health Sciences Network Installation Guide [this document]*
- *Oracle Health Sciences Network User's Guide*
- *Oracle Health Sciences Network Release Notes*
- *Oracle Health Sciences Network Security Guide*
- *Oracle Health Sciences Network Administrator's Guide*

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

1 Installation Overview

You can download the Health Sciences Network (HSN) media pack from the Automated Release Update (ARU) system. Files mentioned in the installation steps are available in corresponding folder hierarchy. The HSN media pack contains the following applications:

- HSnPManApp
  - **EAR** - Deployable EAR file for HSnPManApp
  - **SQL** - SQL scripts to create and configure the registry schema
- HSnP-SOA
  - **MDS** - Metadata Services (MDS) artifacts used in Service-Oriented Architecture (SOA) composites
  - **SCA** - SOA composites for HSnP services
  - **Sensor** - HSN sensor implementation to track the usage of HSnP services
- CDM-ODB
  - CDM installation scripts
  - ODB installation scripts
  - CDM ETL scripts
  - ODB Data Loaders
- PVPR
  - **EAR** - Deployable EAR file for PVPR
  - **SQL** - SQL scripts to create the Patient Validator and Patient Recruiter (PVPR) schema
- wls
  - WebLogic Scripting Tool (WLST) scripts used for Oracle Web Services Manager (OWSM) configuration of PVPR and HSnPManApp

1.1 Prerequisites

The following servers must have synchronized clock:

- HSNManApp - Database server and Application server
- SOA server
- PVPR - Database server and Application server

You should set up the following:

- Oracle WebLogic Server (10.3.6) with OWSM and Enterprise Manager for HSNManApp and PVPR installations
- Oracle SOA Suite (11.1.1.6.0) and OWSM on WebLogic installation for HSN-SOA

2
Installing the Platform

This chapter provides the instructions to install the Platform services of the Health Sciences Network (HSN).

This chapter contains the following sections:

- Section 2.1, "Installing HSN Database"
- Section 2.2, "Installing HSN ManApp"
- Section 2.3, "Configuring HSN-SOA"
- Section 2.4, "Configuring SOA MDS"
- Section 2.5, "Configuring HSN Tracking for SOA Composites"
- Section 2.6, "Setting Transaction Timeout for Service-Oriented Architecture"
- Section 2.7, "Deploying SOA Composite"

2.1 Installing HSN Database

This section contains the following topics:

- Section 2.1.1, "Creating HSN Tablespace"
- Section 2.1.2, "Creating HSN Database User"
- Section 2.1.3, "Installing HSN Database Objects"

2.1.1 Creating HSN Tablespace

To create tablespace for the HSN database, perform the following:

1. Edit `hsnp_create_tablespace.sql`.
2. Enter the following details:
   - appropriate path for data file (line starting with data file)
   - size and auto extend size (line starting with SIZE)
3. Log in to the database as a user with privilege to create tablespace and execute the script.
4. Enter the name of the tablespace you want to create when prompted.

See also Section 3.1.

2.1.2 Creating HSN Database User

To create HSN database user, perform the following:

1. Log in to the database as a user with privilege to create user using SQLPlus.
2. In the SQLPlus prompt, execute the `@hsnp_create_user.sql` script.
3. Enter the corresponding values as prompted.

> **Note:** Ensure that you specify the tablespace name created in Section 2.1.1 when prompted.

4. Exit SQLPlus.

2.1.3 Installing HSN Database Objects

This section describes how to create database objects for HSN and initialize the database with seed data.

To install the HSN database objects, perform the following:

1. Log in to the database as HSN user (created in Section 2.1.2) using SQLPlus.
2. In the SQLPlus prompt, execute the `HSNP_ddl.sql` script.

   This creates the required database objects.
3. Update the SOA and ManApp service URL in the BPEL_PROCESS_MASTER and MANAGEMENT_CONFIGURATION tables as per the environment in HSNP_seed.sql.
4. Execute the `HSNP_seed.sql` script.

   This inserts the seed data in the database objects created.
5. Exit SQLPlus.

Running Post-Installation Scripts

During schema creation, access rights are granted to the schema user which are required only for database configuration. Post database schema creation, the access rights need to be revoked. The access rights can be revoked using the post installation scripts.

1. Connect to the database as a user with sysdba privilege.
2. Execute the `@hsnp_post_install.sql` script.

2.2 Installing HSN ManApp

This section contains the following topics:

- Section 2.2.1, "Enabling JPA 2.0"
- Section 2.2.2, "Configuring Data Source"
- Section 2.2.3, "Setting Transaction Timeout"
- Section 2.2.4, "Deploying EAR"
- Section 2.2.5, "Configuring Logging"
- Section 2.2.6, "Configuring the Oracle Web Services Manager"

2.2.1 Enabling JPA 2.0

To enable JPA 2.0, perform the following:

1. Edit the <MIDDLEWARE_HOME>/wlserver_10.3/common/bin/commEnv.sh file to add the PRE_CLASSPATH variable at the end of the file.
2. Verify the JAR version number in the <MIDDLEWARE_HOME>/modules folder and update the following statement accordingly:

   ```
   PRE_CLASSPATH=${MODULES_DIR}/javax.persistence_1.1.0.0_2-
   
   0.jar:${MODULES_DIR}/com.oracle.jpa2support_1.0.0.0_2-
   
   1.jar
   
   export PRE_CLASSPATH
   ```

2.2.2 Configuring Data Source

To configure data source, perform the following:

1. Log in to the Oracle WebLogic server console for the HSnP domain.
2. Create data source using the schema created in database setup steps.
3. Enter the jndi name as **jdbc/HAFDBDS** and assign it to the HSnPManApp server as target.
4. Restart the server.

2.2.3 Setting Transaction Timeout

To set the transaction timeout for the WebLogic application server, perform the following:

1. Go to **Services > JTA** in the **WebLogic** console.
2. Update timeout seconds to 600 and save.

2.2.4 Deploying EAR

To deploy EAR, perform the following:

Note: Ensure that the application name is set to HSnPMan-EAR during deployment.

1. Extract the HSnPManApp EAR file from the media pack.
2. Deploy the EAR file to the Oracle WebLogic server, where HSnPManApp need to be installed.

2.2.5 Configuring Logging

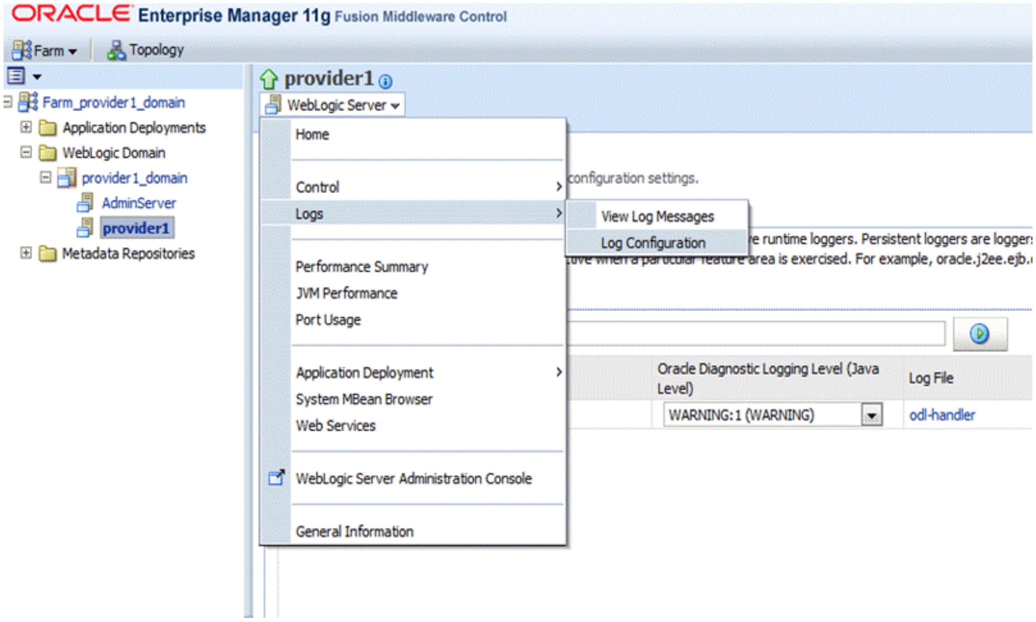
To configure logging, perform the following:

1. Log in to the Enterprise Manager of WebLogic server.
2. In the pane on the left side of the window, click the **HSnPManApp** domain in the WebLogic Domain folder and select the target **HSnPManApp** server.

   For example, provider1.

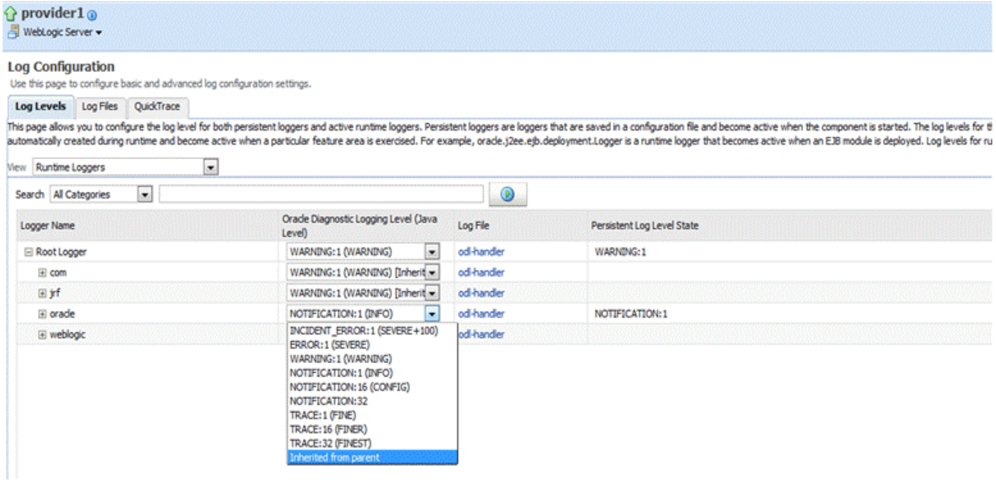
3. From the **WebLogic Server** drop-down list, select **Logs** and then select **Log Configuration**.

Figure 2–1 Log Configuration



4. Expand **Root Logger**.

Figure 2–2 Root Logger



Log Configuration

Use this page to configure basic and advanced log configuration settings.

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are loggers that are saved in a configuration file and become active when the component is started. The log levels for t automatically created during runtime and become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime logger that becomes active when an EJB module is deployed. Log levels for ru

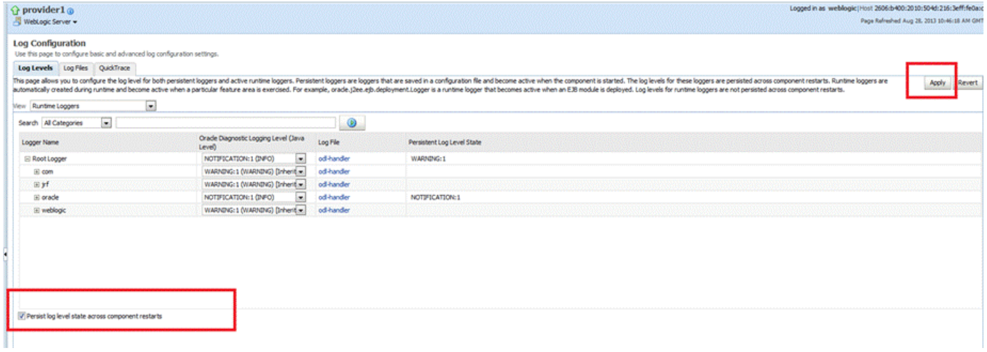
Logger Name	Oracle Diagnostic Logging Level (Java Level)	Log File	Persistent Log Level State
⊟ Root Logger	WARNING:1 (WARNING)	odl-handler	WARNING:1
⊞ com	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ jrf	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ oracle	NOTIFICATION:1 (INFO)	odl-handler	NOTIFICATION:1
⊞ weblogic		odl-handler	

INCIDENT_ERROR:1 (SEVERE+100)
ERROR:1 (SEVERE)
WARNING:1 (WARNING)
NOTIFICATION:1 (INFO)
NOTIFICATION:16 (CONFIG)
NOTIFICATION:32
TRACE:1 (FINE)
TRACE:16 (FINER)
TRACE:32 (FINEST)
Inherited from parent

5. For Oracle, change the log level and select **Inherited from Parent**.

6. Select **Persist log level state across component restarts** and click **Apply Changes**.

Figure 2–3 Log Levels


provider1
WebLogic Server
Logged in as weblogic | Host 2606:b400:2010:504d:216:3eff:fe0a:c
Page Refreshed Aug 28, 2013 10:46:18 AM GMT
Log Configuration
Log Levels
Log Files
QuickTrace
Apply
Revert

Use this page to configure basic and advanced log configuration settings.

