Oracle® Health Sciences Information Manager

Policy Engine Installation and Configuration Guide

Release 1.2

E22759-01

June 2011

Oracle Health Sciences Information Manager Policy Engine Installation and Configuration Guide, Release 1.2

E22759-01

Primary Author: Louis J. Kraft

Contents

Preface

Oracle Health Sciences Information Manager (OHIM) leverages the CONNECT open source, reference architecture and Oracle server virtualization to provide a broad range of international-standards-based web services to HIE applications in a management and performanceoptimized solution, an ideal complement to the Oracle Exadata hardware appliance and pre-installed Oracle VM.

Audience

This document is intended for users who plan to install and configure the OHIM Policy Engine components and templates, and configure the CONNECT software on the Oracle Health Sciences Information Gateway (OHIG) Adapter and Gateway VMs.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Health Sciences Information Manager Release 1.2 documentation set:

- *Oracle Health Sciences Information Manager Release Notes* (Part Number E22763-01)
- *Oracle Health Sciences Information Manager Record Locator Service Installation and Configuration Guide* (Part Number E22761-01)
- *Oracle Health Sciences Information Manager Policy Monitor Installation and Configuration Guide* (Part Number E22760-01)
- *Oracle Health Sciences Information Manager OHMPI Installation and Configuration Guide* (Part Number E22762-01)

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 Installing and Configuring OHIM Policy Engine

This chapter provides the instructions to install and configure the Policy Engine VM template. Also, it provides the instructions on how to configure CONNECT software on OHIG Adapter/Gateway VMs to make use of openSSO-based Policy Engine.

This chapter includes the following sections:

- "Understanding OHIM Policy Engine Components and Templates"
- "Importing the OHIM Policy Engine Template"
- "Creating the OHIM Policy Engine VM"
- "Configuring the OHIM Policy Engine VM"
- "Installing OHIG Adapter and Gateway VM Certificates on Policy Engine VM"
- "Configuring CONNECT Software on OHIG Adapter VM for OpenSSO Policy Engine"
- "Configuring CONNECT Software on OHIG Gateway VM for OpenSSO Policy Engine"
- "Consumer Preferences Document Creation Using SoapUI"
- "Validating CONNECT on OHIG Gateway and Adapter VMs"
- "Avoiding a Java Security Certificate Exception"

1.1 Understanding OHIM Policy Engine Components and Templates

The OHIM Policy Engine template uses the "Paravirtualized" virtualization method. The template is distributed as a compressed tar file (`*.tgz`). The compressed tar file contains two binary files and a text file. The binary files are the disk images taken from a fully configured and functional VM. The text file is a VM configuration file.

1.1.1 OHIM Policy Engine Components

The contents of the compressed tar file is listed below:

- Disk Image with Oracle Software

  `/appliance.img`

- Disk Image with Operating System

  `/System.img`

- VM Configuration File

  `/vm.cfg`

1.1.2 OHIM Policy Engine VM Template

The VM consists of the following pre-installed software:

- Oracle Enterprise Linux 5 (as in `System.img`)

  http://www.oracle.com/technetwork/topics/linux/whatsnew/index.html

- OHIM specific software (as in `appliance.img`)

  - Apache Ant 1.8.1

    Install directory: `/home/common/ant`

  - Java Development Kit 1.6.0_X

    Install directory: `/home/common/java/latest` *`(symbolic link to JDK 1.6.0_X)`*

  - For hiauser *only*:

    * OHIM Ant Configuration Utility

      Install directory: `/home/hiauser/config`

    * Netbeans 6.7.1

      Install directory: `/home/hiauser/netbeans-6.7.1`

    * Glassfish Enterprise Server 2.1.1

      Install directory: `/home/hiauser/SUNWappserver`

      Admin user

      - Username: `admin`

      - Password: `adminadmin`

      Admin Console

      - `http://`*`<VM_IP or VM_HOST_NAME`* `>:4848`

    * OpenSSO 8.0 Update 2

      Install directory: `/home/hiauser/opensso`

      OpenSSO Admin user

      - Username: `amAdmin`

      - Password: `adminadmin`

      OpenSSO Admin Console

      - `http://`*`<VM_IP or VM_HOST_NAME`* `>:8080/opensso`

- VM Memory Settings:

  - 2 GB (2048 MB) of RAM

> **Note:** The RAM memory setting can be changed after installation in VM Manager.

