Highly Available Identity Management Deployment Example - Rack-Mounted Identity Management

An Oracle White Paper
April 2004

ORACLE

Highly Available Identity Management Deployment Example - Rack-Mounted Identity Management

Introduction

This paper describes the installation and configuration of a rack-mounted identity management architecture, which provides high availability of the identity management. It does not address high availability for database servers that store directory data. This configuration involves running multiple identity management instances on different hardware nodes. The identity management components are connected to the same directory store, which uses one of the high availability configurations for the database server, such as Oracle Real Application Clusters.

Deployment Example - Rack-Mounted Identity Management

In this architecture, Oracle Application Server Metadata Repository is installed into an existing Oracle10*g* Release 1 (10.1.0.2.0) Real Application Clusters database using OracleAS Repository Creation Assistant (OracleAS RepCA). The Oracle Internet Directory (OID) and Oracle Single Sign-On (SSO) and Delegated Administration Services (DAS) are deployed on two (or more) servers in the Identity Management (IM) tier.

One alternative to the Rack-Mounted Identity Management architecture is to separate out the SSO and DAS components on two (or more) servers in the SSO/DAS tier. This allows for a deployment of the SSO/DAS tier in the DMZ, while protecting the OID tier by deploying it in the intranet. Availability of SSO and DAS in the DMZ enables deployment of applications that use these for authentication and which gets accessed from the Intranet and the Internet. This is recommended to provide both security and availability. The OracleAS Infrastructure is then deployed in three tiers- (1) Database (2) Rack-Mounted Directory Server/OID tier and (3) SSO/DAS tier.

> **Note:**
>
> For more information about Distributed Identity Management, see the *Highly Available Distributed Identity Management* whitepaper available online on the Oracle Technology Network (OTN) Web site:
>
> http://otn.oracle.com/products/ias/hi_av/904_Distributed_AFC

Database Tier

This tier of the OracleAS Infrastructure is on a two-node hardware cluster. It is comprised of an Oracle 10g, Release 1 (10.1.0.2.0) Real Application Clusters (RAC) database and its corresponding instances on the two nodes of the cluster. OracleAS RepCA is used to install the OracleAS Metadata Repository into the existing RAC database.

Identity Management (OID and SSO/DAS) Tier

This tier of the OracleAS Infrastructure has a minimum of two servers for availability. The two machines are typically not part of a hardware cluster. Both servers are functionally equivalent and run active instances of OC4J_SECURITY providing SSO and DAS services and OID processes simultaneously. In case of failure of one node, the surviving node continues to provide service.