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are loggers that are saved in a configuration file and become active when the component is started. The log levels for these loggers are persisted across component restarts. Runtime loggers are automatically created during runtime and become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime logger that becomes active when an EJB module is deployed. Log levels for runtime loggers are not persisted across component restarts.

View: Runtime Loggers

Search: All Categories

Logger Name	Oracle Diagnostic Logging Level (Java Level)	Log File	Persistent Log Level State
⊟ Root Logger	NOTIFICATION:1 (INFO)	odl-handler	WARNING:1
⊞ com	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ jrf	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ oracle	NOTIFICATION:1 (INFO)	odl-handler	NOTIFICATION:1
⊞ weblogic	WARNING:1 (WARNING) [Inherit	odl-handler	

☑ Persist log level state across component restarts

2.2.6 Configuring the Oracle Web Services Manager

To execute the following commands you need to set the JAVA_HOME environment variable to point to JDK referred in the HSnP domain:

- `export JAVA_HOME=<Path to JDK referred with hsnp domain>`
- `export PATH=$JAVA_HOME/bin:$PATH`

1. Generate private key to be used in the HSnP ManApp and SOA servers using keytool utility available in the JDK bin directory.
2. In the following command, replace the <KEY_LOCATION> as required.

   ```
   keytool -genkey -alias hsnp-key -keyalg "RSA" -sigalg "SHA1withRSA"
   -dname "cn=HSNP, ou=HSGBU, o=ORACLE, c=US" -keystore <KEY_
   LOCATION>/hsnpkey.jks -validity 3650
   ```

   a. Enter the keystore password and the key password when prompted.
3. Copy the generated keystore hsnpkey.jks to the <HSNP_DOMAIN_HOME>/config/fmwconfig folder.
4. Open the <HSNP_DOMAIN_HOME>/config/fmwconfig/jps-config.xml file.
5. Search for `default-keystore.jks` in the file.

   It should be similar to <serviceinstance name="keystore" provider="keystore.provider" location="./default-keystore.jks">.
6. Replace `./default-keystore.jks` with `./hsnpkey.jks` and save the file.
7. Restart the WebLogic server instances for the HSnP domain.
8. Copy the HSnP_OWSM_Config.py and GrantIdentity_to_HSnP.py files from the media pack to a location to which the operating system user has read and execute permissions.
9. Execute the following commands on the command prompt:
   - `cd <MIDDLEWARE_HOME>/oracle_common/common/bin`
   - `./wlst.sh <ABSOLUTE FILE_PATH to HSnP_OWSM_Config.py>`

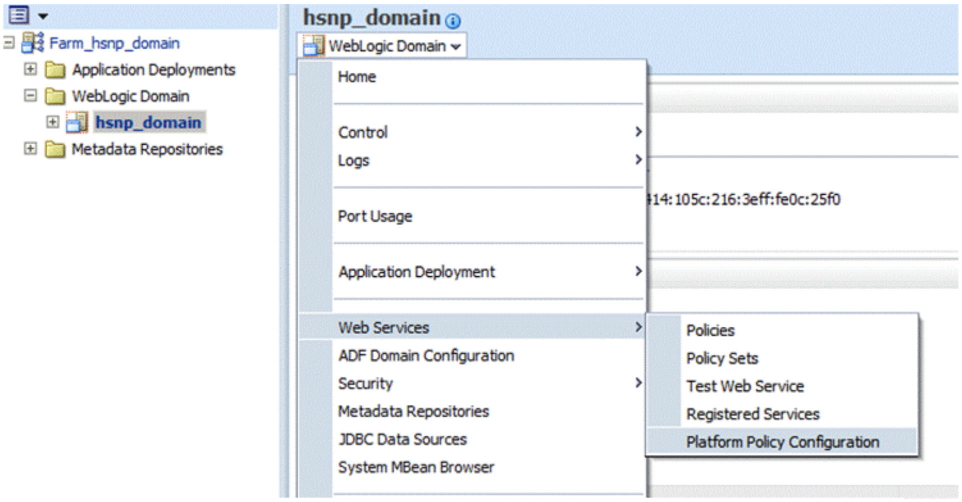
     a. Enter the corresponding values as prompted by the script.
   - `./wlst.sh <ABSOLUTE FILE PATH to GrantIdentity_to_HSnP.py>`

     a. Enter the corresponding values as prompted.

The HSnP_OWSM_Config.py script adds credentials for the hsnpkey.jks file. The GrantIdentity_to_HSnPMan.py file grants identity permission to the HSnPMan-Ear application.

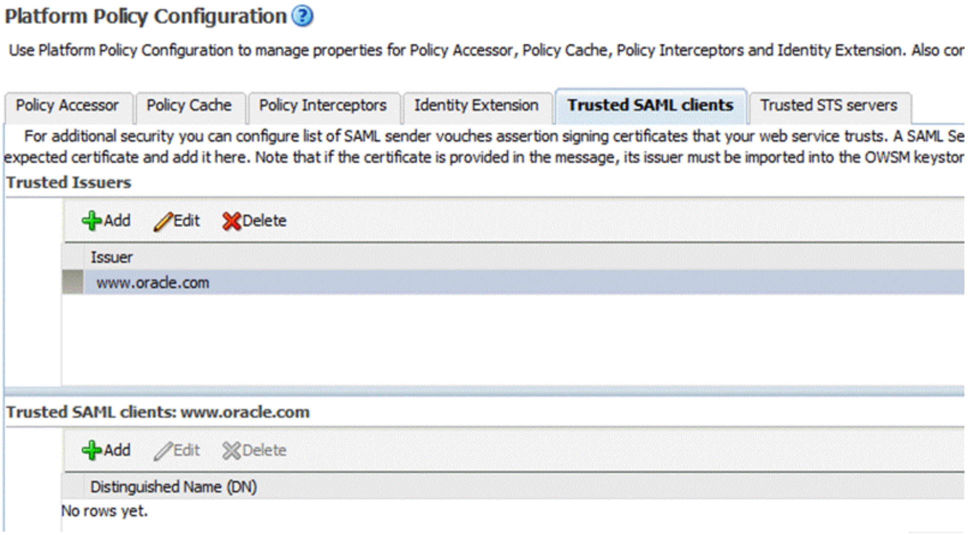
10. Login to the Enterprise Manager of the HSnP domain.
11. In the left pane, click the HSnP domain in the WebLogic domain folder.
12. From the **WebLogic Domain** drop-down list, select **Web Services** and then select **Platform Policy Configuration**.

Figure 2–4 WebLogic Domain Drop-down List



13. Click the **Trusted SAML clients** tab in the Platform Policy Configuration page.
14. Select `www.oracle.com` issuer in the Trusted Issuers pane.

Figure 2–5 Platform Policy Configuration



Use Platform Policy Configuration to manage properties for Policy Accessor, Policy Cache, Policy Interceptors and Identity Extension. Also cor

For additional security you can configure list of SAML sender vouches assertion signing certificates that your web service trusts. A SAML Se expected certificate and add it here. Note that if the certificate is provided in the message, its issuer must be imported into the OWSM keystor

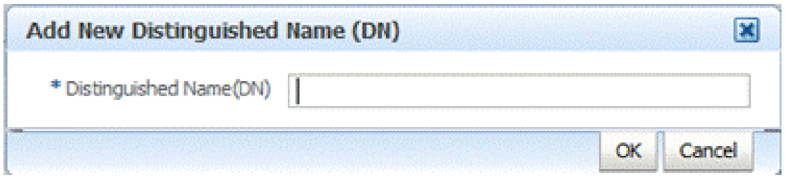
Issuer
www.oracle.com

Distinguished Name (DN)
No rows yet.

15. Click **Add** in the Trusted SAML clients: www.oracle.com pane.

    The Add New Distinguished Name (DN) window is displayed.

Figure 2–6 Add New Distinguished Name (DN) Window



16. Add text cn=HSN-PVPR, ou=HSGBU, o=ORACLE, c=US and click **OK**.
17. Repeat steps 14 and 15 to add cn=HSNP, ou=HSGBU, o=ORACLE, c=US as trusted SAML client.
18. Click **Apply**.
19. Log out of the Enterprise Manager.
20. Create the WebLogic user **hsn_system** to be used for the HSnP domain.
21. Restart the WebLogic server instances for the HSnP domain.

2.3 Configuring HSN-SOA

This chapter contains the following topics:

- Section 2.3.1, "Increasing PermGen Memory When Using Sun JDK"
- Section 2.3.2, "Installing SOA Security Patch"
- Section 2.3.3, "Configuring Logging"
- Section 2.3.4, "Configuring Oracle Web Services Manager"

2.3.1 Increasing PermGen Memory When Using Sun JDK

To increase PermGen memory, perform the following:

1. Edit the <HSNP-SOA_DOMAIN_HOME>/bin/setSOADomainEnv.sh file to increase the permgen memory allocation.
2. Increase the following values:

   if ["${JAVA_VENDOR}" != "Oracle"] ; then

   DEFAULT_MEM_ARGS="${DEFAULT_MEM_ARGS} -XX:PermSize=128m -XX:MaxPermSize=256m"

   PORT_MEM_ARGS="${PORT_MEM_ARGS} -XX:PermSize=256m -XX:MaxPermSize=512m"

   fi

   to these values:

   if ["${JAVA_VENDOR}" != "Oracle"] ; then

   DEFAULT_MEM_ARGS="${DEFAULT_MEM_ARGS} -XX:PermSize=512m -XX:MaxPermSize=1024m"

   PORT_MEM_ARGS="${PORT_MEM_ARGS} -XX:PermSize=1024m -XX:MaxPermSize=1024m"

   fi

2.3.2 Installing SOA Security Patch

To install SOA security patch, perform the following:

1. Install the SOA Security Patch 16622432 for SOA version 11.1.1.6.0.
2. Download the patch from the following link and follow the install procedure for the Oracle SOA Platform:

