

# Highly Available Distributed Identity Management

*An Oracle White Paper  
April 2004*

# Highly Available Distributed Identity Management

Executive Overview .....	4
Introduction .....	6
Paper Overview .....	7
Distributed AFC Architecture .....	9
Architecture Diagram .....	9
Architecture Overview .....	9
Database/OID Tier .....	10
SSO/DAS Tier .....	10
Distributed CFC Architecture .....	12
Architecture Diagram .....	12
Architecture Overview .....	12
Database/OID Tier .....	13
SSO/DAS Tier .....	13
Deployment Scenarios for the two architectures .....	13
High Availability Capabilities of the two Architectures .....	15
Install .....	17
AFC Database/OID Tier Install .....	17
A. Pre-Install Tasks .....	17
B. Install .....	19
C. Post-Install Tasks .....	19
D. Validation .....	20
CFC Database/OID Tier Install .....	22
A. Pre-Install Tasks .....	22
B. Install .....	23
C. Post-Install Tasks .....	24
D. Validation .....	24
SSO/DAS Tier Install for Distributed Identity Management .....	25
A. Pre-Install Tasks .....	25
B. Install .....	26
C. Post-Install Tasks .....	27
D. Validation .....	30
Run Time considerations .....	30
Load Balancer Management .....	30
Virtual Hostname Management .....	30
Backup & Recovery .....	31
Backup .....	32
Restore .....	32

Runtime file change sync up .....	33
Middle tier association.....	33
Summary .....	34
Acknowledgements .....	34
Appendix - Templates .....	35
Template for Database/OID tier staticports.ini.oid file.....	35
Template for SSO/DAS tier staticports.ini.sso file .....	35
Template for dbca_raw_config.....	35

# Highly Available Distributed Identity Management

## EXECUTIVE OVERVIEW

Centralized and integrated identity management has rapidly become a critical business requirement with the deployment and growth of many enterprise applications. It streamlines, among other things, administration of users (including employees, contractors, customers and partners) and their permissions to access a variety of key business data and applications. Oracle Identity Management (IM) provides a robust and reliable solution, which allows companies to manage identity effectively by improving access to such information while maintaining the security of this information at the same time. It is available with the Oracle Application Server and is installed as part of the Oracle Application Server Infrastructure. With Oracle Application Server 10g, Identity Management can be deployed in a variety of high availability configurations such as Cold Failover Cluster (CFC), Active Failover Cluster (AFC) and IM only highly available configurations.

### Cold Failover Cluster

In CFC, the OracleAS infrastructure is deployed on a hardware cluster and any one node of the cluster provides the infrastructure service at any given time. The software is installed on a shared disk and uses a virtual hostname. The virtual hostname is bound to any one node of the cluster at a time but can float over to any other node. A node of the cluster that has the shared disk mounted and virtual hostname has the infrastructure processes running. The cluster manager software automatically manages failover of the service across the nodes of the cluster. CFC is an Active-Passive solution and provides local high availability with a single out-of-the-box install.

### Active Failover Cluster

AFC refers to the deployment of identity management (and the metadata repository) on hardware clusters where each node of the cluster runs the database instances as well as the identity management processes and all of them access a shared Real Application Clusters (RAC) database as their repository. In the default configuration, all of the above components are installed on nodes of the same cluster. AFC is an Active-Active solution with all nodes of the cluster in service and provides local high availability with a single out-of-the-box install.

**Rack-Mounted Identity Management High Availability**

A Rack-Mounted Identity Management configuration refers to the deployment of only the identity management service in an active-active configuration, with the metadata repository created using repCA (Repository Creation Assistant). This configuration involves running multiple identity management instances on different hardware nodes (which do not need to be part of a hardware cluster). The identity management components reference the same repository created by repCA, which uses one of the high availability configurations for the database server, such as Real Application Clusters.