  - 16 GB of Disk Space
- Linux Users:
  - Root user
    - Username: `root`
    - Linux Group: `root`
    - Password: `ovsroot`
  - OHIM specific user
    - Username: `hiauser`
    - Linux Group: `hiauser`
    - Password: `hiapass`

    Tip: For security purposes, it is recommended that you change the default passwords after installation.

1.2 Importing the OHIM Policy Engine Template

To import the OHIM Policy Engine VM template:

1. Copy the OHIM Policy Engine VM template `.tgz` file to the `/OVS/seed_pool` directory of your Oracle VM Server machine.
2. Uncompress the `.tgz` file:

   ```
   > tar -zxvf <FILENAME>.tgz
   ```

   This step creates a directory with the name of the template.

   Example:

   ```
   > cd /OVS/seed_pool
   > tar -zxvf /OVS/seed_pool/OVM_HIMV12_X86_POLICYENGINE_PVM.tgz
   ```

   Creates the directory:

   `/OVS/seed_pool/OVM_HIMV12_X86_POLICYENGINE_PVM`

   Note: If you are using 64 bits, you would use `OVM_HIMV12_X86_64_POLICYENGINE_PVM`.

3. Log in to the Oracle VM Manager

   Note: The default location for the Oracle VM Manager log in screen is `http://<VM_MANAGER_HOST_NAME>:8888/OVS`.

4. From the Oracle VM Manager console:
   a. Click the **Resources** tab. The Virtual Machine Templates screen is displayed.
   b. Click the **Import** button. The Source screen is displayed.
   c. Choose the **Select from Server Pool (Discover and register)** radio button.
   d. Click **Next**. The General Information screen is displayed.

Enter or select the following general information:

- The server pool on which the virtual machine will be located.

Server Pool Name: <*SERVER_POOL_NAME*>

- The operating system of the Virtual Machine Operating System:

`Oracle Enterprise Linux 5`

- The Oracle VM template to be imported.

Virtual Machine Template Name: <*VM_TEMPLATE_NAME*>

- The username used to log in to the Virtual Machine.

Virtual Machine System Username: `root`

- The password used to log in to the Virtual Machine.

Virtual Machine System Password: `ovsroot`

e. Click **Next**. The Confirm Information screen is displayed.

f. Click **Confirm**. The Virtual Machine Template screen is displayed with a message to confirm the VM template has been imported.

5. Click the **Resources** tab to see the list of available VM templates.
6. To make the Virtual Machine template available for use, select the Virtual Machine template and click **Approve**, moving the VM template from the "Pending" state to the "Active" state.

   The VM template is imported and ready for use in Oracle VM Manager.

1.3 Creating the OHIM Policy Engine VM

To create the OHIM Policy Engine VM from the VM template:

1. Create a new VM using the Policy Engine VM template just installed by following the instructions in the *VM Manager 2.2 User's Guide* (refer to Section 6.3.1, "Creating Virtual Machine from a Template").
2. To power on the Virtual Machine select the **Virtual Machines** tab, select the **Virtual Machine Name**, and click **Power On**.
3. In the VM Manager Console ensure that the Policy Engine VM is now in the running state (Status=Running).

1.4 Configuring the OHIM Policy Engine VM

This section provides instructions for configuring the OHIM Policy Engine VM.

- "How to VNC into a VM"
- "Configuring the VM Network Settings"
- "Configuring OHIM Policy Engine VM"

1.4.1 How to VNC into a VM

To VNC into a VM:

Note: To enable the VNC Port link in the VM Manager follow the instructions in "Installing OVM Console" at `http://oss.oracle.com/oraclevm/manager/RPMS/README-console`.

Expand the details of the VM by clicking the **+** on **Show**. You can VNC into the box from the VM Manager by clicking on the VNC Port link under the VM details, or you can use a VNC client to log in using the address:

`<VM_SERVER_HOST_NAME>:<VM_VNC_PORT>`

1.4.2 Configuring the VM Network Settings

To configure the VM to use static IP:

Note: The VM is configured by default to use DHCP to assign an IP address.