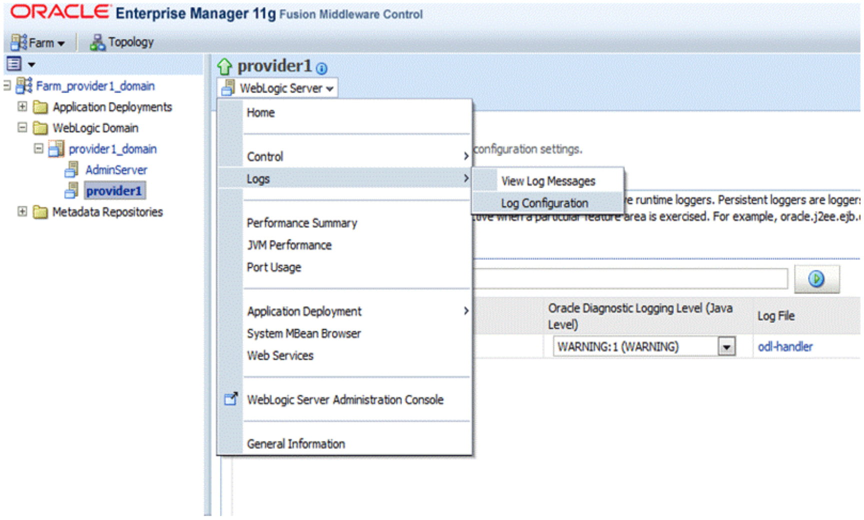
   https://support.oracle.com/epmos/faces/PatchDetail?_afrLoop=446908509299957&patchId=16622432&_afrWindowMode=0&_adf.ctrl-state=1dv0u5xlba_4

2.3.3 Configuring Logging

To configure logging, perform the following:

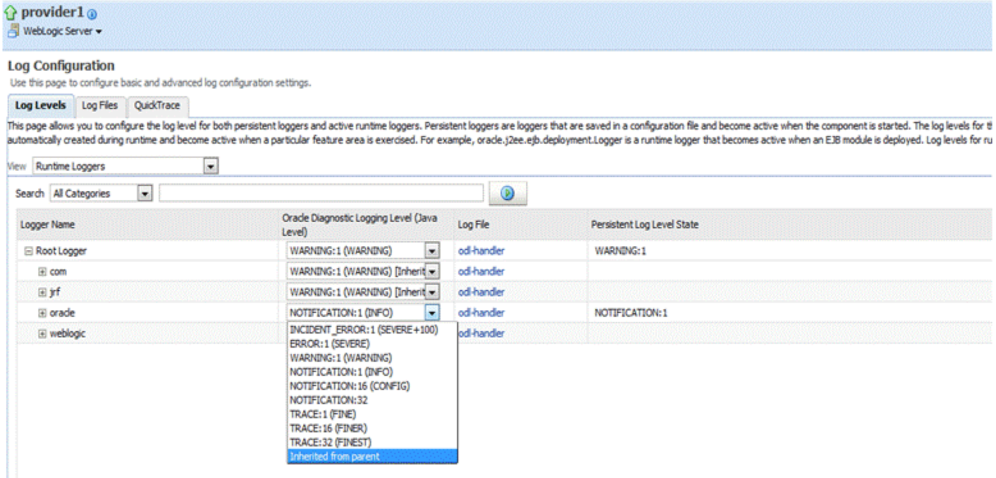
1. Log in to the Enterprise Manager.
2. In the pane on the left side of the window, click the SOA domain in the WebLogic Domain folder and select the target SOA server.
3. From the **WebLogic Server** drop-down list, select **Logs** and then select **Log Configuration**.

Figure 2–7 Log Configuration



4. Expand **Root Logger**.
5. For Oracle, change the log level and select **Inherited from Parent**.

Figure 2–8 Root Logger



Log Configuration

Use this page to configure basic and advanced log configuration settings.

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are loggers that are saved in a configuration file and become active when the component is started. The log levels for th
automatically created during runtime and become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime logger that becomes active when an EJB module is deployed. Log levels for ru

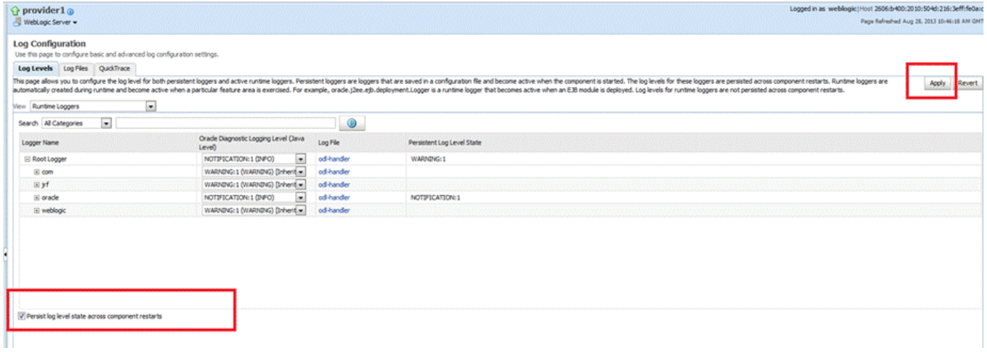
View: Runtime Loggers

Search: All Categories

Logger Name	Oracle Diagnostic Logging Level (Java Level)	Log File	Persistent Log Level State
⊟ Root Logger	WARNING:1 (WARNING)	odl-handler	WARNING:1
⊞ com	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ jrf	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ oracle	NOTIFICATION:1 (INFO)	odl-handler	NOTIFICATION:1
⊞ weblogic		odl-handler	

6. Select **Persist log level state across component restarts** and click **Apply Changes**.

Figure 2–9 Log Levels



provider1
WebLogic Server
Logged in as weblogic|Host 2606:b400:2010:504d:216:3eff:fe0a:c
Page Refreshed Aug 28, 2013 10:46:18 AM GMT
Log Levels
Log Files
QuickTrace
Apply
Revert

Log Configuration

Use this page to configure basic and advanced log configuration settings.

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are loggers that are saved in a configuration file and become active when the component is started. The log levels for these loggers are persisted across component restarts. Runtime loggers are automatically created during runtime and become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime logger that becomes active when an EJB module is deployed. Log levels for runtime loggers are not persisted across component restarts.

View: Runtime Loggers

Search: All Categories

Logger Name	Oracle Diagnostic Logging Level (Java Level)	Log File	Persistent Log Level State
⊟ Root Logger	NOTIFICATION:1 (INFO)	odl-handler	WARNING:1
⊞ com	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ jrf	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ oracle	NOTIFICATION:1 (INFO)	odl-handler	NOTIFICATION:1
⊞ weblogic	WARNING:1 (WARNING) [Inherit	odl-handler	

☑ Persist log level state across component restarts

2.3.4 Configuring Oracle Web Services Manager

To configure Oracle Web Services Manager, perform the following:

1. Copy the hsnpkey.jks keystore file generated as part of OWSM configuration in the HSnP domain to the <HSNP-SOA_DOMAIN_HOME>/config/fmwconfig folder.

2. Open the <HSNP-SOA_DOMAIN_HOME>/config/fmwconfig/jps-config.xml file.

3. Search for **default-keystore.jks** in the file.

   It should be like <serviceinstance name="keystore" provider="keystore.provider"location="./default-keystore.jks">

4. Replace `./default-keystore.jks` with `./hsnpkey.jks` and save the file.

5. Restart the WebLogic server instances for the HSnP-SOA domain.

6. Copy the HSnP_OWSM_Config.py file from the media pack to a location to which the operating system user has read and execute permissions.

7. Execute the following commands on the command prompt:

   - `cd <MIDDLEWARE_HOME>/oracle_common/common/bin`

   - `./wlst.sh <ABSOLUTE FILE_PATH to HSnP_OWSM_Config.py>`

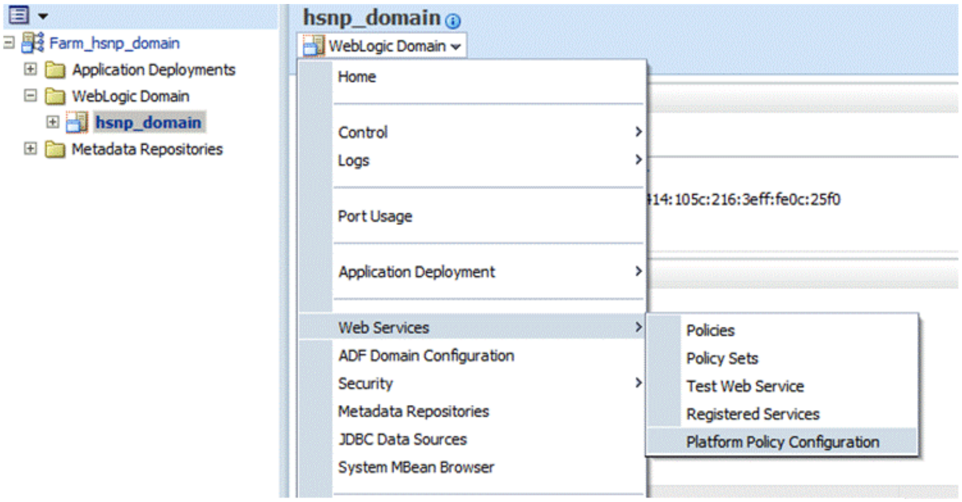
   a. Enter the corresponding values as prompted by the script.

8. Log in to the Enterprise Manager of the HSnP-SOA domain.

9. In the left pane, click the HSnP-SOA domain in the WebLogic Domain folder.

10. From the **WebLogic Domain** drop-down list, select **Web Services** and then select **Platform Policy Configuration**.

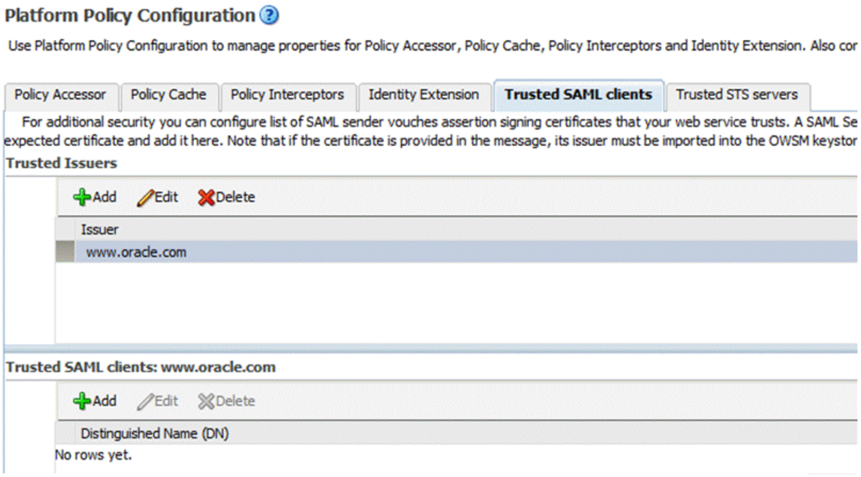
Figure 2–10 WebLogic Domain Drop-down List



11. Click the **Trusted SAML clients** tab in the Platform Policy Configuration page.

12. Select `www.oracle.com` issuer in the Trusted Issuers pane.

Figure 2–11 Platform Policy Configuration



Platform Policy Configuration

Use Platform Policy Configuration to manage properties for Policy Accessor, Policy Cache, Policy Interceptors and Identity Extension. Also cor

For additional security you can configure list of SAML sender vouches assertion signing certificates that your web service trusts. A SAML Se
expected certificate and add it here. Note that if the certificate is provided in the message, its issuer must be imported into the OWSM keystor

Trusted Issuers

Issuer
www.oracle.com

Trusted SAML clients: www.oracle.com

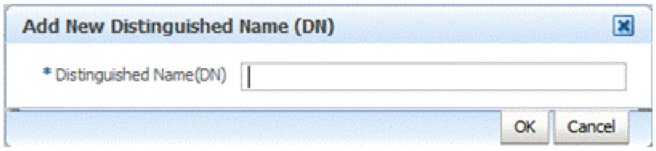
Distinguished Name (DN)

No rows yet.

13. Click **Add** in the Trusted SAML clients: www.oracle.com pane.

    The Add New Distinguished Name (DN) window is displayed.