**Cold Failover Cluster Identity Management High Availability**

Cold Failover Cluster Identity Management configuration refers to the deployment of only the identity management service in an active-passive configuration, with the metadata repository created using repCA (Repository Creation Assistant). This configuration involves running a single identity management instance on a hardware cluster configured for cold failover. The identity management components reference the same repository created by repCA, which uses one of the high availability configurations for the database server, such as cold failover cluster.

**Distributed Identity Management for High Availability**

CFC, AFC, and IM only highly available configurations can also be deployed in a more distributed architecture. They differ from the default configuration in that the Single Sign-On (SSO) & Delegated Administration Services (DAS) resides on two (or more) separate servers and the OID component resides either:

- on its own on two (or more) separate servers (in case of IM only)
- on a hardware cluster with the database, which is a RAC database (in case of AFC)
- on a cluster managed single instance database (in case of CFC).

This allows deployment of the SSO & DAS tier in the DMZ while protecting the OID tier by deploying it in the intranet. Availability of SSO & DAS in the DMZ enables deployment of applications that use these for authentication and which get accessed from the Intranet and the Internet. We expect this architecture to be one of the typical deployments for enterprise class applications. The architecture provides a local high availability solution, which is secure, scalable with application growth while allowing a great deal of flexibility in deployment.

## INTRODUCTION

Oracle Application Server Infrastructure provides a centralized security and management platform for deploying applications. It includes the Oracle Identity Management infrastructure as well as a facility for centralized Product Metadata management and configuration management. The infrastructure was introduced in Oracle9i Application Server 9.0.2 and it continues to provide this role in Oracle Application Server 10g (9.0.4).

A highly available Oracle Application Server deployment requires a highly available Infrastructure service. In particular, uninterrupted access to Oracle Identity Management, which is installed as part of the infrastructure, is in the critical path to availability of other application services. It is important that it be highly available and scalable.

With Oracle9i Application Server 9.0.2, it was possible to deploy the infrastructure in an active-passive mode in a cold failover cluster (CFC) deployment on some platforms. Oracle Application Server 10g (9.0.4) release supports CFC out-of-the-box on all supported platforms. In CFC, any one of the cluster (at a time) runs the database instances as well as the identity management processes. The database and the software reside on a shared disk. The services are accessed using a virtual hostname that is bound to the node currently running the identity management processes.

Oracle Application Server 10g (9.0.4) release additionally supports infrastructure deployment in an active-active mode on clusters. This is the Active Failover Cluster (AFC) deployment. Each node of the cluster runs the database instances as well as the identity management processes and all of them access a shared Real Application Clusters database as their repository. A load balancer front-ends the cluster. In the default configuration, all of the infrastructure components are installed on the same cluster.

Oracle Application Server 10g (9.0.4) release also supports other IM only highly available solutions. An active-passive solution supported is the install of the Identity Management Service alone in a cold failover cluster deployment. An active-active solution supported is the Rack Mounted install of the Identity Management Service. In both the above cases, the metadata repository is created using repCA (Repository Creation Assistant). The detailed install and configuration steps of these are described in other Oracle white papers and are not specifically listed here since there are not any changes to these procedures. For the distributed IM only HA configurations, just OID should be installed on one tier, and the same steps described in section (f) (as listed in the Paper Overview section) for the SSO & DAS tier should be followed.

Both CFC & AFC solutions provide the local high availability (in varying degrees) for the infrastructure. A single out-of-the-box install deploys the following components to all nodes of the cluster –

- Oracle Internet Directory (OID)
- Oracle Single Sign-On (SSO)
- Delegated Administration Services (DAS)
- Oracle Directory Integration and Provisioning (DIP)
- OID repository and Metadata repository database on RAC

The default out-of-the-box install requires very little post-install configuration. Please refer to the Oracle Application Server 10g Installation guide and Oracle Application Server 10g High Availability guide for more information on this configuration.