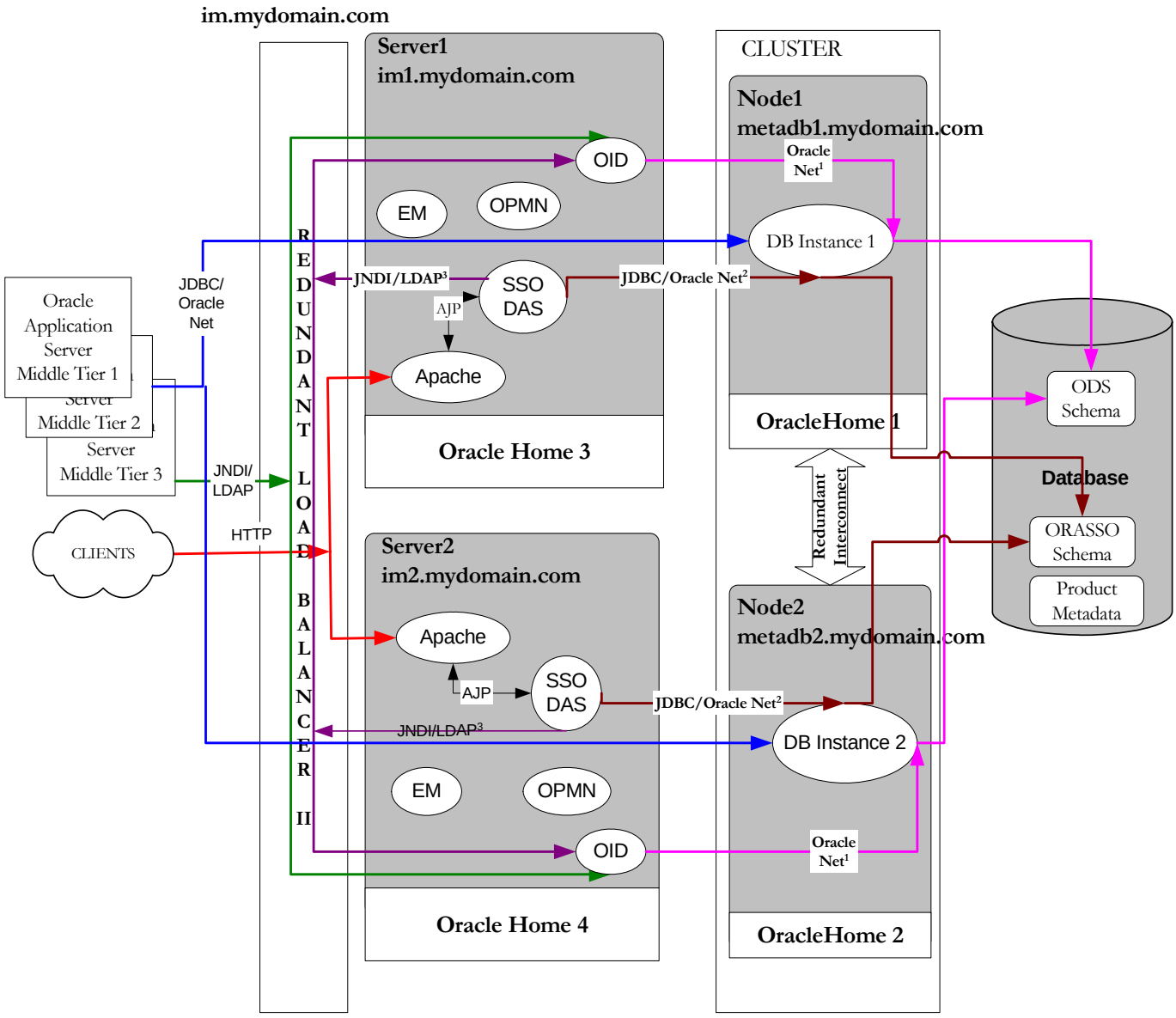
There is a load balancer providing a virtual server name/IP address in front of the IM tier. Mid-tier or end user access to the IM components is always through the virtual server name which load balances across the two servers. The database access from IM tier gets distributed to both the RAC instances using the Oracle Net load balancing mechanism.

Alternatively, you can pull out the SSO/DAS components on to separate servers. This distributed configuration is appropriate when you want to position a firewall between the SSO/DAS and the OID servers.

Related Documents

For more information, refer to these Oracle Resources:

- Oracle Application Server 10*g* High Availability Guide
- Oracle Application Server 10*g* Installing the OracleAS Metadata Repository into an Existing Database Guide
- Oracle Application Server 10*g* Installation Guide
- Oracle Application Server 10*g* Release Notes for most current information. You can find the latest version of the release note document on Oracle Technology Network: http://otn.oracle.com/documentation/ias.html



1 OID accesses the database through the DB instance on either node of the cluster. Load balancing achieved by Oracle Net.
2 SSO establishes connection pools to access the database. A connection in the pool can be to any of the DB instance in the cluster through Oracle Net load balancing.
3 SSO & DAS access OID using the load balancer address. The load balancer directs this traffic to OID on either servers.
4 SSO & DAS applications are deployed in a single OC4J instance (OC4J_SECURITY).
5 OPMN - Provides process management services (start, stop, monitor) and notification services
6 EM is Enterprise Manager related daemons (the OracleAS Control & agent)

Install Overview

1. Install OracleAS 10*g* Release 9.0.4 Metadata Repository into an existing Oracle Database 10*g*, Release 1 (10.1.0.2.0) Real Application Clusters database using OracleAS RepCA (metadb1.mydomain.com AND metadb2.mydomain.com).

Note:

The database where you want to install the OracleAS Metadata Repository must meet the OracleAS RepCA requirements.