If you are using DHCP addressing you can skip the following steps.

1. To configure the VM to use static IP, log in as the root user (default password: `ovsroot`) and set the IP using the following steps:

   a. Select **System**, **Administration**, and then **Network**.

   b. Choose **Devices**, click **Edit**, select the **Statically Set IP Address** radio button, and then enter the following values:

   - Address: *`<VM_IP>`*

   - Subnet mask: *`<SUBNET_MASK>`*

   - Default Gateway address: *`<DEFAULT_GATEWAY_ADDRESS>`*

   - From the Ethernet Device panel, select the **Hardware Device** tab, and then click the **Probe** button that corresponds to "Bind to MAC address".

   This sets the correct MAC address for this machine.

   Note: Make certain that you a record the MAC address.

   ---

   c. Click **OK**.

   d. Choose **File** and then click **Save**.

   e. Click the **DNS** tab and then enter the following values:

   - Hostname: *`<VM_HOST_NAME>`*

   - Primary DNS: *`<PRIMARY_DNS>`*

   - Secondary DNS: *`<SECONDARY_DNS>`*

   - Tertiary DNS: *`<TERTIARY_DNS>`*

   - DNS search path: *`<VM_NAME_SUFFIX>`*

   f. Choose **Next** and then click **Save**.

   g. Choose the **Hosts** tab, click **New**, and then enter the following values:

- Address: *<VM_IP>*

- Hostname: *<VM_HOST_NAME>*

- Aliases: *<VM_NAME_PREFIX>* hostname

h. Click **OK**.

i. Choose **File** and then click **Save**.

j. Restart Network Services from a terminal window.

```
> service network restart
```

k. Check the output for *<VM_IP>*.

```
> ifconfig
```

l. Check the output for *<VM_HOST_NAME>*.

```
> hostname
```

m. Check the success of:

```
> ping <VM_IP>
```

n. Check the success of:

```
> ping <VM_HOST_NAME>
```

Note: (Optional) In order to preserve the static IP address when the OVM is powered off, follow below steps, but only if the line

```
vif = ['mac=AA:BB:CC:DD:AA:CC,bridge=xenbr0']
```

does not match what you have in the `vm.cfg` file (see below).

1. Power off the Virtual Machine by selecting the **Virtual Machines** tab in the VM Manager, choose the **Virtual Machine Name**, and click **Power Off**.
2. Edit the `vm.cfg` file that is found on the VM Server under `/OVS/seed_pool/`*<template_name>* by replacing the line:

   ```
   vif = ['bridge=xenbr0,type=netfront']
   ```

   with the MAC corresponding to that virtual machine:

   ```
   vif = ['mac=AA:BB:CC:DD:AA:CC,bridge=xenbr0']
   ```

   where `AA:BB:CC:DD:AA:CC` is the MAC corresponding to the created OVM noted above.

1.4.3 Configuring OHIM Policy Engine VM

To configure the OHIM Policy Engine VM:

1. Log in to the VM as `hiauser` (default password: `hiapass`).
2. Start the application server using the following commands

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin start-domain domain1`
3. Navigate to the directory: `/home/hiauser/config`.

4. Run the script `import-policyengine-svc-cfg.sh` to import the service configuration data to the opensso configuration datastore, and to update the bootstrap file which is used by opensso to retrieve configuration data to bootstrap itself.

   > **Note:** You can run `ifconfig` on your VM to determine the ip address.

   Example:

   ```
   >sh import-policyengine-svc-cfg.sh

   - The VM_IP address of your Policy Engine Virtual Machine

     Enter policy_engine_host_ip: <POLICY_ENGINE_VM_IP>

   - The VM_IP address of your Gateway Virtual Machine

     Enter gateway_host_ip: <GATEWAY_VM_IP>

   - For the commnad, "Directory Service contains existing data. Do you want to
   delete it? [y|N]"

     Provide y as the option, and hit Enter key. You will see the following
   message on the console

     Please wait while we import the service configuration...

     Upon successful completion of the service configuration import, you will see
   the message

     Service Configuration was imported.
   ```

5. Stop the application server using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin stop-domain domain1`

6. Navigate to the directory: `/home/hiauser/config`.

   > **Note:** Before proceeding to the next step, make sure that the hostname does not return a fully configured name for the Virtual Machine. Please check the following commands before proceeding:
   >
   > `> hostname` (should return just the hostname)
   >
   > `> hostname -f` (should return a fully configured hostname)
   >
   > `> hostname -d` (should return the domain)

   The following step produces a self-signed certificate for use during initial installation and testing. Use appropriate signed certificates for production use.

