

# Highly Available Identity Management Deployment Example –Cold Failover Cluster Identity Management

*An Oracle White Paper  
April 2004*

# Highly Available Distributed Identity Management

Introduction.....	3
Install Overview .....	5
Installation of a Cold Failover Cluster Identity Management Configuration .....	5
i. Database Tier.....	5
ii. Identity Management Tier.....	6
iii. Validation .....	7

## ***Introduction***

This paper describes the installation and configuration of a cold failover cluster 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 a single identity management instance on a hardware cluster configured for cold failover. The identity management components are connected to the directory store, which uses one of the high availability configurations for the database server, such as cold failover cluster.

### **Deployment Example - Cold Failover Cluster Identity Management**

In this architecture, Oracle Application Server Metadata Repository is installed into an existing Oracle10g, Release 1 (10.1.0.2.0) database using Oracle Application Server Repository Creation Assistant (OracleAS RepCA). The Oracle Internet Directory (OID) and Oracle Single Sign-On (SSO) and Delegated Administration Services (DAS) are deployed on one of the hardware cluster nodes in the Identity Management (IM) tier.

### **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) database that is configured for cold failover. OracleAS RepCA is used to install the OracleAS Metadata Repository into the existing database.

### **Identity Management (OID and SSO/DAS) Tier**

This tier of the OracleAS Infrastructure is on a two-node hardware cluster. The IM tier can be co-located on the same hardware cluster as the Database tier. IM components are configured in active-passive configuration. In case of failure of one node, the IM components are started up on the surviving node and provide service.

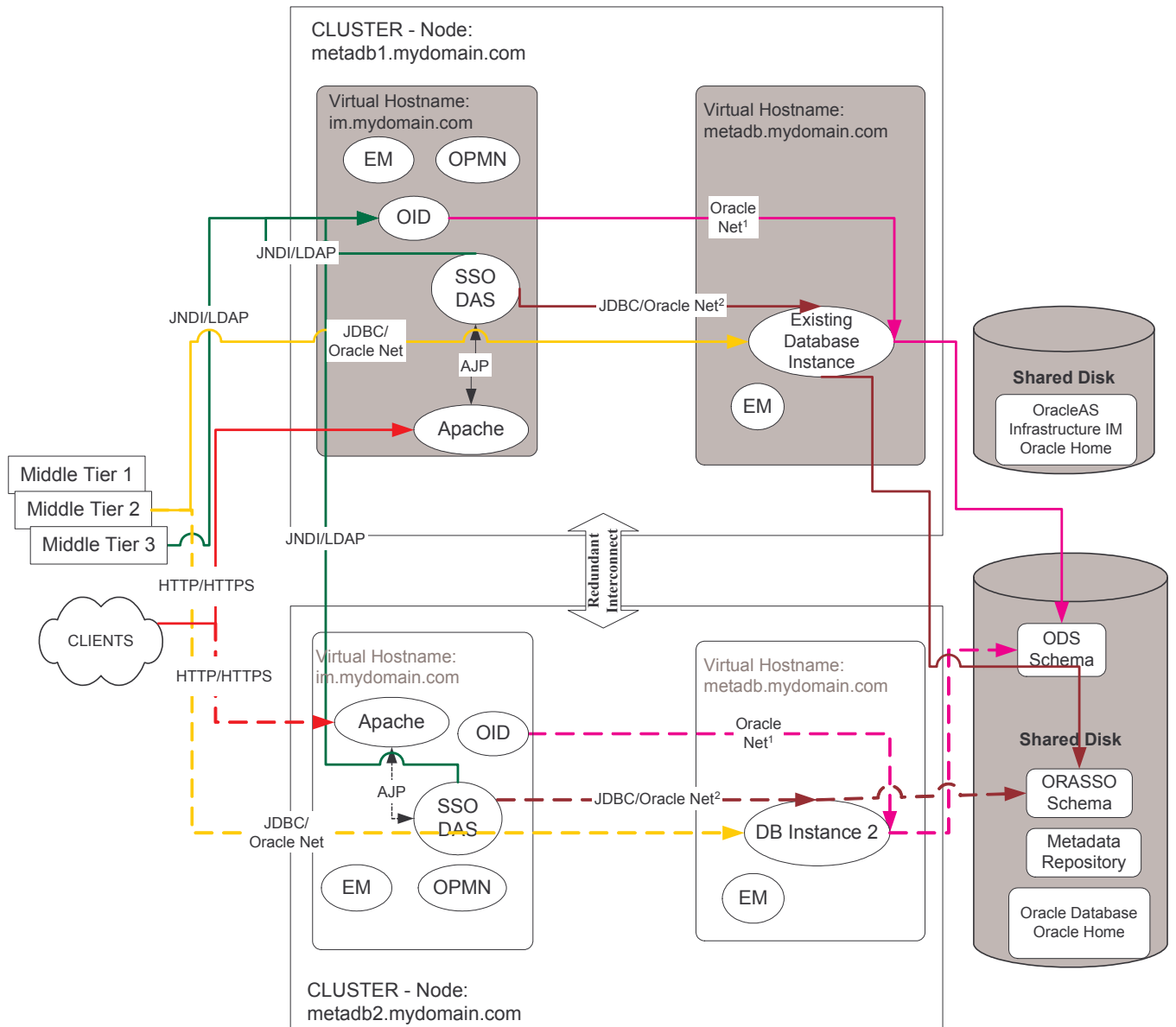
There is a virtual hostname/IP address that is associated with the Database and IM tier. Mid-tier or end user access to the Database and IM components are always through the virtual hostname which directs the request to the active node for the particular tier.