See "Database Requirements" of the Oracle Application Server Repository Creation Assistant - Installing the Oracle Application Server Metadata Repository into an Existing Database 10g (9.0.4) for your operating system.

2. Install OracleAS 10*g*, Release 9.0.4 Identity Management components, including Oracle Internet Directory on one node (im1.mydomain.com).
3. This installs Oracle Internet Directory and configures the base schema against the remote database created from Step 1.

   Install OracleAS 10*g*, Release 9.0.4 Identity Management component, **excluding** Oracle Internet Directory on second node (im2.mydomain.com). This installs Oracle Internet Directory but does not attempt to configure the schema against the remote database.
4. Apply the post-install steps.

Installation of a Rack-Mounted Identity Management Configuration

i. Database Tier

Install OracleAS Metadata Repository into an Existing Oracle10*g* RDBMS Real Application Cluster Database.

To install the OracleAS Metadata Repository into an existing database, you run a tool called the Oracle Application Server Repository Creation Assistant (OracleAS RepCA).

Please refer to the OracleAS 10*g* Installation Guide (9.0.4) and "Installing OracleAS Metadata Repository in a Real Application Clusters Database" of the In the Oracle Application Server Repository Creation Assistant – Installing the Oracle Application Server Metadata Repository into an Existing Database 10*g* (Release 9.0.4) for your operating system to get an understanding of the pre-install requirements.

Pre-Install Tasks

1. Decide on the install node. A single install session installs and configures the components on all nodes of the cluster. Let this be the node metadb1.mydomain.com in our case.

2. Create raw devices required for the OracleAS Metadata Repository tablespaces. Please refer to "Installing OracleAS Metadata Repository in a Real Application Clusters Database" section of the Installing the Oracle Application Server Metadata Repository into an Existing Database 10*g* (Release 9.0.4) guide for the size of the raw devices.

3. Create the dbca_raw_config file to be used. This should be inline with the raw devices created above. If you do not create this file, you can still run the OracleAS RepCA to install the OracleAS Metadata Repository in a Real Application Clusters database. On the screen where OracleAS RepCA would have displayed the data read from the file, it leaves the fields blank, and you need to enter the data manually. Set up environment variables –

   DBCA_RAW_CONFIG=*/path/to/dbca_raw_config*
   export DBCA_RAW_CONFIG

4. Ensure the Real Application Clusters database and listeners are up and running before you start OracleAS RepCA.

Install

From the install node (metadb1.mydomain.com)

1. The OracleAS RepCA is a wizard that enables you to install the OracleAS Metadata Repository into an existing database.
   runRepca –OH <*Oracle home*> -RAC –LOGDIR <*log file directory*>

2. In the **Specify Database Connect** screen, enter all the node names in the Real Application Clusters database, plus the listener port numbers for each node. Use the format node:port separating the pair with a comma.
   For example: If you have 2 nodes (metadb1.mydomain.com AND metadb2.mydomain.com) in the cluster, and the listener listens on port 1521 for all nodes, then you would enter:

   metadb1.mydomain.com:1521,metadb2.mydomain.com:1521

3. In the **Register with Oracle Internet Directory**, select **Register Later.**

4. Let OracleAS RepCA continue to the end.

ii. Identity Management Tier

Install the Identity Management (IM) Components – On the First Rack-Mounted Node.

Perform this procedure to install Identity Management components without installing an OracleAS Metadata Repository.

Pre-Install Tasks

1. For this installation, both servers must have the same Oracle home path and the appropriate file system mount point must be available on both the servers.

2. Ensure that the OracleAS Metadata Repository database instances and listeners are up on both nodes of the database tier.

3. Decide on the ports to be used for the install in this tier. These ports should be free on both the servers.

4. Create staticports.ini.im with the port numbers decided above. The ports of particular interest are the **Oracle HTTP Server port, Oracle HTTP Server SSL port** (**sso_port** and **sso_ssl_port** respectively), **Oracle Internet Directory port** and **Oracle Internet Directory (SSL) port** (**oid_port** and **oid_ssl_port** respectively). The staticports.ini.im file should be available on both the servers in this tier.