7. Run the script `create-and-import-selfsigned-certs.sh` to install the self-signed certificate. It does the following things.

   - Creates the keystore for the private internal key
   - Exports the certificate that will authenticate the internal key

- Imports the trusted certificates into the truststore
- Provides these certificates to `appserver` to use for authentication purposes

```
>sh create-and-import-selfsigned-certs.sh
```

1.5 Installing Self-signed Certificates on OHIG Adapter VM (if not done already)

1. Log in to the Adapter VM as `hiauser` (password: `hiapass`)
2. Stop the application server using the following commands:
   a. `> cd /home/hiauser/SUNWappserver/bin`
   b. `> asadmin stop-domain domain1`
3. Navigate to the directory `/home/hiauser/config/scripts` using the following command:

   ```
   > cd /home/hiauser/config/scripts
   ```
4. Run the script `create-and-import-selfsigned-certs.sh` to install the self-signed certificate. It does the following things:
   - Creates the keystore for the private internal key
   - Exports the certificate that will authenticate the internal key
   - Imports the trusted certificates into the truststore
   - Provides these certificates to `appserver` to use for authentication purposes

   ```
   > sh create-and-import-selfsigned-certs.sh
   ```
5. Install the certificates from the other components that will communicate with the Adapter (Gateway, OHMPI, Record Locator, Policy Engine, and so on). Copy the certificate of the component VM *`<VM_HOSTNAME.cer>`* to the `/home/hiauser/SUNWappserver/domains/domain1/config` folder. Navigate to and run the scripts `/home/hiauser/config/scripts/import-others-cert.sh`. When prompted by the scripts, enter the VM hostname (it should match with the cert file you copied to the `config` folder without ".cer" suffix).

   ```
   >bash import-others-cert.sh
   ```

1.6 Installing Self-signed Certificates on OHIG Gateway VM (if not done already)

1. Log in to the Gateway VM as `hiauser` (password: `hiapass`)
2. Stop the application server using the following commands:
   a. `> cd /home/hiauser/SUNWappserver/bin`
   b. `> asadmin stop-domain domain1`
3. Navigate to the directory `/home/hiauser/config/scripts` using the following command:

   ```
   > cd /home/hiauser/config/scripts
   ```
4. Run the script `create-and-import-selfsigned-certs.sh` to install the self-signed certificate. It does the following things:

- Creates the keystore for the private internal key
- Exports the certificate that will authenticate the internal key
- Imports the trusted certificates into the truststore
- Provides these certificates to `appserver` to use for authentication purposes

```
> sh create-and-import-selfsigned-certs.sh
```

5. Install the Adapter VM certificate. Copy the certificate of Adapter VM *<ADAPTER_VM_HOSTNAME.cer>* to the `/home/hiauser/SUNWappserver/domains/domain1/config` folder. Navigate to and run the scripts `/home/hiauser/config/scripts/import-others-cert.sh`. When prompted by the scripts, enter the Adapter VM hostname (it should match with the cert file you copied to the config folder without ".cer" suffix).

   ```
   >bash import-others-cert.sh
   ```

1.7 Installing OHIG Adapter and Gateway VM Certificates on Policy Engine VM

1. Log in to the Policy Engine VM as `hiauser` (password: `hiapass`)
2. Ensure that the application server is not running. If it is running, stop it using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin stop-domain domain1`
3. Navigate to the directory `/home/hiauser/config` using the following command:

   ```
   > cd /home/hiauser/config
   ```

   > **Note:** Before proceeding to the next step, copy the certificate of the Adapter VM *<ADAPTER_VM_HOSTNAME.cer>* to the `/home/hiauser/SUNWappserver/domains/domain1/config` folder.