This paper describes installation and configuration of an alternative distributed architecture that may be more desirable for many enterprise class deployments. It differs from the default configuration in that the SSO & DAS components reside on two (or more) separate servers and the OID component resides on a hardware cluster with the database. Since users access most enterprise applications from both within the company intranet as well as the internet, their access needs to be authenticated by Identity Management (IM) in both cases. A distributed IM deployment where the SSO & DAS components reside in the DMZ meets this requirement elegantly. It is also important that while users are allowed to authenticate and access applications, their authentication data is well protected from unauthorized access from the Internet. Locating OID and the database repository for the identity data in the intranet ensures this. The load balancer front ending the two tiers hides the hostname of the actual servers/nodes where these services reside. This further secures the IM infrastructure. Further, if necessary, the SSO/DAS tier servers can be co-located with the middle tier servers (in separate oracle homes) in the DMZ allowing them to be scaled in tandem with mid-tier growth.

This architecture provides a highly available Identity Management solution, which enables deployment of enterprise class applications. It is secure; scales with application growth and allows a great deal of flexibility in deployment.

## **PAPER OVERVIEW**

The rest of the paper describes the implementation details of the distributed architecture for both the AFC and CFC deployments. Since many aspects of deploying the two configurations are similar, the common elements are described

together. For cases where configuration details are specific to a particular architecture (CFC or AFC), a qualifier has been provided in the sidebar.

The main sections in the rest of the paper are:

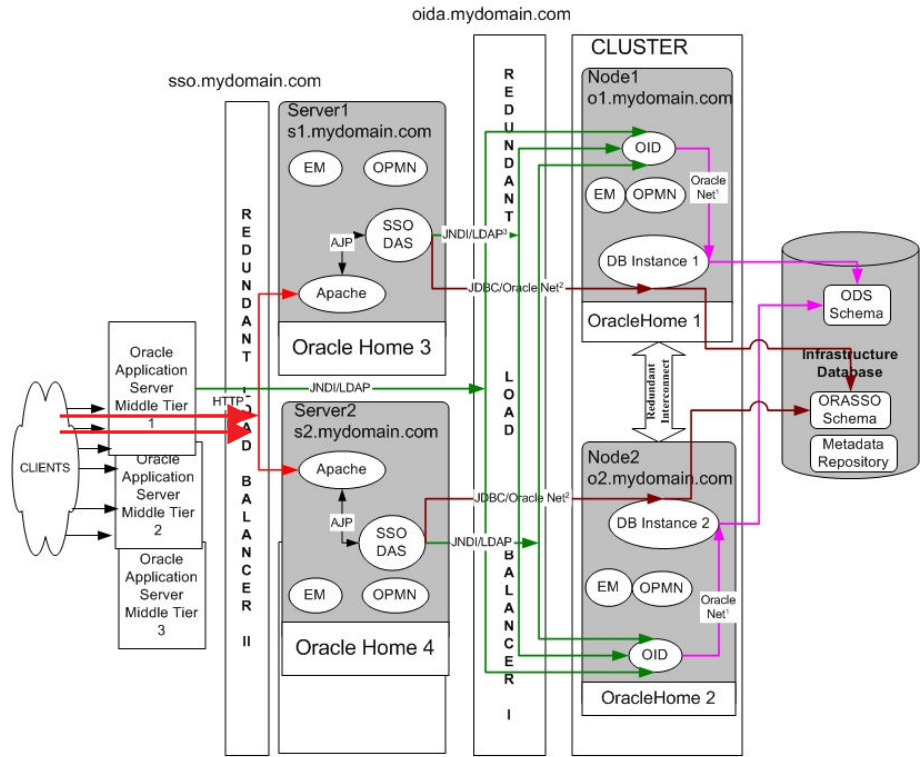
- a) Architecture description of distributed AFC configuration.
- b) Architecture description of distributed CFC configuration.
- c) Deployment scenarios for the two architectures.
- d) Install procedure for the Database/OID tier for distributed AFC.
- e) Install procedure for the Database/OID tier for distributed CFC.
- f) Install procedure for the SSO/DAS tier.