5. Set up the load balancer.

    - Decide on the virtual server names and ports for the SSO/DAS and LDAP tier. You can use separate virtual server names for the HTTP and LDAP connections (such as ssodas.mydomain.com for the SSO/DAS HTTP connections and ldap.mydomain.com for the OID LDAP connections) or, alternatively, use the same virtual server name with different ports for each one of the protocols[1]. Obtain an IP address for the virtual servers that you decide to use and ensure that they are part of your DNS.

    - Configure your load balancer with the decided virtual server names and associated ports: The port mapping must be one to one for OID connections but can be different for SSO/DAS connections. This means that you must use the same port in the OID virtual server and the OID nodes but you can use different ports in the SSO/DAS virtual servers and the SSO/DAS nodes.

        - Configure a virtual server for LDAP connections and associate the two LDAP servers and respective ports to it. (im1.mydomain.com:ldap_port and im2.mydomain.com: ldap_port).

        - Configure a virtual server for HTTP connections and associate the two SSO/DAS servers and respective ports to it (im1.mydomain.com:http_port and im2.mydomain.com: http_port). The virtual server should be configured to load balance all HTTP traffic across the two servers

    - Set up Cookie Persistence for the HTTP traffic associated with the IM virtual server for SSO. Of the two expected HTTP traffic streams on this virtual server (SSO and DAS), persistence is required for DAS alone. These are the ones with URI (Uniform

[1] A host:port combination is, effectively, a different virtual server definition in most load balancers

Resource Identifier) starting with /oiddas/. If your load balancer allows a more granular setting of persistence at the URI level, set cookie persistence for the above URI alone; otherwise set cookie persistence for all HTTP traffic. The cookie should be set to expire with the expiration of the browser session. Please refer to your load balancer guide for additional information on setting up your load balancer.

Install

The IM tier requires separate installs for each server. Ensure the following for the IM tier installs so that they are equivalent in all respects:

1. Provide the same Oracle home location for both the installs.
2. Provide the same Oracle Application Server instance name for both the installs.
3. Use the same staticports.ini.im ensures that both the installs use the same ports numbers.
4. The system clocks are synchronized on all the servers.

To perform the install, on the **first** rack-mounted node (im1.mydomain.com)

1. Start the install with the following command:

   runInstaller
   oracle.iappserver.infrastructure:s_staticPorts=*/path/to/staticports.ini.im*

   Follow the install instructions for the **OracleAS Infrastructure 10*g* → Identity Management** install type.

2. In **Select Configuration Options** screen:
   - Select Oracle Internet Directory, OracleAS Single Sign-On, and Delegated Administration Services.
   - Select Oracle Directory Integration and Provisioning (if you need the services provided by this component).
   - Do not select Oracle Certificate Authority and High Availability Addressing.
3. In the **Specify Metadata Repository Login and Connect Information** screen, enter:
   - **Username**: Enter the SYS username.
   - **Password**: Enter the SYS user's password.

- **Hostname and Port**: Enter the name of the database nodes, and the listener port numbers.
  For the database node - enter all the node names in the Real Application Clusters, plus the listener port numbers for each node. Use the format node:port. Separate the pairs with a comma character.

  For example, if you have two nodes (metadb1.mydomain.com AND metadb2.mydomain.com) in the cluster, and the listener listens on port 1521 for all nodes, then you would enter:

  ```
  metadb1.mydomain.com:1521,metadb2.mydomain.com:1521
  ```

- **Service Name**: Enter the service name of the database. Service name must include the database domain name.

5. Let the install continue to the end.

Install the Identity Management (IM) Components– On Each Other Rack-Mounted Node, Except the First Node.

This procedure will install additional OracleAS Single Sign-On, Oracle Delegated Administration Services components against an existing Oracle Internet Directory.

To perform the install, on each other node (im2.mydomain.com)

1. Start the install with the following command

   ```
   runInstaller
   oracle.iappserver.infrastructure:s_staticPorts=/path/to/staticports.ini.im
   ```

2. Follow the install instructions for an **OracleAS Infrastructure 10*g* → Identity Management** install type.
3. In **Select Configuration Options** screen:
   - Select OracleAS Single Sign-On and Delegated Administration Services.
   - Do not select Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Certificate Authority and High Availability Addressing.
4. In **Register with Oracle Internet Directory** screen, enter:
   - **Hostname**: Enter the name of the computer where Oracle Internet Directory is running (im1.mydomain.com).
   - **Port**: Enter the port on which Oracle Internet Directory is listening.