4. To install the Adapter VM certificate, run the script `import-others-cert.sh`:

   ```
   > sh import-others-cert.sh
   ```

   - The hostname of the Adapter VM whose certificate is being imported into the appserver's truststore

     Enter the hostname of the machine whose certificate is being imported into appserver's truststore:

     <ADAPTER_VM_HOSTNAME>

   > **Note:** Before proceeding to the next step, copy the certificate of the Gateway VM *<GATEWAY_VM_HOSTNAME.cer>* to the `/home/hiauser/SUNWappserver/domains/domain1/config` folder.

5. To install the Gateway VM certificate, run the script `import-others-cert.sh`:

   ```
   > sh import-others-cert.sh
   ```

   - The hostname of the Gateway VM whose certificate is being imported into the appserver's truststore

     Enter the hostname of the machine whose certificate is being imported into the appserver's truststore:

     <GATEWAY_VM_HOSTNAME>

6. Start the application server using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin start-domain domain1`

1.8 Configuring CONNECT Software on OHIG Adapter VM for OpenSSO Policy Engine

1. Log in to the Adapter VM as `hiauser` (password: `hiapass`).
2. Get the `/home/hiauser/config/ada_gw_pe_config.zip` file from the Policy Engine VM using `hiauser` (password: `hiapass`).
3. Ensure that the application server is not running. If it is running, stop it using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin stop-domain domain1`

4. Navigate to the directory `/home/hiauser/config` using the following command:

   ```
   > cd /home/hiauser/config
   ```

5. Unzip the `ada_gw_pe_config.zip` file to the `config` folder

   ```
   > unzip <FILE_PATH>/ada_gw_pe_config.zip
   ```

   Note: `FILE_PATH` should be replaced with the absolute path to which the `ada_gw_pe_config.zip` file was downloaded.

6. Run the script `config-adapter-policyengine.sh` to configure the CONNECT Adapter which enables it to interact with openSSO-based Policy Engine.

   Note: You can run `ifconfig` on your Policy Engine VM to determine the ip address.

   ```
   > sh config-adapter-policyengine.sh
   ```

   - The `VM_IP` address of your Policy Engine Virtual Machine

     Enter `policy_engine_host_ip:` *<POLICY_ENGINE_VM_IP>*

   - The HTTP Port of the GlassFish Application Server which is installed on Policy Engine Virtual Machine

Enter `policy_engine_http_port:` *<GF_HTTP_PORT>*

7. Start the application server using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin start-domain domain1`

1.9 Configuring CONNECT Software on OHIG Gateway VM for OpenSSO Policy Engine

1. Log in to the Gateway VM as `hiauser` (password: `hiapass`).

2. Get the `/home/hiauser/config/ada_gw_pe_config.zip` file from the Policy Engine VM using `hiauser` (password: `hiapass`).

3. Ensure that the application server is not running. If it is running, stop it using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin stop-domain domain1`

4. Navigate to the directory `/home/hiauser/config` using the following command:

   ```
   > cd /home/hiauser/config
   ```

5. Unzip the `ada_gw_pe_config.zip` file to the `config` folder

   ```
   > unzip <FILE_PATH>/ada_gw_pe_config.zip
   ```

   > **Note:** `FILE_PATH` should be replaced with the absolute path to which the `ada_gw_pe_config.zip` file was downloaded.

6. Run the script `config-gateway-policyengine.sh` to configure the CONNECT Gateway which enables it to interact with openSSO-based Policy Engine.

   > **Note:** You can run `ifconfig` on your Policy Engine VM to determine the ip address.

   ```
   > sh config-gateway-policyengine.sh
   ```

   - The `VM_IP` address of your Policy Engine Virtual Machine

     Enter `policy_engine_host_ip:` *<POLICY_ENGINE_VM_IP>*

   - The HTTP Port of the GlassFish Application Server which is installed on Policy Engine Virtual Machine

     Enter `policy_engine_http_port:` *<GF_HTTP_PORT>*

7. Start the application server using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin start-domain domain1`

1.10 Consumer Preferences Document Creation Using SoapUI

This section assumes the following have already been setup, and applications/services on the OHIG Adapter and Gateway are ready to test from the SoapUI project.