*This section applies to any active-active infrastructure deployment where SSO/DAS has been pulled out, including distributed CFC, distributed AFC, Rack mounted IM and CFC IM only installs.*

- g) Runtime Considerations for distributed CFC and distributed AFC.

# DISTRIBUTED AFC ARCHITECTURE

## Architecture Diagram



- 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 node of the cluster.
- 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 iASConsole & agent)

## Architecture Overview

In the above architecture, Oracle Application Server Infrastructure is deployed in two tiers. The Database and Oracle Internet Directory (OID) components in the Database/OID tier are deployed on a hardware cluster. Oracle Single Sign-On (SSO) and Delegated Administration Services (DAS) are deployed on two (or more) servers in the SSO/DAS tier. Together they provide the Identity management service.

## Active Failover Cluster

### Database/OID Tier

This tier of the infrastructure is on a two-node hardware cluster. It comprises of a Real Application Clusters (RAC) database and its corresponding instances on the two nodes of the cluster. The database repository resides on a SAN or dual attached shared disk. Each node has a local Oracle Home for the installed software. The Oracle Application Server component on this tier is OID. OID processes run on each node of the cluster. The two nodes are functionally equivalent and simultaneously active. 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 cluster. We refer to this as the OID load balancer virtual server. Clients of OID access LDAP services using this virtual server hostname. These incoming LDAP requests are load balanced across the respective OID processes on the cluster nodes. The database access from OID gets distributed to both the instances. This is done using the Oracle Net load balancing mechanism.

This tier is installed by choosing Active Failover Cluster, **Identity Management and Metadata repository** install for the Infrastructure and then choosing just OID (and DIP, if needed) as the component to be installed.

In our example, the two nodes of the cluster are o1.mydomain.com & o2.mydomain.com. The OID load balancer virtual server is oida.mydomain.com.

### SSO/DAS Tier

This tier has a minimum of two servers for availability. The two machines are typically not part of a hardware cluster. Both the servers are functionally equivalent and run simultaneously active instances of OC4J\_SECURITY providing SSO and DAS services. In case of failure of one server, the surviving server continues to provide service.

The database access from the SSO tier is distributed across both the database instances in the Database/OID tier using the Oracle Net load balancing mechanism. OID access by SSO and DAS uses the OID load balancer virtual server (oida.mydomain.com) and is distributed to both nodes of the Database/OID tier cluster.

The SSO/DAS tier is also front-ended by a load balancer virtual server – separate from the OID virtual server. Mid-tier or end-user access to the SSO & DAS

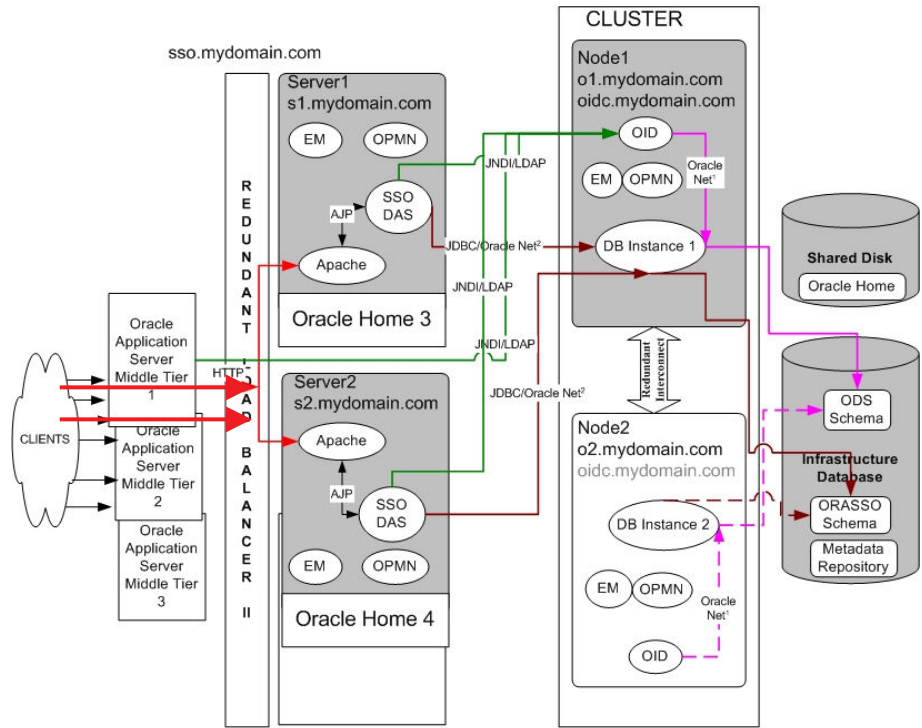
service is always through this SSO virtual server hostname. The incoming HTTP traffic for SSO and DAS services is load balanced across the two servers.