5. Let the install continue to the end.

iii. Post-Install Tasks

For Oracle Internet Directory

1. On each other rack-mounted nodes, except the first node (im2.mydomain.com)
   - Copy the $ORACLE_HOME/network/admin/tnsnames.ora file from the first rack-mounted node.
   - Edit the following entries in $ORACLE_HOME/config/ias.properties to modify the following entries to the new values as shown below:

From	To
OID.LaunchSuccess = false	OID.LaunchSuccess = true
DIP.LaunchSuccess = false ***	DIP.LaunchSuccess = true
OIDhost =	OIDhost = *im2.mydomain.com*

*** Only if you selected Oracle Directory Integration and Provisioning during install.

   - Copy ORACLE_HOME/opmn/conf/opmn.xml from first rack-mounted node to the other rack-mounted nodes and update all occurrences of the hostname values to the local host name.
   - Example:

```
<ias-component id="OID" status="enabled">
  <process-type id="OID" module-id="OID">
    <stop timeout="1800"/>
    <process-set id="OID" numprocs="1">
      <dependencies>
        <database db-connect-info="database-name"/>
      </dependencies>
      <module-data>
        <category id="oidctl-parameters">
          <data id="connect" value=" database-name "/>
          <data id="startoidldapd" value="true"/>
        </category>
```

```
<category id="oidmon-parameters">
  <data id="connect" value=" database-name "/>
</category>
</module-data>
</process-set>
</process-type>
</ias-component>
```

- Execute the OID Database Password Utility to set up the wallet. To do this, enter:

  oidpasswd connect=*connect_string_for_the_database_node* create_wallet=TRUE current_password=*Oracle Application Server_admin_password*

  The *connect_string_for_the_database_node* is the same as that in the tnsnames.ora file you just copied from the first rack-mounted node.

  The *Oracle Application Server_admin_password* is the same as the one you used when installing on the first rack-mounted node.

2. On all rack-mounted nodes (im1.mydomain.com AND im2.mydomain.com)
   - Reload the opmn configuration as follows: ORACLE_HOME/opmn/bin/opmnctl reload
   - Start the directory server as follows:

     ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID

   - Validate OID using ldapbind on all rack-mounted nodes.

     ldapbind –h *OID_host* -p *OID_port*

   - Change OID configuration to use the load balancer's virtual server name (im.mydomain.com).
     - Shutdown IM components on all rack-mounted nodes.
     - Update $ORACLE_HOME/config/ias.properties.

       OIDhost=<*load balancer's virtual server name*>

       OIDport=<*load balancer's virtual server port number*>

     - Validate OID using the ldapbind command.
   - Change the configuration for SSO to use the load balancer's virtual server name for the OID on each node.

- Make sure the LD_LIBRARY_PATH environment variable contains $ORACLE_HOME/lib.
- Update Single Sign-On

  $ORACLE_HOME/jdk/bin/java –jar $ORACLE_HOME/sso/lib/ossoca.jar \ reassoc –repos *$ORACLE_HOME*

  - Update the DIRECTORY_SERVERS in $ORACLE_HOME/network/admin/ldap.ora file on each rack-mounted node to show the load balancer's virtual server name.
  - Validate OID, SSO and DAS.

For Oracle Single Sign-On

1. On all rack-mounted nodes (im1.mydomain.com AND im2.mydomain.com), change the Web server configuration as follows –
   - When a load balancer is placed between the user and the Oracle HTTP Server, the effective URL of the Single Sign-On server changes. The Oracle HTTP configuration file, $ORACLE_HOME/Apache/Apache/conf/httpd.conf, on all Single Sign-On servers must be modified to reflect this change. Edit $ORACLE_HOME/Apache/Apache/conf/httpd.conf to modify the following three directives to the new values as shown below:

From	To
KeepAlive On	KeepAlive Off
ServerName *im1.mydomain.com (or im2.mydomain.com)*	ServerName *im.mydomain.com*
Port *sso_port*	Port *sso_port_new*

     Note: The "Port" entry needs to be changed only if sso_port is being changed at this stage from the one chosen in the staticports.ini.im file at the time of install.