- OpenSSO Instance has been installed and configured on Policy Engine VM
- GlassFish Application Server on Policy Engine VM is up and running
- OHIG Gateway and Adapter are configured to interact with Policy Engine VM for authentication/authorization services
- GlassFish Application Servers on OHIG Gateway VM, and OHIG Adapter VM are up and running
- A test machine with SoapUI application installed on it

1. If the GlassFish Application Server is not running on any of the VMs, start it by using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin start-domain domain1`

2. Launch the SoapUI application on the test machine.

3. Copy the `/home/hiauser/config/files/opensso/soapui/AdapterPEPWS-soapui-project.xml` file from Policy Engine VM to a directory on the test machine.

4. From the **File** menu, click the **Import Project** sub-menu. This will display the "Select soapUI Project Files dialog" window

5. Enter `<`*`FILEPATH`*`>/AdapterPEPWS-soapui-project.xml` as the filename.

   > **Note:** `FILE_PATH` represents the absolute path to which the `AdapterPEPWS-soapui-project.xml` file has been copied.

6. Click the **Open** button. The `AdapterPEPWS-soapui-project.xml` file is imported into your soapUI application.

7. Open the test by selecting **AdapterPEPWS** -> **AdapterPIPBindingSoap** -> **StorePtConsent** -> **StorePatientConsent1**.

   > **Note:** While testing using the default CONNECT Adapter provided Master Patient Index (`mpi.xml`), use the Patient ID: `D123401`.

   To ensure that the patient consent is not changed during SoapUI testing, make the following changes to the endpoint URL. Perform the following for this step (**StorePatientConsent1**) and step 11 (**StorePatientConsent2**).

   > **Note:** If you use a database-based repository, you do not need to change the endpoint URL for either step.

   - To update `internalConnectionInfo.xml` from the OHIG Adapter and Gateway servers, replace:

     ```
     <service>
     <name>adapterxdsbdocrepository</name>
     ```

```
<description>Adapter Document Retrieve</description>
<endpointURL>http://<hig_adapter_
IP>:8080/CONNECTAdapterDocReposSoap12/AdapterDocRepository2Soap12Service</e
ndpointURL>
</service>
```

with

```
<service>
<name>adapterxdsbdocrepository</name>
<description>Adapter Document Retrieve</description>
<endpointURL>http://<hig_adapter_
IP>:8080/CONNECTAdapter/DocumentRepository_Service</endpointURL>
</service>
```

- After performing this update, restart the OHIG Adapter and Gateway GlassFish servers.

8. In the StorePatientConsent1 window, using the edit current option, set the endpoint URL for the request by using the correct IP address of OHIG Adapter VM.

9. Run the test by clicking the **green arrow** near the top left corner of the StorePatientConsent1 window.

10. Run the test **AdapterPEPWS** -> **AdapterPIPBindingSoap** -> **RetrievePtConsentByPtId** -> **RetrievePatientConsent** to verify that the document was stored successfully.

11. Update the patient preference by modifying the **StorePatientConsent2** (**AdapterPEPWS** -> **AdapterPIPBindingSoap** -> **StorePtConsent** -> **StorePatientConsent2**) SOAP request where you use "false" for the "optIn" element, and include the policyOID element, which can be found in the response of the **RetrievePatientConsent** request.

    The modified request looks like:

    ```
    <soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
    xmlns:urn="urn:gov:hhs:fha:nhinc:common:nhinccommonadapter">
    <soapenv:Header/>
    <soapenv:Body>
    <urn:StorePtConsentRequest>
    <urn:patientPreferences>
    <urn:patientId>0000000000</urn:patientId>
    <urn:assigningAuthority>1.1</urn:assigningAuthority>
    <urn:optIn>false</urn:optIn>
    <urn:fineGrainedPolicyMetadata>
    <urn:policyOID>20.200.20.31</urn:policyOID>
    </urn:fineGrainedPolicyMetadata>
    </urn:patientPreferences>
    </urn:StorePtConsentRequest>
    </soapenv:Body>
    </soapenv:Envelope>
    ```

    Execute the modified **StorePatientConsent2** request. This will update the patient's preference.

12. Open the test **AdapterPEPWS** -> **AdapterPEPBindingSoap** -> **CheckPolicy** -> **DocumentQueryIn**. Use "false" for the "optIn" element.