This tier is installed by doing a single node, **Identity Management only** install for the Infrastructure and then choosing just SSO and DAS as components to be installed.

In our example, the two servers in this tier are s1.mydomain.com & s2.mydomain.com. The SSO load balancer virtual server is sso.mydomain.com.

# DISTRIBUTED CFC ARCHITECTURE

## Architecture Diagram



- 0 Only one node of the cluster is active. The virtual hostname (oidc.mydomain.com) resides on the active node with the Application Server and DB instance processes. The Oracle\_Home is on a shared disk 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 .
- 3 SSO & DAS access OID using the virtual hostname address. Their request is directed to OID on the active node.
- 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 iASConsole & agent)

## Architecture Overview

Just like distributed AFC; the Infrastructure is deployed in two tiers. The Database and Oracle Internet Directory (OID) components in the Database/OID tier are deployed on a hardware cluster. Oracle Single Sign-On (SSO) and Delegated Administration Services (DAS) are deployed on two (or more) servers in the SSO/DAS tier. Together they provide the Identity management service.

## Cold Failover Cluster

### Database/OID Tier

This tier of the infrastructure is on a hardware cluster. But only one node of the cluster provides the infrastructure service at a time. The OracleAS infrastructure software and the repository are on a shared disk that can be mounted by a node of the cluster. The database repository (and the installed software) resides on a SAN or dual attached shared disk or a Network attached storage (NAS). This database is not a RAC database. The Oracle Application Server component on this tier is OID. OID processes run on the currently active node of the cluster.

A virtual hostname (and IP) is associated with the currently active node. This virtual hostname can, if required, failover to any node of the cluster and the cluster manager software typically manages any such failover. We refer to this virtual hostname as the OID virtual hostname. Clients of OID access LDAP services using this virtual hostname.

This tier is installed by choosing Cold Failover Cluster, **Identity Management and Metadata repository** install for the Infrastructure and then choosing just OID (and DIP, if needed) as the component to be installed.

In our example, the two nodes of the cluster are o1.mydomain.com & o2.mydomain.com. The OID virtual hostname is oidc.mydomain.com.

### SSO/DAS Tier

The SSO/DAS tier in this architecture is very similar as the one described for the distributed AFC architecture in the previous section. The only difference is that the OID access by SSO and DAS uses the virtual hostname (oidc.mydomain.com) and is directed to the node currently bounded to the virtual hostname of the Database/OID tier cluster.

## DEPLOYMENT SCENARIOS FOR THE TWO ARCHITECTURES

The architecture diagrams above are a generic description of the respective architecture. Some alternative deployment scenarios based on this are described here.

### Shared Load Balancer

## Active Failover Cluster only

For distributed AFC, the typical install is expected to share a load balancer hardware device between the two tiers. This reduces the overall deployment cost. This load balancer should be redundant for HA. Two virtual servers - oida.mydomain.com & sso.mydomain.com – are configured with this load balancer. We will assume such a scenario for our install.

Some deployments may also choose to have individual redundant load balancer device for the two tiers.

**Active Failover Cluster only**

**Firewall considerations for distributed AFC**

For distributed AFC, the typical install will have the servers and the load balancer in SSO/DAS tier in the DMZ (De-militarized zone) and the Database/OID tier in the intranet. In such a case, if the two tiers share a single load balancer hardware device, a firewall will separate the hardware cluster in the Database/OID tier and the load balancer in the DMZ. We will assume such a scenario for our install.