Figure 2–12 Add New Distinguished Name (DN) Window



14. Add text cn=HSN-PVPR, ou=HSGBU, o=ORACLE, c=US and click **OK**.
15. Repeat steps 12 and 13 to add cn=HSNP, ou=HSGBU, o=ORACLE, c=US as trusted SAML client.
16. Log out of the Enterprise Manager.
17. Create the WebLogic user hsn_system to be used for the HSnP-SOA domain.
18. Restart the WebLogic server instances for the HSnP-SOA domain.

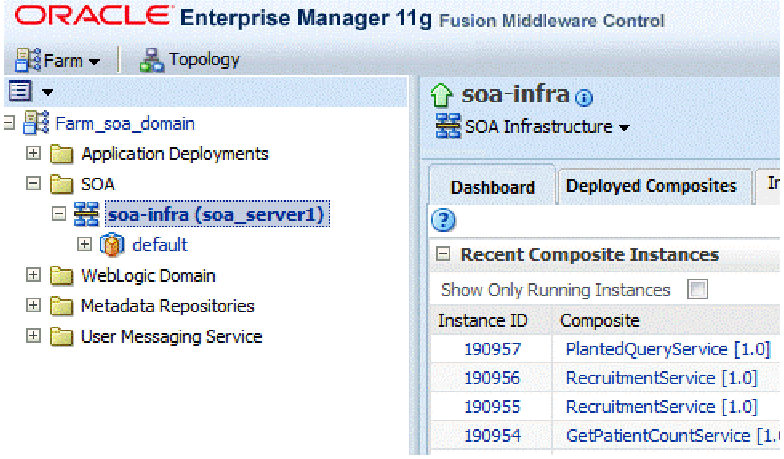
2.4 Configuring SOA MDS

To configure HSN-SOA MDS, perform the following:

1. Extract the soa_mds_<<buildNumber>>.zip file and soa_mds_endpoint_<<buildNumber>>.zip file for MDS from the media pack.
2. Create a folder named apps on your local system and extract the JAR file from the soa_mds_<<buildNumber>>.zip file in the folder.
3. Zip the apps folder.
4. Log in to the Enterprise Manager of the SOA server.
5. Expand **SOA** under **Farm_soa_domain** and click **soa-infra (soa_server1)**.

   The SOA Infra Home Page screen is displayed.

Figure 2–13 SOA Infra Home Page

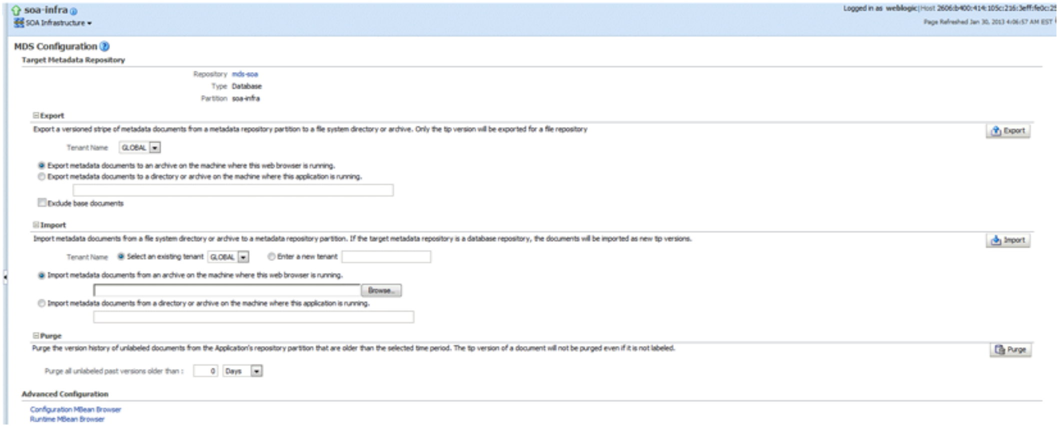


Instance ID	Composite
190957	PlantedQueryService [1.0]
190956	RecruitmentService [1.0]
190955	RecruitmentService [1.0]
190954	GetPatientCountService [1.(

6. Click **SOA Infrastructure**.
7. Select **Administration** and then select **MDS Configuration**.

   The MDS Configuration screen is displayed. This screen lets you import and export MDS archives.

Figure 2–14 MDS Configuration



Logged in as weblogic | Host 2606:b400:414:105c:216:3eff:fe0c:25

Page Refreshed Jan 30, 2013 4:06:57 AM EST

MDS Configuration

Target Metadata Repository

Repository mds-soa

Type Database

Partition soa-infra

Export

Export a versioned stripe of metadata documents from a metadata repository partition to a file system directory or archive. Only the tip version will be exported for a file repository

Tenant Name GLOBAL

● Export metadata documents to an archive on the machine where this web browser is running.

○ Export metadata documents to a directory or archive on the machine where this application is running.

□ Exclude base documents

Import

Import metadata documents from a file system directory or archive to a metadata repository partition. If the target metadata repository is a database repository, the documents will be imported as new tip versions.

Tenant Name ● Select an existing tenant GLOBAL ○ Enter a new tenant

● Import metadata documents from an archive on the machine where this web browser is running.

○ Import metadata documents from a directory or archive on the machine where this application is running.

Purge

Purge the version history of unlabeled documents from the Application's repository partition that are older than the selected time period. The tip version of a document will not be purged even if it is not labeled.

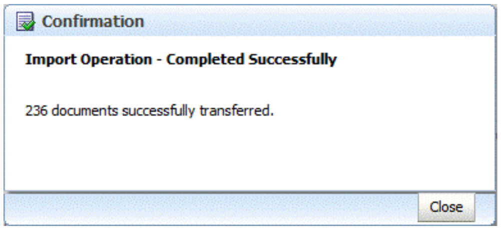
Purge all unlabeled past versions older than : 0 Days

8. Click **Import** and select the apps.zip folder.

Note: You cannot cancel the import operation once it is initiated.

You have successfully imported the archives.

Figure 2–15 Import Operation Successful



Import Operation - Completed Successfully

236 documents successfully transferred.

9. Create a folder named apps on your local system and extract the JAR file from the soa_mds_endpoint_<<buildNumber>>.zip file in the folder.
10. Navigate to the apps\soa_mds\Reference\dvm path within the apps folder.
11. Edit the SOAServiceEndpoint.dvm file.

    This file contains endpoint URL for the SOA and registry services.

    - For SOA services, update the domain and port as per the SOA server details.
    - For registry services, update the domain and port as per the target server where HSnPManApp is deployed.
12. Update the URLs of SOA services as per the target SOA server and registry services as per the ManApp deployment server.
13. Repeat steps 3 through 8 to import the new apps.zip file.

2.5 Configuring HSN Tracking for SOA Composites

This section contains the following topics:

- Section 2.5.1, "Configuring Data Source"
- Section 2.5.2, "Configuring the SOA Server"

2.5.1 Configuring Data Source

To configure data source, perform the following:

1. Log in to the WebLogic console of the SOA server.
2. Create a data source using the ManApp schema credentials.
3. Enter jdbc/HAFDBDS as jndi name and assign it to the SOA server as target server.
4. Restart the SOA server.

2.5.2 Configuring the SOA Server

To configure SOA server, perform the following:

1. Extract the HsnSensor JAR from the media pack.
2. Shut down the server.
3. Copy the HsnSensor-<<buildNumber>>.jar file to <MIDDLEWARE_HOME>/Oracle_SOA1/soa/modules/oracle.soa.ext_11.1.1 on target server.
4. Navigate to <MIDDLEWARE_HOME>/Oracle_SOA1/soa/modules/oracle.soa.ext_11.1.1.
5. Execute the following commands:
   a. `/bin/sh`
   b. `source <MIDDLEWARE_HOME>/wlserver_10.3/server/bin/setWLSEnv.sh`
   c. `ant`
6. Wait for the build successful message.
7. Start the server.

2.6 Setting Transaction Timeout for Service-Oriented Architecture

To set transaction timeout for SOA, the administrator need to set the SyncMaxWaitTime property value in seconds using the following steps:

1. To set timeout for BPEL:
   a. Log in to the Enterprise Manager.
   b. On the left of the navigation menu, expand the **SOA** folder and select **soa-infra (soa_server1)**.
   c. On the right top of the Details screen, expand the **SOA Infrastructure** drop-down menu and select **SOA Administration, BPEL Properties**.

      The BPEL Service Engine Properties screen is displayed.
   d. Click **More BPEL Configuration Properties**.

      The Application Defined MBeans: BPELConfig:bpel screen is displayed.
   e. Edit the SyncMaxWaitTime setting in the list to set timeout to 720 seconds.
2. To set timeout in the SOA EJBs:
   a. Log in to the WebLogic console.
   b. On the left of the navigation menu, click **Deployments**.

c. Click **soa-infra** in the list of deployments.

   The Settings for soa-infra screen is displayed.

d. In the **Modules and Components** list, click each of the following EJBs to increase the transaction timeout value in the corresponding **Configuration** tab.

   BPELEngineBean

   BPELDeliveryBean

   BPELActivityManagerBean

   BPELServerManagerBean

   BPELProcessManagerBean

   BPELInstanceManagerBean

   BPELFinderBean

e. Set the timeout to 960 seconds.

3. To set timeout for JTA:

   a. On the left side of the navigation menu, select **soa_domain** and increase the JTA timeout.

   b. Select **JTA** in the **Configuration** tab.

   c. Set the timeout to 1200 seconds.

2.7 Deploying SOA Composite

You can deploy the following SOA services from their respective JAR files:

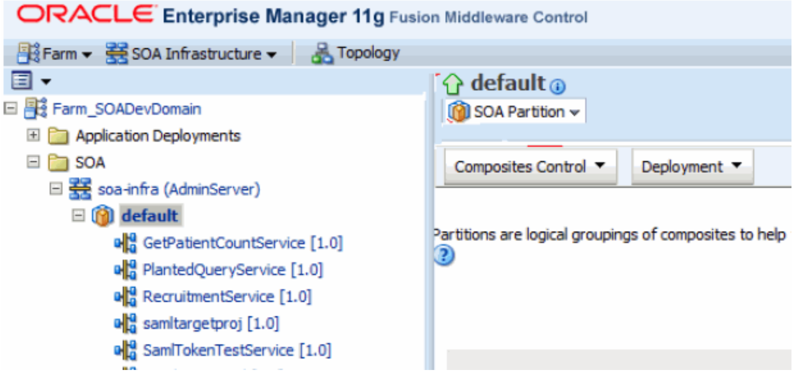
- GetNetworkCountService
- PlantedQuerySerrvice
- RecruitmentService
- GetPatientCountService
- GetCriteriaAnalysisCountService

To deploy SOA services, perform the following:

1. Extract the following files from the media pack:
   - sca_NetworkCountService_rev<<buildNumber>>.jar
   - sca_PlantedQueryService_rev<<buildNumber>>.jar
   - sca_RecruitmentService_rev<<buildNumber>>.jar
   - sca_GetPatientCountService_rev<<buildNumber>>.jar
   - sca_CriteriaSetAnalysisService_rev<<buildNumber>>.jar
2. Log in to the Enterprise Manager of the SOA server.
3. Expand **SOA** and select **default**.

   The Enterprise Manager - SOA Default Node screen is displayed.