   - Execute the following command to update the DCM schema with the changes:

     $ORACLE_HOME/dcm/bin/dcmctl updateConfig -v –d

2. Configure the Identity Management infrastructure database by running the following on any one of the servers (im1.mydomain.com OR im2.mydomain.com). This script configures the Single Sign-On server to

accept authentication requests from the externally published address of the Single Sign-On server.

$ORACLE_HOME/sso/bin/ssocfg.sh http *im.mydomain.com 7777*

3. Re-register `mod_osso` on the first rack-mounted node's Single Sign-On server (im1.mydomain.com).
    - Set the ORACLE_HOME environment variable.
    - Include $ORACLE_HOME/lib in LD_LIBRARY_PATH environment variable (SHLIB_PATH on HPUX).
    - Include $ORACLE_HOME/jdk/bin in the PATH environment variable.
    - Run the registration script. For the URLs, be sure to substitute values appropriate for your installation. In the example, the script creates a partner application called im.mydomain.com.

      $ORACLE_HOME/jdk/bin/java -jar ORACLE_HOME/sso/lib/ossoreg.jar

      -oracle_home_path $ORACLE_HOME

      -site_name *im.mydomain.com*

      -config_mod_osso TRUE

      -mod_osso_url *http://im.mydomain.com:7777*

      -u userid

      where userid is the UNIX username who will start the HTTP server in this tier. Typically, if the sso_port is less than 1024 (e.g. 80), this will be root; otherwise it will be the owner of the oracle software (e.g. oracle). If running as root, please refer to Oracle HTTP Server Administrator's Guide 10*g* (9.0.4) for additional changes required for running Oracle HTTP Server as root.
    - Restart the IM components on all rack-mounted nodes (im1.mydomain.com AND im2.mydomain.com).

      $ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=HTTP_Server

      $ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY

      $ORACLE_HOME/opmn/bin/opmnctl startproc process-type=HTTP_Server

      $ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY

4. Re-register mod_osso on each other rack-mounted nodes (im2.mydomain.com).

    - From any browser, log in to the Single Sign-On administration pages as the Single Sign-On administrator. Be sure to log in to

      http://im.mydomain.com:7777/pls/orasso

    - Use the **Administer Partner Applications** page to delete the existing entry for the partner application corresponding to that server (im2.mydomain.com).

    - From the command line on each other rack-mounted nodes (im2.mydomain.com):

        - Backup $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf file.

        - Copy the osso.conf file from the first rack-mounted node (im1.mydomain.com) to the same location on each other rack-mounted nodes (im2.mydomain.com). Make sure that you use binary mode if you FTP the file.

        - Synchronize the DCM repository with the file copy. You do this by running the following command on im2.mydomain.com:

          $ORACLE_HOME/Apache/Apache/bin/ssotransfer \

          $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf

        - Restart SSO on this server (im2.mydomain.com).

          $ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=HTTP_Server

          $ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY

          $ORACLE_HOME/opmn/bin/opmnctl startproc process-type=HTTP_Server

          $ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY

For Oracle Delegated Administration Services

1. Change the operation URL for DAS as follows:

    - Login to one of the OID nodes (im1.mydomain.com OR im2.mydomain.com) as the oracle owner.

- Start the OID admin tool –
  - Set the ORACLE_HOME environment variable.
  - Set the DISPLAY environment variable, if required.
  - Start OID admin tool:

    $ORACLE_HOME/bin/oidadmin
- Set the Server to the local host and the Port to oid_port
- Log in as cn=orcladmin.
  - Go to the entry that contains the **orcldasurlbase** attribute by navigating through, **Entry Management → cn=OracleContext → cn=Products → cn=DAS → cn=OperationURLs**
  - Change the **orcldasurlbase** attribute value to the following value below and click on Apply:

    http://im.mydomain.com:7777/

  Make sure that you include the backslash after the host name and port number.