### **Related Documents**

For more information, refer to these Oracle Resources:

- Oracle Application Server 10g High Availability Guide
- Oracle Application Server 10g Installing the OracleAS Metadata Repository into an Existing Database Guide
- Oracle Application Server 10g Installation Guide

- Oracle Application Server 10g 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>



- 0 Only one node of the cluster is active. The virtual hostnames (im.mydomain and metadb.mydomain) resides on the active node. The Oracle\_Homes reside on shared disks which is mounted on the active node.
- 1 OID accesses the database through the DB instance on the active node of the cluster.
- 2 SSO establishes connection pools to access the database. A connection in the pool is to the active DB instance in the cluster .

## ***Install Overview***

1. Install OracleAS 10g Release 9.0.4 Metadata Repository in an existing Oracle Database 10g, Release 1 (10.1.0.2.0) database using OracleAS RepCA (metadb1.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 10g, Release 9.0.4 Identity Management components, including Oracle Internet Directory on one of the node (metadb1.mydomain.com) using a virtual host name of im.mydomain.com.
3. This installs Oracle Internet Directory and configures the base schema against the remote database created from Step 1.

## ***Installation of a Cold Failover Cluster Identity Management Configuration***

### **i. Database Tier**

#### **Install OracleAS Metadata Repository into an Existing Oracle10g RDBMS Database.**

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

Please refer to the OracleAS 10g Installation Guide (9.0.4) and “Installing OracleAS Metadata Repository into an Existing Database” of the In the Oracle Application Server Repository Creation Assistant – Installing the Oracle Application Server Metadata Repository into an Existing Database 10g (Release 9.0.4) for your operation 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 component on the install node. Let this be the node metadb1.mydomain.com in our case.

2. Ensure the database and listener are up and running before you start the 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 in an existing database.

```
runRepca -OH <Oracle home> -LOGDIR <log file directory>
```

2. In the **Specify Database Connect** screen, enter the node name and the listener port number for the database. Use the format node:port.  
For example:

```
metadb1.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.

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

#### Pre-Install Tasks

1. Two nodes running cluster ware, such as Sun Cluster.
2. Storage device for IM tier's Oracle home that can be accessed by both nodes. You will install OracleAS Infrastructure 10g – Identity Management components on the shared storage device.
3. Virtual hostname and it's associated IP address.
4. Ensure that the OracleAS Metadata Repository database and listener are up and running.
5. Decide on the ports to be used for the install in this tier. These ports should be free on both the nodes.
6. 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).

### Install

The IM tier requires an install on a separate Oracle home on one of the hardware cluster node.

To perform the install, on one of the hardware cluster node (metadb1.mydomain.com)

1. Start the install with the following command

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

2. In the **Specify Hardware Cluster Installation Node** screen, select **Single Node or Cold Failover Cluster Installation**.

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

3. In **Select Configuration Options** screen:

- Select Oracle Internet Directory, OracleAS Single Sign-On, Delegated Administration Services, and High Availability Addressing.
- Select Oracle Directory Integration and Provisioning (if you need the services provided by this component).
- Do not select Oracle Certificate Authority.

4. 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 node, and the listener port number.  
For the database node - enter the virtual hostname and the listener port number for each node. Use the format node:port.  
For example:  

```
metadb.mydomain.com:1521
```
- **Service Name:** Enter the service name of the database. Service name must include the database domain name.

5. In **Specify High Availability Addressing** screen, enter the virtual hostname for the Cold Failover Cluster Identity Management environment (im.mydomain.com).

6. Let the install continue to the end.

### iii. Validation

1. At this stage, the following processes should be up on the node:
  - 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.





Highly Available Distributed Identity Management with Active Failover Cluster

April 2004

Author Susan Kornberg , High Availability Systems Group

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](http://www.oracle.com)

Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation. All other product and service names mentioned may be trademarks of their respective owners.

Copyright © 2001 Oracle Corporation  
All rights reserved.