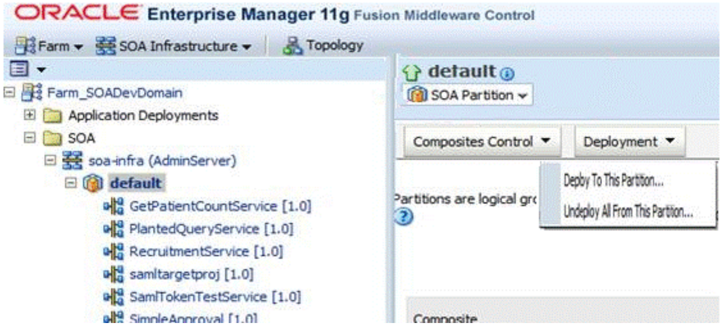
Figure 2–16 Enterprise Manager - SOA Default Node



Partitions are logical groupings of composites to help

4. From **SOA Partition**, select **Deployment** and then select **Undeploy All From This Partition**.

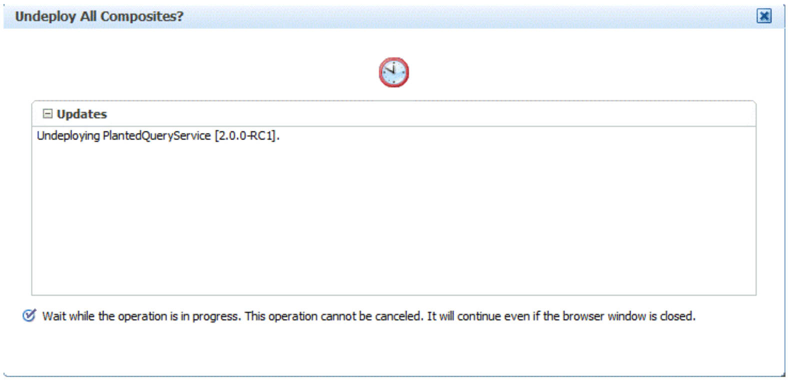
Figure 2–17 Undeploying Composites from a Partition



Partitions are logical grc

All the available composites are undeployed from the server.

Figure 2–18 Undeploying Composites



Undeploying PlantedQueryService [2.0.0-RC1].

Wait while the operation is in progress. This operation cannot be canceled. It will continue even if the browser window is closed.

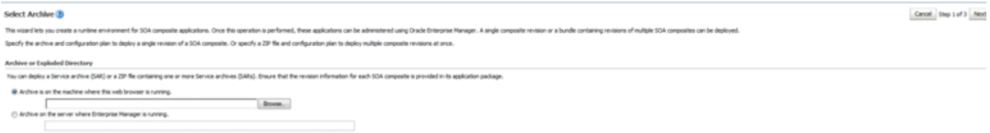
Note: You cannot stop the undeploying operation once it is initiated.

---

5. From **SOA Partition,** select **Deployment** and then select **Deploy To This Partition.**

6. Select the deployable composite JAR from your system and keep clicking **Next.**

Figure 2–19 Selecting an Archive



Select Archive

This wizard lets you create a runtime environment for SOA composite applications. Once this operation is performed, these applications can be administered using Oracle Enterprise Manager. A single composite revision or a bundle containing revisions of multiple SOA composites can be deployed.

Specify the archive and configuration plan to deploy a single revision of a SOA composite. Or specify a ZIP file and configuration plan to deploy multiple composite revisions at once.

Archive or Exploded Directory

You can deploy a Service archive (SAR) or a ZIP file containing one or more Service archives (SARs). Ensure that the revision information for each SOA composite is provided in its application package.

● Archive is on the machine where this web browser is running.

○ Archive on the server where Enterprise Manager is running.

The selected JAR file is deployed on the SOA server.

7. Repeat step 6 to deploy all the required services.

3 Installing PVPR

This chapter contains the following sections:

- Section 3.1, "Installing PVPR Database"
- Section 3.2, "Installing the PVPR Middle-Tier"
- Section 3.3, "Configuring Logging"
- Section 3.4, "Configuring Oracle Web Services Manager"

3.1 Installing PVPR Database

This section describes how to create schema for PVPR.

This section contains the following topics:

- Section 3.1.1, "Prerequisites"
- Section 3.1.2, "Creating PVPR Tablespace"
- Section 3.1.3, "Creating PVPR Database User"
- Section 3.1.4, "Granting Privileges and Creating Synonyms"
- Section 3.1.6, "Installing PVPR Database Objects"

3.1.1 Prerequisites

- The CDM installation for PVPR is completed.
- The ODB (if required) installation for PVPR is completed.
- Registry is configured with a new company and required services are provisioned to it.

The CDM installation scripts are part of installable bundle and are to be used for CDM installation. For a summary of steps involved in installing CDM, see Section 3.1.1.1.

If Omics Lite features are supported or used by a company, then Omics Data Bank (ODB) installation is also completed. For sponsor environment, ODB is to be installed if it has to query or perform recruitment on any partner on an Omics criterion. For provider environment, ODB is to be installed if the company supports Omics.

The ODB installation scripts are part of the installable bundle and are to be used for ODB installation. For a summary of steps involved in installing ODB, see Section 3.1.1.2.

3.1.1.1 Installing CDM

To install CDM, perform the following:

1. Create CDM data tablespace.
2. Create CDM Index tablespace.
3. Create CDM user.
4. Provide maximum quota for the CDM user on the data tablespace.
5. Create the following Datamart roles:
   - CohortDatamartUser;
   - CohortDatamartAdmin;
6. Provide grants to the CDM user by executing the `grant_schema_priv.sql` file in the cdm-odb folder.
7. Execute the CDM installation script by running the `install_cdm.sql` script, giving the runtime parameters as specified in the TRC installation guidelines.

For more information on how to install CDM, see *Oracle Health Sciences Translational Research Center Installation Guide (release 3.0.1)*.

3.1.1.2 Installing ODB

To install ODB, perform the following:

1. Create ODB data tablespace.
2. Create ODB Index tablespace.
3. Create ODB LOB tablespace.
4. Create ODB user.
5. Provide maximum quota for the ODB user on the Data tablespace.
6. Provide grants to the ODB user by executing the `grant_schema_priv.sql` file in the cdm-odb folder.
7. Execute the ODB installation script by running the `install_ODB.sh` script in the odb_install folder, giving the runtime parameters as specified in the ODB installation guidelines.

For more information on how to install ODB, see *Oracle Health Sciences Omics Data Bank Installation Guide (release 3.0.1).*

3.1.2 Creating PVPR Tablespace

To create tablespace for the PVRR database, perform the following:

1. Log in to the database as a user with privilege to create tablespace.
2. Execute the `pvpr_create_tablespace.sql` script.
3. Edit the `pvpr_create_tablespace.sql` script.
4. Enter the following details:
   - Appropriate path for the datafile (line starting with datafile)
   - Size and autoextend size (line starting with SIZE)
5. Log in to the database as system user and execute the script. When prompted, enter the name of the tablespace you want to create.

3.1.3 Creating PVPR Database User

To create PVPR database user, perform the following:

1. Log in to the database as a user with privilege to create user.
2. In the SQLPlus prompt, execute the `@pvpr_create_user.sql` script.
3. Enter the corresponding values as prompted.

> **Note:** Ensure that you specify the tablespace name created in Section 3.1.2 when prompted.

3.1.4 Granting Privileges and Creating Synonyms

PVPR need to access the tables and views of CDM and ODB, and so you must grant privileges and create synonyms.

To grant privileges and create synonyms, perform the following:

CDM Installation

If only CDM is installed, then:

1. Go to the PVPR/SQL folder and run the following scripts:
   - `grant_cdm_select.sql`
   - `create_synonyms.sql`
2. Enter the values when prompted.

CDM-ODB Installation

If both CDM and are installed, then:

1. Go to the CDM-ODB-Install folder and edit the `install_final.sql` script.
2. Run the `install_final.sql` script.
3. Enter the values when prompted.

3.1.5 Configuring Dimension Data Export and Import

The dimension data from the Provider side should be exported and then imported on to the Sponsor side. From the Provider side, the dimension data is exported as files to the Sponser side. The data from these files is loaded to the dimension tables at Sponser side.

To configure dimension data export and import, perform the following:

1. In the SQLPlus prompt, log in as sys user and execute the following:
   - CREATE OR REPLACE DIRECTORY PVPR_EXT_TAB_DIR AS '&&pvpr_external_dir';
   - GRANT read, write on directory PVPR_EXT_TAB_DIR to &&pvpr_user;
   - GRANT read, write on directory PVPR_EXT_TAB_DIR to &&cdm_user;

Notes:

- Replace `&&pvpr_external_dir` with the actual directory path in the database machine where you want to save the files.
- Replace `&&pvpr_user` with the schema name of the PVPR user.
- Replace &&cdm_user with the schema name of the CDM user.

2. If the installation is done for a Sponsor, then from the SQLPlus promt, execute the @PV_install_dim_ddl.sql script in the PVPR/SQL folder and enter the values as prompted.

3.1.6 Installing PVPR Database Objects

This section describes how to create database objects such as tables and procedures for PVPR, and to initialize the database with seed data.

1. In the SQL prompt, execute `@install_pvpr_env.sql` by providing the values as prompted.
2. Connect to the database as PVPR user.
3. In the SQL prompt, execute `@config_pvpr_env.sql`. This script prompts for the following inputs:
    - **SOA Server URL:** URL of the server where SOA services are deployed.
    - **SOA Server PORT:** Port of the SOA server.
    - **HSn-ManApp Server URL:** URL of the server where Hsn-ManApp is deployed.
    - **HSn-ManApp Server PORT:** Port of the Hsn-ManApp server.
    - **PVPR Server URL:** URL of the server where PVPR is deployed.
    - **PVPR Server PORT:** Port of the PVPR server.
    - **My Company Id:** You need to configure the company ID during registry configuration of Hsn-ManApp.
    - **My Company Name:** You need to configure the company name during registry configuration of Hsn-ManApp.
    - **Is Omics Supported (Y/N):** Enter Y if Omics features are supported or used. Otherwise, enter N.

This configures the company ID, company name, and service URLs of the platform services in the PVPR application.

Seed Data

The initial seed data required for PVPR is populated as part of the preceeding PVPR database installation. This includes the default roles and privileges, among other basic data.

The default dimension codes for Gender and Marital Status codes are also included as a part of the preceeding installation.

Running Post-Installation Scripts

During schema creation, access rights are granted to the schema user, which are required only for database configuration. Post database schema creation, the access rights need to be revoked. The access rights are revoked using post-installation scripts.

1. Connect to the database as a user with sysdba privilege.
2. Run the `@pvpr_post_install.sql` script.

3.1.7 Loading Data to ODB and CDM

After the database is installed, the data is loaded to ODB and CDM.

3.1.7.1 Loading Data to ODB

At the Sponsor side, only the ODB reference data is required. Since this release supports only the searches by gene and mutation, only the EMBL and GVF reference loaders are required. However, the Providers require both reference loaders and result loaders. For more information on how to load data to ODB, see *Oracle Health Sciences Omics Data Bank Programmer's Guide (release 3.0.1)*.

3.1.7.2 Loading Data to CDM

At the Sponsor side, only the CDM reference data is required. However, the reference (dimension) data has to be loaded from each Provider.

At the Provider side, perform the following steps to export data:

1. In the SQLPlus prompt, execute the `@PR_run_exp_data_dim.sql` script in the PVPR/SQL/ref-data folder.
2. Enter the values as prompted.

The required dimension data is exported into files present in the configured external directory. For more details, see Section 3.1.5.

At the Sponsor side, perform the following steps to load the data from the data files into the actual Sponsor dimension tables.

1. In the SQLPlus prompt, execute the `@PV_merge_dim.sql` script in the PVPR/SQL/ref-data folder.
2. Enter the values as prompted.

3.2 Installing the PVPR Middle-Tier

This section explains how to install the PVPR Middle-Tier.

3.2.1 Creating Data Source in the Oracle WebLogic Server

To create data source in the Oracle WebLogic server, perform the following:

1. Log in to the Oracle WebLogic server console.
2. Create a new data source by providing the following details:
   - **Data Source Name:** Specify a name that represents the underlying database schema and environment. For example, JDBC-DS-Provider1
   - **JNDI Name:** jdbc/PVPR.
3. Specify the PVPR database user and password on the Connection Pool details screen.