Note: While testing using the default CONNECT Adapter provided Master Patient Index (`mpi.xml`), for the `resource-id` attribute, use the string `D123401` as the attribute value.

13. In the DocumentQueryIn window, using the edit current option, edit the endpoint URL for the request by using the IP address of OHIG Gateway VM.
14. Run the test by clicking the **green arrow** near the top left corner of the DocumentQueryIn window. You will observe "Deny" in the response.
15. Run the SOAP request **AdapterPEPWS** -> **AdapterPIPBindingSoap** -> **StorePtConsent** -> **StorePatientConsent2**. This time use "true" for the "optIn" element. This will again update the patient's preference.
16. Rerun the test **AdapterPEPWS** -> **AdapterPEPBindingSoap** -> **CheckPolicy** -> **DocumentQueryIn**. This time you will observe "Permit" in the response.

1.11 Validating CONNECT on OHIG Gateway and Adapter VMs

To validate the CONNECT software on the OHIG Gateway and Adapter VMs after they are configured to use openSSO Policy Engine:

1. Ensure that the GlassFish Application Server is up and running on Policy Engine, Gateway, and Adapter VMs using the following commands:

   a. `> cd /home/hiauser/SUNWappserver/bin`

   b. `> asadmin start-domain domain1`

2. Validate the configuration using the sample universal client distributed with the Gateway:

   a. Launch the application by navigating to the following URL:

      `http://<GATEWAY_VM_IP>:8080/UniversalClientGUI/`

      The authentication page is displayed asking for user account details.

   b. Enter a valid username and password (`user1/password`)

   c. Click the **Login** button.

      - If the account details are correct, the Universal Client GUI Main page has the **patient search** tab enabled, while the rest of the tabs are disabled.

      - If the provided account details are incorrect, you will be prompted to enter the correct account details again.

   d. Search for a patient with the last name: “Younger”.

   e. If the installation is correct, this returns a page with the PatientId for the patient.

   f. Click the PatientId hyperlink for additional details on the patient.

   g. The **Document** tab is now enabled and you can search for patient documents by date range. Search for date range 08/01/2000 to 08/01/2010

   h. Click on the document URL to retrieve the document.

1.12 Avoiding a Java Security Certificate Exception

To avoid a `java.security.cert.CertificateException` you need to ensure that your OHIM hostnames are not fully qualified.

To Make the Hostname Not Fully Qualified

1. Set the OHIM and OHIG hostnames to be not fully qualified.
2. Add aliases for all hosts.
3. Regenerate and re-import the certificates.
4. Restart all the servers.
5. Test that you do not have a Java security certificate exception.

A

References

This section provides links to supporting documentation and resources.

A.1 Oracle Virtual Machine

Oracle Virtual Machine (VM) Documentation Index

http://download.oracle.com/docs/cd/E15458_01/index.htm

Oracle VM Manager Release Notes

http://download.oracle.com/docs/cd/E15458_01/doc.22/e15440/toc.htm

Oracle® VM Manager Installation Guide

Release 2.2, Part Number E15439-01

http://download.oracle.com/docs/cd/E15458_01/doc.22/e15439/toc.htm

Oracle VM Manager User Guide

Release 2.2, Part Number E15441-02

http://download.oracle.com/docs/cd/E15458_01/doc.22/e15441/toc.htm

Oracle VM Server Release Notes

http://download.oracle.com/docs/cd/E15458_01/doc.22/e15443/toc.htm

Oracle® VM Server Installation Guide

Release 2.2, Part Number E15442-01

http://download.oracle.com/docs/cd/E15458_01/doc.22/e15442/toc.htm

Oracle VM Server User Guide

Release 2.2, Part Number E15444-03

http://download.oracle.com/docs/cd/E15458_01/doc.22/e15444/toc.htm

Installation of Oracle 11g Database Release 1

Oracle 11g is also available as a VM template

`http://www.oracle.com/pls/db111/homepage`

Oracle 11g VM Template

`http://www.oracle.com/technetwork/server-storage/vm/database-092479.html`

B
Acronyms

This section provides a list of commonly used acronyms.