Validation

1. At this stage, the following processes should be up on the servers.
   - Web server Apache processes
   - OID processes
   - OC4J_SECURITY instance
   - OPMN processes
   - Application Server Control console daemon and Oracle Management daemon
2. Test the partner application oiddas by accessing: http://im.mydomain.com:7777/oiddas multiple times and validate that everything is working.
3. Test the Single Sign-On administration application by accessing: http://im.mydomain.com:7777/pls/orasso multiple times and validate that everything is working.

Enabling management of OID from Oracle Application Server Control in all the nodes

To get Oracle Application Server Control to show Oracle Internet Directory on the second node, you will have to replicate the configuraton of

$ORACLE_HOME/sysman/emd/targets.xml in the first node (im1.mydomain.com) to the second node (im2.mydomain.com) substituting the fields where the hostname appears with your second host name. So I your first node's $ORACLE_HOME/sysman/emd/targets.xml looks like this

<Target TYPE="oracle_ldap" NAME="**im.im1.mydomain.com_LDAP**"

DISPLAY_NAME="OID" VERSION="2.5"

ON_HOST="im1.mydomain.com">
<Property NAME="OracleHome" VALUE="/u01/app/oracle/product/im904"/>
<Property NAME="password" VALUE="34f1e8efcde589a4"
ENCRYPTED="TRUE"/>

<Property NAME="LDAPScriptsPath" VALUE="/sysman/admin/scripts"/>
<Property NAME="host" VALUE="im1.mydomain.com"/>
<Property NAME="UserName" VALUE="98b968d1ec165c4e"
ENCRYPTED="TRUE"/>

<Property NAME="LDAPBindDN"
VALUE="c45105a7897a90de6523d47146232a86d48e0e4676967ee12b5f6ad96a46fa7c5
b878fe7dc1aab8a65fc8a1cc762b0ff" ENCRYPTED="TRUE"/>

<Property NAME="LDAPBindPwd" VALUE=""/>
<Property NAME="version" VALUE="9.0.4"/>
<Property NAME="ConnectDescriptor"
VALUE="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(
HOST=metadb1.mydomain.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(
HOST=metadb2.mydomain.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_
NAME=meta.mydomain.com)))"/>

<CompositeMembership>
<MemberOf TYPE="oracle_ias" NAME**="im.im1.mydomain.com**"
ASSOCIATION=" "/>
</CompositeMembership>

</Target>

You should edit your second node's $ORACLE_HOME/sysman/emd/targets.xml to look like this:

<Target TYPE="oracle_ldap" NAME="**im.im2.mydomain.com_LDAP**"
DISPLAY_NAME="OID" VERSION="2.5" ON_HOST="**im2.mydomain.com**">
<Property NAME="OracleHome" VALUE="/u01/app/oracle/product/im904"/>

```
 <Property NAME="password" VALUE="manager1"
ENCRYPTED="FALSE"/>

<Property NAME="LDAPScriptsPath" VALUE="/sysman/admin/scripts"/>
<Property NAME="host" VALUE="im2.mydomain.com"/>
 <Property NAME="UserName" VALUE="ods" ENCRYPTED="FALSE"/>
 <Property NAME="LDAPBindDN" VALUE="cn=emd admin,cn=oracle internet
directory" ENCRYPTED="FALSE"/>
 <Property NAME="LDAPBindPwd" VALUE=""/>
 <Property NAME="version" VALUE="9.0.4"/>
 <Property NAME="ConnectDescriptor"
VALUE="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(
HOST=metadb1.mydomain.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(
HOST=metadb2.mydomain.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_
NAME=meta.mydomain.com)))"/>

<CompositeMembership>
    <MemberOf TYPE="oracle_ias" NAME="im.im2.mydomain.com"
ASSOCIATION=" "/>
 </CompositeMembership>

</Target>
```

After these changes are applies issue "emctl reload" on the second node. Oracle Application Server Control should now display the second OID and you should be able to perform control operations for it

Highly Available Identity Management Deployment Example - Rack-Mounted Identity Management
April 2004
Author: Susan Kornberg, Pradeep Bhat - HA Systems Group, Fermin Castro, Oracle Application Server Product Management

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com