4. Specify database connection details for the PVPR database.
5. Apply the data source to the server in the Targets section.

3.2.2 Setting Transaction Timeout for the WebLogic Application Server

To set transaction timeout for the WebLogic application server, perform the following:

1. Go to **Services > JTA** in the WebLogic console.
2. Update timeout seconds to 600 and save.

3.2.3 Enabling JPA 2.0 and Jackson

To enable JPA 2.0 and Jackson, perform the following:

1. Edit the <MIDDLEWARE_HOME>/wlserver_10.3/common/bin/commEnv.sh file to add the PRE_CLASSPATH variable at the end of the file.
2. Verify JAR version number in the <MIDDLEWARE_HOME>/modules folder and update the following statement accordingly:

   ```
   PRE_CLASSPATH=${MODULES_DIR}/javax.persistence_1.1.0.0_2-

   0.jar:${MODULES_DIR}/com.oracle.jpa2support_1.0.0.0_2-

   1.jar:${MODULES_DIR}/org.codehaus.jackson.mapper.asl_1.0.0.0_1-8-

   3.jar:${MODULES_DIR}/org.codehaus.jackson.core.asl_1.0.0.0_1-8-3.jar

   export PRE_CLASSPATH
   ```

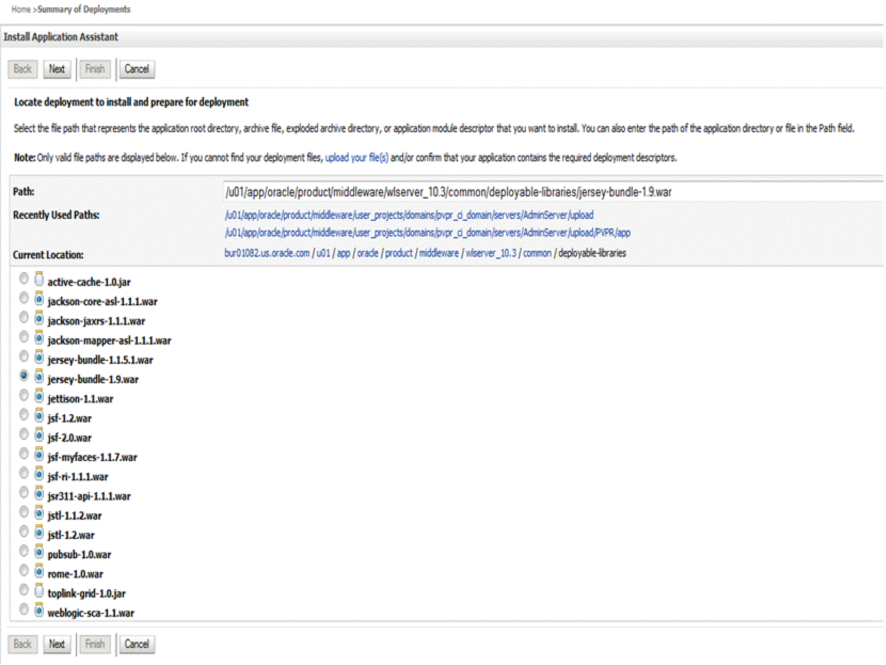
3.2.4 Referring Shared Jersey Library

To refer shared jersey libraries from PVPR, perform the following:

1. From the Administration Console, click **Summary of Deployment**.
2. Click **Install**.

   The Install Application Assistant screen is displayed.
3. Navigate to the required path and select the required JAR file as shown in the figures 3-1, 3-2, and 3-3:

Figure 3–1 Install Application Assistant



Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or file in the Path field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the required deployment descriptors.

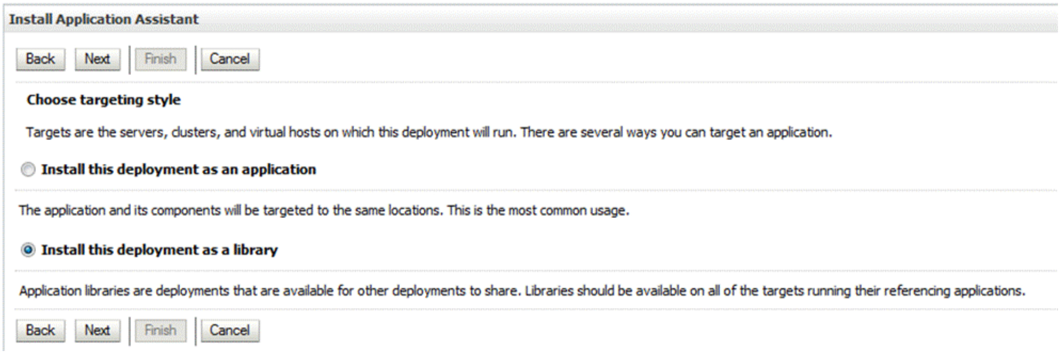
Path: /u01/app/oracle/product/middleware/wlserver_10.3/common/deployable-libraries/jersey-bundle-1.9.war

Recently Used Paths:
/u01/app/oracle/product/middleware/user_projects/domains/pvpr_ci_domain/servers/AdminServer/upload
/u01/app/oracle/product/middleware/user_projects/domains/pvpr_ci_domain/servers/AdminServer/upload/PVPR/app

Current Location: bur01082.us.oracle.com / u01 / app / oracle / product / middleware / wlserver_10.3 / common / deployable-libraries

○ active-cache-1.0.jar
○ jackson-core-asl-1.1.1.war
○ jackson-jaxrs-1.1.1.war
○ jackson-mapper-asl-1.1.1.war
○ jersey-bundle-1.1.5.1.war
● jersey-bundle-1.9.war
○ jettison-1.1.war
○ jsf-1.2.war
○ jsf-2.0.war
○ jsf-myfaces-1.1.7.war
○ jsf-ri-1.1.1.war
○ jsr311-api-1.1.1.war
○ jstl-1.1.2.war
○ jstl-1.2.war
○ pubsub-1.0.war
○ rome-1.0.war
○ toplink-grid-1.0.jar
○ weblogic-sca-1.1.war

Figure 3–2 Install Application Assistant - Choose Targeting Style



Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

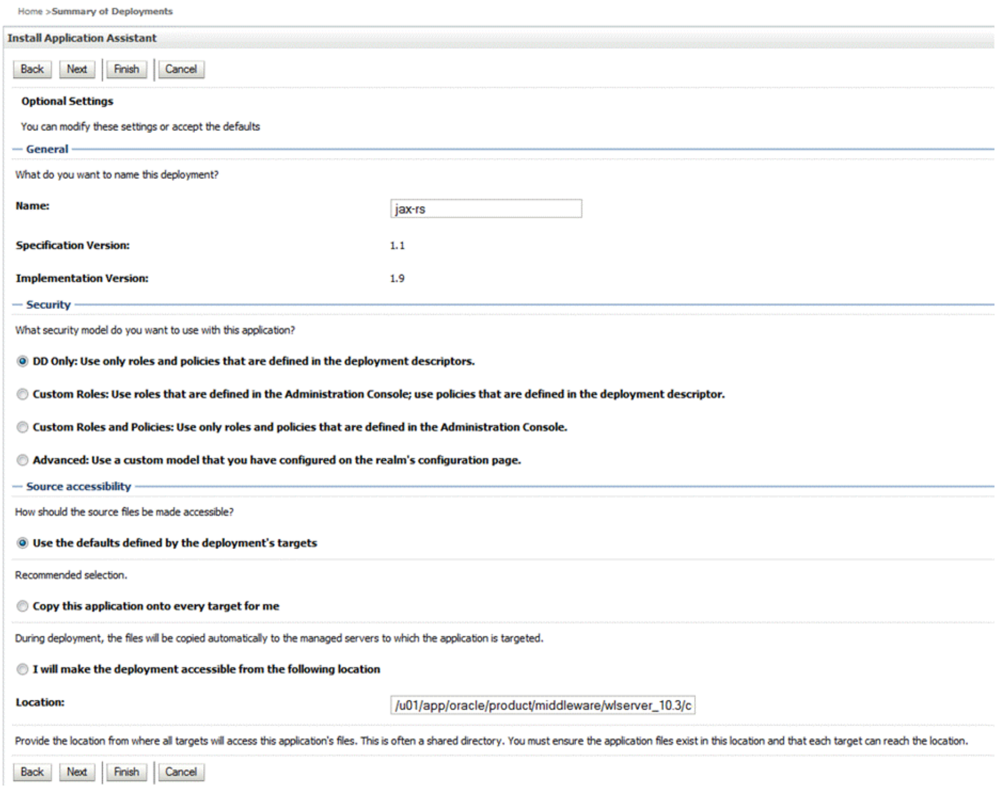
○ **Install this deployment as an application**

The application and its components will be targeted to the same locations. This is the most common usage.

● **Install this deployment as a library**

Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

Figure 3–3 Install Application Assistant - Optional Settings



Optional Settings

You can modify these settings or accept the defaults

General

What do you want to name this deployment?

Name: jax-rs

Specification Version: 1.1

Implementation Version: 1.9

Security

What security model do you want to use with this application?

● **DD Only: Use only roles and policies that are defined in the deployment descriptors.**

○ **Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.**

○ **Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.**

○ **Advanced: Use a custom model that you have configured on the realm's configuration page.**

Source accessibility

How should the source files be made accessible?

● **Use the defaults defined by the deployment's targets**

Recommended selection.

○ **Copy this application onto every target for me**

During deployment, the files will be copied automatically to the managed servers to which the application is targeted.

○ **I will make the deployment accessible from the following location**

Location: /u01/app/oracle/product/middleware/wlserver_10.3/c

Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

3.2.5 Deploying EAR

To deploy EAR, perform the following:

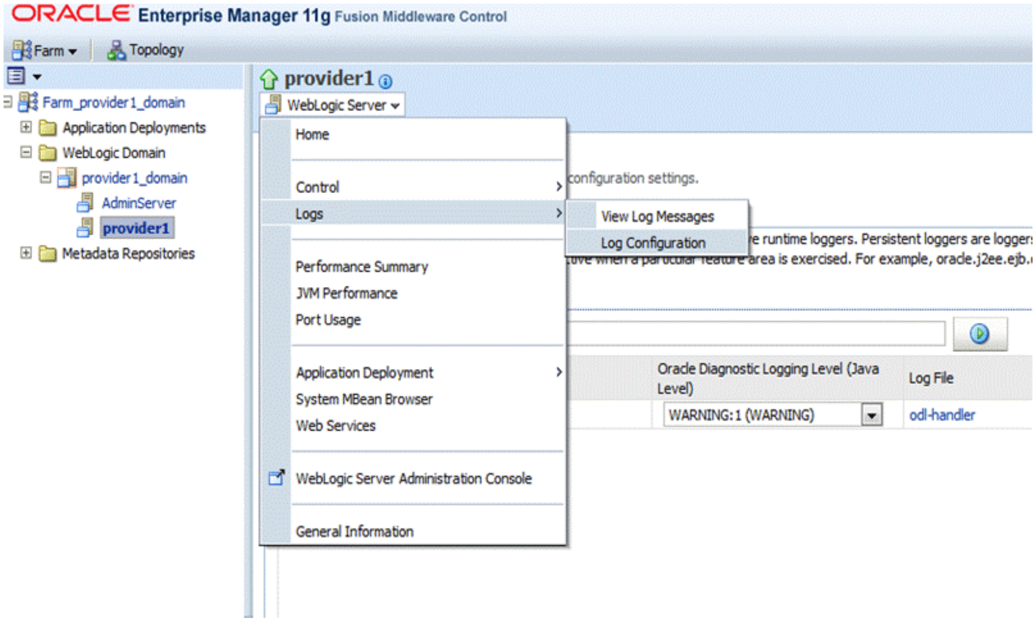
1. Extract the PVPR EAR file from the media pack.
2. Deploy the EAR file to the server, where PVPR need to be installed.