B.1 Acronyms

ARR
Audit Record Repository

CCD
Continuity of Care Document

CDA
Clinical Document Architecture

DER
Distinguished Encoding Rules

HIE
Health Information Exchange

HIO
Health Information Organization

HL7
Health Level 7

IHE
Integrating the Healthcare Enterprise

NAV
Notification Of Document Availability

NHIE
Nationwide Health Information Exchange

NHIN
Nationwide Health Information Network

NHIO
Nationwide Health Information Organization

OHIG
Oracle Health Sciences Information Gateway

OHIM
Oracle Health Sciences Information Manager

SAML
Security Assertion Markup Language

VM
Oracle Virtual Machine

WSDL
Web-Service Definition Language

XDM
Cross-Enterprise Document Media Interchange

Glossary

This section provides definitions of commonly used words.

CONNECT

Is a software solution that supports health information exchange that implements Nationwide Health Information Network (NHIN) standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country. It enables public and private organizations to participate in the NHIN by leveraging their existing health information systems.

CONNECT Adapter

The portion of the CONNECT architecture that encapsulates the components most likely to be customized or replaced by an organization implementing CONNECT.

CONNECT Gateway

The portion of the CONNECT architecture that encapsulates the components most likely to be use as-is by an organization without modification. These components are primarily responsible for orchestrating information exchange with the NHIN.

Health Information Exchange

Health Information Exchange is an entity that enables the movement of health-related data among entities within a state, a region, or a non-jurisdictional participant group, which might include "classic" regional health information organizations at regional and state levels, Health Information Organization integrated delivery systems and health plans, or health data banks that support health information exchange.

Health Information Organization

Health Information Organization is an organization that enables the movement of health-related data among entities, evolving as a replacement term for health information exchange or HIE. Healthcare Information Technology Standards Panel Or simply HITSP, a cooperative partnership between the public and private sectors formed and supported by ONC for the purpose of harmonizing and integrating standards that will meet clinical and business needs established by AHIC use cases for sharing information among organizations and systems.

Integrating the Healthcare Enterprise

Integrating the Healthcare Enterprise is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information, promoting and coordinating the use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care. The Nationwide Health Information Network is being developed by ONC to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare.

Nationwide Health Information Network

Nationwide Health Information Network is a set of standards, services and policies that enable secure health information exchange over the Internet. The network will provide a foundation for the exchange of health information across diverse entities, within communities and across the country, helping to achieve the goals of the HITECH Act. This critical part of the national health IT agenda will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care so as to improve population health.

Nationwide Health Information Network Gateway

Within the CONNECT solution, the implementation of the core NHIN services and service interface specifications, comprising the CONNECT gateway and CONNECT adapter. The NHIN health information exchange or NHIE, a health information exchange that implements the NHIN architecture, processes, and procedures, is accredited as a participant of the NHIN.

Oracle Virtual Machine

Oracle Virtual Machine is a platform that provides a fully equipped environment for better leveraging the benefits of virtualization technology. Oracle VM enables you to deploy operating systems and application software within a supported virtualization environment.

Oracle Virtual Machine Manager

Oracle Virtual Machine Manager provides the user interface, which is a standard ADF (Application Development Framework) web application, to manage Oracle VM Servers. It manages virtual machine lifecycle, including creating virtual machines from installation media or from a virtual machine template, deleting, powering off, uploading, deployment and live migration of virtual machines. It manages resources, including ISO files, virtual machine templates, and sharable hard disks.

Oracle Virtual Machine Server

Oracle Virtual Machine Server allows a self-contained virtualization environment designed to provide a lightweight, secure, server-based platform for running virtual machines. Oracle VM Server is based upon an updated version of the underlying Xen hypervisor technology, and includes Oracle VM Agent.

Oracle Virtual Machine Template

Oracle Virtual Machine Template provides an innovative approach to deploying a fully configured software stack by offering pre-installed and pre-configured software images. Use of Oracle VM templates eliminates the installation and configuration costs, and reduces the ongoing maintenance costs helping organizations achieve faster time to market and lower cost of operations.

Security Assertion Markup Language

Security Assertion Markup Language is an XML-based standard for exchanging authentication and authorization data between security domains.

Web Services Description Language

Web Services Description Language is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.

XML Schema

XML Schema is a means for defining the structure, content, and semantics of XML documents.