3.3 Configuring Logging

To configure logging, perform the following:

1. Log in to the Enterprise Manager.
2. In the pane on the left side of the window, click **pvpr domain** in the WebLogic Domain folder and select the target pvpr server.
3. From the **WebLogic Server** drop-down list, select **Logs** and then select **Log Configuration**.

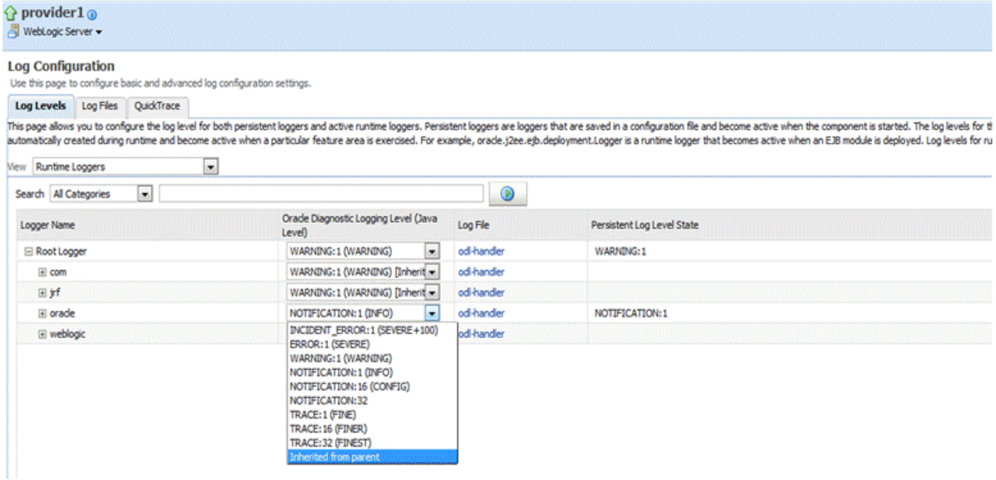
Figure 3–4 Log Configuration



4. Expand **Root Logger**.

5. For Oracle, change the log level and select **Inherited from Parent**.

Figure 3–5 Root Logger



Log Configuration

Use this page to configure basic and advanced log configuration settings.

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are loggers that are saved in a configuration file and become active when the component is started. The log levels for t
automatically created during runtime and become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime logger that becomes active when an EJB module is deployed. Log levels for ru

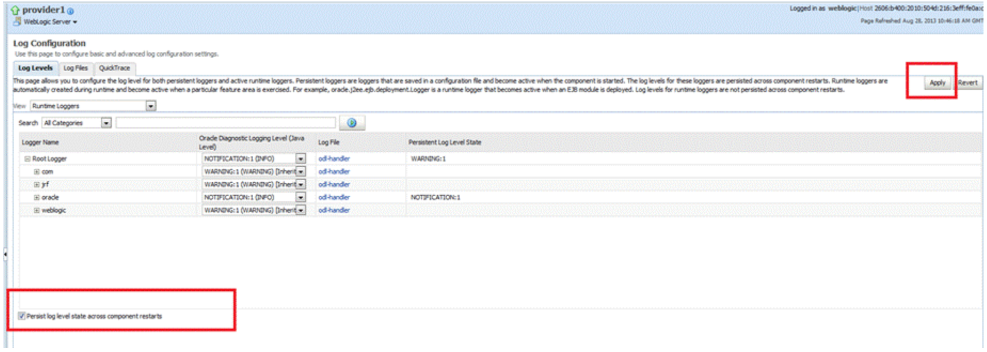
View: Runtime Loggers

Search: All Categories

Logger Name	Oracle Diagnostic Logging Level (Java Level)	Log File	Persistent Log Level State
⊟ Root Logger	WARNING:1 (WARNING)	odl-handler	WARNING:1
⊞ com	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ jrf	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ oracle	NOTIFICATION:1 (INFO)	odl-handler	NOTIFICATION:1
⊞ weblogic		odl-handler	

6. Select **Persist log level state across component restarts** and click **Apply Changes**.

Figure 3–6 Log Levels



provider1
WebLogic Server

Logged in as weblogic | Host 2606:b400:2010:504d:216:3eff:fe0a:c
Page Refreshed Aug 28, 2013 10:46:18 AM GMT

Log Configuration

Use this page to configure basic and advanced log configuration settings.

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are loggers that are saved in a configuration file and become active when the component is started. The log levels for these loggers are persisted across component restarts. Runtime loggers are automatically created during runtime and become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime logger that becomes active when an EJB module is deployed. Log levels for runtime loggers are not persisted across component restarts.

View: Runtime Loggers

Search: All Categories

Logger Name	Oracle Diagnostic Logging Level (Java Level)	Log File	Persistent Log Level State
⊟ Root Logger	NOTIFICATION:1 (INFO)	odl-handler	WARNING:1
⊞ com	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ jrf	WARNING:1 (WARNING) [Inherit	odl-handler	
⊞ oracle	NOTIFICATION:1 (INFO)	odl-handler	NOTIFICATION:1
⊞ weblogic	WARNING:1 (WARNING) [Inherit	odl-handler	

☑ Persist log level state across component restarts

3.4 Configuring Oracle Web Services Manager

This section contains the following topics:

- Section 3.4.1, "Generating Keystore and Configuring Trusted Certificate"
- Section 3.4.2, "Configuring Keystore on HSnP and SOA Server"
- Section 3.4.3, "Keystore Configuration on PVPR Server"

3.4.1 Generating Keystore and Configuring Trusted Certificate

---

Note: : You need to perfrom the following steps only once. Share the generated and updated keystore file for all the PVPR instances.

To execute the following commands, you need to set the JAVA_HOME environment variable to point to JDK (version 1.6 and later) referred in the PVPR domain.

- `export JAVA_HOME=<Path to JDK referred with pvpr domain>`
- `export PATH=$JAVA_HOME/bin:$PATH`

1. Generate the private key to be used in the PVPR servers using the keytool utility available in JDK.
2. In the following command, replace <KEY_LOCATION> as required:

   ```
   keytool -genkey -alias hsn-pvpr-key -keyalg "RSA" -sigalg "SHA1withRSA"
   -dname "cn=HSN-PVPR,ou=HSGBU,o=ORACLE,c=US" -keystore <KEY_
   LOCATION>/pvprkey.jks -validity 3650
   ```

   a. Enter the keystore password and the key password when prompted.
3. Export the certificate of pvprkey using the following command:

Note: Replace <PVPR_KEY_LOCATION>, <PVPR_CERTIFICATE_LOCATION>, <HSNP_KEY_LOCATION>, and <HSNP_CERTIFICATE_LOCATION as required in the following steps.

   ```
   keytool -export -alias hsn-pvpr-key -keystore <PVPR_KEY_LOCATION
   >/pvprkey.jks -file <PVPR_CERTIFICATE_LOCATION>/hsn-pvpr.cer
   ```

   a. Enter the keystore password when prompted.

4. Copy hsnpkey.jks from the HSNP ManApp server.

   For more information on <HSNP_KEY_LOCATION>/hsnpkey.jks, see Section 2.2.6.

5. Export the certificate of hsnp-key using the following command:

   ```
   keytool -exportcert -alias hsnp-key -keystore <HSNP_KEY_
   LOCATION>/hsnpkey.jks -file <HSNP_CERTIFICATE_LOCATION>/hsnp.cer
   ```

   a. Enter the keystore password when prompted.

6. Use the following commands to import the keys in other keystore files for the trust:

   - Command to import hsnp-key certificate to pvprkey:

     ```
     keytool -import -alias hsnp-key -file <HSNP_CERTIFICATE_
     LOCATION>/hsnp.cer -keystore <PVPR_KEY_LOCATION>/pvprkey.jks
     ```

   - Commands to import hsn-pvpr-key and orakey certificates to hsnpkey:

     Note: Enter the keystore password when prompted.

     ```
     keytool -import -alias hsn-pvpr-key -file <PVPR_CERTIFICATE_
     LOCATION>/hsn-pvpr.cer -keystore <HSNP_KEY_LOCATION>/hsnpkey.jks
     ```

     ```
     keytool -import -alias orakey -file <PVPR_CERTIFICATE_
     LOCATION>/hsn-pvpr.cer -keystore <HSNP_KEY_LOCATION>/hsnpkey.jks
     ```

3.4.2 Configuring Keystore on HSnP and SOA Server

Note: You need to perform the following steps only once.

1. Copy the updated keystore hsnpkey.jks to the <HSNP_DOMAIN_HOME>/config/fmwconfig folder. You must perform this step on the HSnP SOA server also.
2. Restart the WebLogic server instances for HSnP and the SOA domain.

3.4.3 Keystore Configuration on PVPR Server

To configure keystore on the PVPR server, perform the following:

1. Copy the generated keystore pvprkey.jks to the <PVPR_DOMAIN_HOME>/config/fmwconfig folder.
2. Open the <PVPR_DOMAIN_HOME>/config/fmwconfig/jps-config.xml file.
3. Search for `default-keystore.jks` in the file.

   It should be similar to the following:

   <serviceinstance name="keystore" provider="keystore.provider" location="./default-keystore.jks">
4. Replace `./default-keystore.jks` with `./pvprkey.jks` and save the file.
5. Restart the WebLogic server instances for the PVPR domain.

6. Copy the PVPR_OWSM_Config.py file from the media pack to a location to which the operating system user has read and execute permissions.

7. Execute the following commands on the command prompt:

   - `cd <MIDDLEWARE_HOME>/oracle_common/common/bin`
   - `./wlst.sh <ABSOLUTE FILE_PATH to PVPR_OWSM_Config.py>`

     a. Enter corresponding values as prompted by the script.

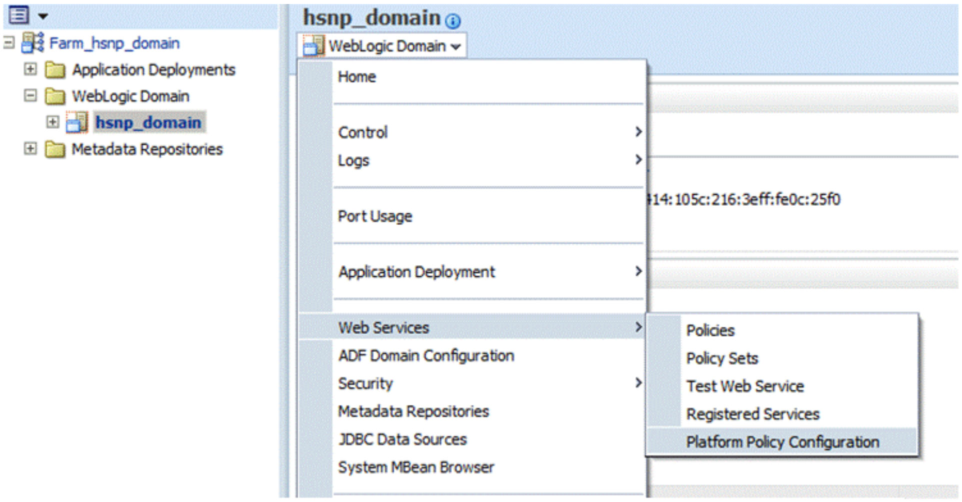
   The PVPR_OWSM_Config.py file adds credentials for the pvprkey.jks file.

8. Login to the Enterprise Manager of the PVPR domain.

9. In the left pane, click **pvpr** domain in the WebLogic domain folder.

10. From the **WebLogic Domain** drop-down list, select **Web Services** and then select **Platform Policy Configuration**.

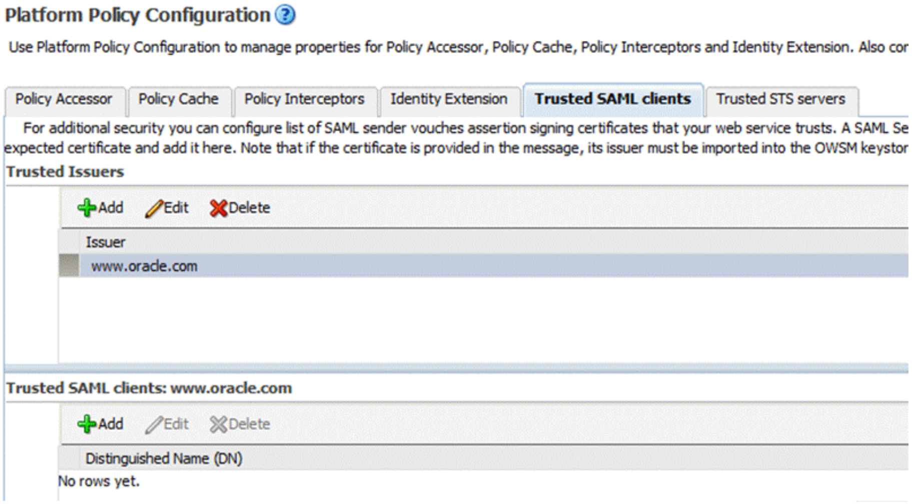
Figure 3–7 WebLogic Domain Drop-down List



11. Click the **Trusted SAML clients** tab in the Platform Policy Configuration page.

12. Select `www.oracle.com` issuer in the Trusted Issuers pane.

Figure 3–8 Platform Policy Configuration



Platform Policy Configuration

Use Platform Policy Configuration to manage properties for Policy Accessor, Policy Cache, Policy Interceptors and Identity Extension. Also cor

For additional security you can configure list of SAML sender vouches assertion signing certificates that your web service trusts. A SAML Se expected certificate and add it here. Note that if the certificate is provided in the message, its issuer must be imported into the OWSM keystor

Trusted Issuers

Issuer
www.oracle.com

Trusted SAML clients: www.oracle.com

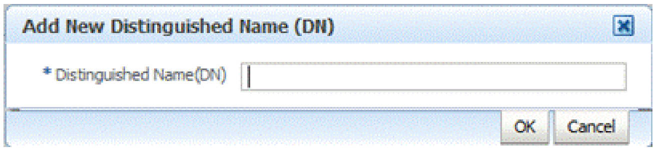
Distinguished Name (DN)

No rows yet.

13. Click **Add** in the Trusted SAML clients: www.oracle.com pane.

    The Add New Distinguished Name (DN) window is displayed.

Figure 3–9 Add New Distinguished Name (DN) Window



Add New Distinguished Name (DN)

* Distinguished Name(DN)

14. Add text cn=HSNP, ou=HSGBU, o=ORACLE, c=US and click **OK**.
15. Click **Apply**.
16. Log out of the Enterprise Manager.
17. Create the WebLogic user hsn_system, to be used for the PVPR domain.
18. Restart the WebLogic server instances for the PVPR domain.

4 Configuring Registry

Through the registry configuration feature, you can perform the following:

- Create companies (hospitals, pharmaceutical companies, research institutes, and so on) that participate on the HSN network.
- Provision service to companies in offer or consumer mode.
- Create relationship between companies for a service.
- Define restriction for a relationship.

SQL scripts are used to configure registry.

You can define the following restrictions for a relationship:

- Data restriction
- Protocol limit

Note: Restrictions are set of policies through which a provider company (Provider) can restrict a consumer company (Sponsor) on a provisioned service usage. For example, a provider company can restrict number of protocols a consumer company can use.

This chapter contains the following topics:

- Section 4.1, "Creating Seed Data"
- Section 4.2, "Creating Company"
- Section 4.3, "Provisioning Service"
- Section 4.4, "Creating Relationship"
- Section 4.5, "Updating Company"
- Section 4.6, "Deleting Provision"

Note: Log in to the database as a HSN user before executing the scripts provided in the following sections.

4.1 Creating Seed Data

To create static seed data required for registry configuration, execute the `App_Service_Capability.sql` seed script.

Note: You need to execute this script under the user created in Section 2.1.2.

This script first deletes the existing entries and creates preconfigured entries in the following tables:

- APP: Creates single entry for application as PVPR_APP and Application ID (appId) as 1.
- Service: The application offers the following services:
  - QUERYCOUNT (Validation service)
  - RECRUITMENT (Recruitment service)
  - CRITERIAANALYSIS (Criteria Analysis service)
  - OMICS (Omics service)
- APP_CAPABILITY: This table contains mode for each that the application supports.

4.2 Creating Company

To create a company and provision an existing application to the company, execute the `Company_AppProvision.sql` script. Enter the following details:

- Name of the company.

  For example, Company1.
- URL of the PVPR application instance.

  For example, if the PVPR application for the company is deployed at http://<server name>:<port number>, the URL should be http://<server name>:<port number>.

Note: If you specify wrong URL, the HSNP.SERVICE.001 is displayed.

The `Company_AppProvision.sql` script creates entries in the following tables:

- Company
- APP_PROVISIONED

You can update the company name or URL using the `Update_Company_AppProvision.sql` script.

4.3 Provisioning Service

To provision a service to a company in consume or offer mode, execute the `Provision_Service.sql` script. By default, this script creates the activation policy for the company.

Enter the following details:

- Company Name: Name of the company to which you want to provision a service.
- Service Name: Name of the service that you want to provision.

- Consume Mode: Set to Y for service to be provisioned in the consume mode, else set to N.
- Offer Mode: Set to Y for service to be provisioned in offer mode, else set to N.

Is relationship required for consuming the service, if offered (Y/N) -

- Y - Service is accessible only if there is a relationship created between sponsor and provider.
- N - Service is accessible by all sponsors participating in the network without any restrictions.

Currently, service that can be provisioned for offer or consume mode can be any one of the services mentioned in the Creating Seed Data section.

The `Provision_Service.sql` script creates entries in the following tables:

- USE_POLICY
- POLICY

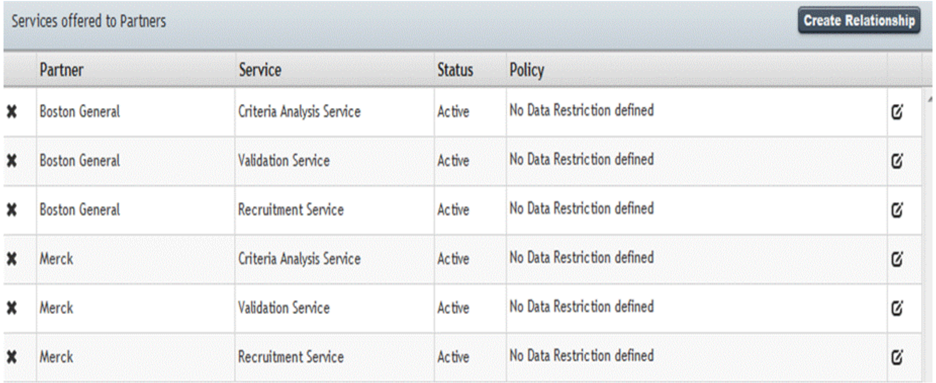
4.4 Creating Relationship

You can create a relationship between two companies to share protocols or for querying patient counts for a protocol.

Companies can offer or consume a service. Services offered to a company can be managed from the company admin screen. A user with the pr_admin role can restrict access to number of protocols and diagnosis codes.

The PVPR Company Admin screen displays the details of services offered to a company along with the status of the service and policies applied on the service.

Figure 4–1 PVPR Company Admin Screen



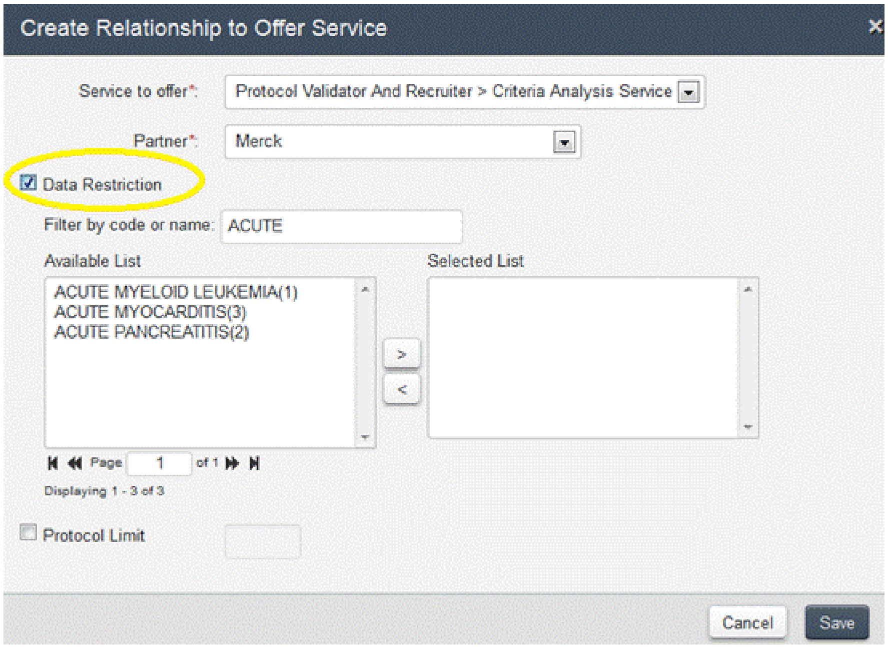
Services offered to Partners

	Partner	Service	Status	Policy	
✖	Boston General	Criteria Analysis Service	Active	No Data Restriction defined	✎
✖	Boston General	Validation Service	Active	No Data Restriction defined	✎
✖	Boston General	Recruitment Service	Active	No Data Restriction defined	✎
✖	Merck	Criteria Analysis Service	Active	No Data Restriction defined	✎
✖	Merck	Validation Service	Active	No Data Restriction defined	✎
✖	Merck	Recruitment Service	Active	No Data Restriction defined	✎

The admin can use the Create Relationship option to:

- Configure the available services to sponsors.
- Apply restrictions on a relationship with sponsor for the selected service.
- Update the existing restrictions defined for the relationship for the services to a sponsor.

Figure 4–2 Create Relationship



Create Relationship to Offer Service

Service to offer*: Protocol Validator And Recruiter > Criteria Analysis Service

Partner*: Merck

☑ Data Restriction

Filter by code or name: ACUTE

Available List

ACUTE MYELOID LEUKEMIA(1)
ACUTE MYOCARDITIS(3)
ACUTE PANCREATITIS(2)

Selected List

Page 1 of 1

Displaying 1 - 3 of 3

☐ Protocol Limit

- **Data Restriction**: to restrict the sponsor to query only for the selected diagnostic codes.
- **Protocol Limit**: to restrict the sponsor to consume the service for the specified number of protocols.

4.5 Updating Company

You can update a company name, or URL, or both. To update, execute the `Update_Company_AppProvision.sql` script.

Note: The URL would be the PVPR application instance URL for the company.

You have to enter the existing company name while updating the company name or URL.

4.6 Deleting Provision

To delete a de-provision service to a company, execute the `Delete_Provision_Service.sql` script. Enter the following details:

- Company Name: Name of the company from which you want to delete the service.
- Service Name: Name of the service that you want to delete.
- Consume Mode: Set to Y for service to be removed for consume mode, else set to N.
- Offer Mode: Set to Y for service to be removed for offer mode, else set to N.

The script deletes entries in the following tables:

- USE_POLICY
- POLICY