Alternatively, If each tier has its own load balancer device, the most likely deployment will have the Database/OID tier and its load balancer in the Intranet with no firewall separating the two and the SSO/DAS tier and its load balancer in the DMZ.

Some deployments may have no firewalls separating any of the components.

**Cold Failover Cluster only**

**Firewall considerations for distributed CFC**

For distributed CFC, the typical install will have the servers and the load balancer in SSO/DAS tier in the DMZ (De-militarized zone) and the Database/OID tier in the intranet. We will assume such a scenario for our install.

Some deployments may have no firewalls separating any of the components.

**Cold Failover Cluster and Active Failover Cluster**

**SSL deployment**

In the above architecture, SSL (secure sockets layer) may be used for one or more of the following –

- LDAP traffic between OID and SSO
- HTTP traffic between the mid-tier & SSO;
- HTTP traffic between the client browser and all the way to SSO.
- HTTP traffic between the client browser and SSO tier load balancer with SSO accelerators/proxies.

This provides a higher level of security. A switch to SSL is a post-install task in case of this install as well as any generic install. Please refer to the Oracle Application Server Single Sign-On Administrator's Guide 10g (9.0.4) for further information on post install migration to SSL.

For this install, we are not considering SSL configuration.

**Cold Failover Cluster and Active Failover Cluster**

**DIP deployment**

A deployment may or may not install Oracle Directory Integration and Provisioning (DIP) depending on the requirement to integrate applications and third-party LDAP directories with the Oracle Internet Directory. If DIP is installed, it will be part of the Database/OID tier. Note that DIP can be configured post-install even if it is not chosen during the Database/OID tier install session. In this example, we will choose DIP.

**Cold Failover Cluster and Active Failover Cluster**

***Using OID Replication and SSO Replication***

The above architecture provides local high availability. A deployment may build on top of this and use OID replication and SSO replication to replicate the IM repository. This provides protection from media failures as well as localized access in case of a geographically distributed deployment. Such a deployment is also active-active in nature. Please refer to the Oracle Internet Directory Administrator's Guide 10g (9.0.4) & Oracle Application Server Single Sign-On Administrator's Guide 10g (9.0.4) to implement this.

**Cold Failover Cluster and Active Failover Cluster**

***Co-existence with Mid-Tier***

The SSO tier may share the same server machines with the mid-tier installs. The two will be in separate Oracle Home on a given box. In this case, if the number of middle tiers servers is more than two, a deployment may choose to have more than two servers in the SSO/DAS tier. We assume two servers in the SSO/DAS tier for this example

**HIGH AVAILABILITY CAPABILITIES OF THE TWO ARCHITECTURES**

The above architectures provide local high availability for Identity Management and provide protection against a variety of planned and unplanned outages. Briefly, the continuous service availability is provided as follows:

- The hardware cluster in the Database/OID tier provides protection against node failures as well as planned outage for node maintenance. A node can be down but the database instance and OID processes on the surviving node continue to provide service. In case of CFC, the database instance and OID processes have to failover to the surviving node. In case of AFC, they are already up and running on the surviving node and the outage time is close to zero.
- The multiple servers in the SSO/DAS tier provide protection against planned and unplanned hardware outages to any of the servers in this tier.
- Fault tolerant redundant load balancers designed to provide continuity of service are strongly recommended. These load balancers check each other's heartbeat and automatically takeover in case of failure of the active load balancer. The load balancers can also be configured to automatically detect node & process failures and direct further traffic to only the surviving nodes. The necessary configuration step to enable this is load balancer specific and not provided by Oracle. Please refer to your vendor specific load balancer documentation on configuring this feature.
- The Real Application Clusters database technology is a proven local high availability solution and provides protection from planned and unplanned Oracle database instance outages.

**Active Failover Cluster only**

#### Active Failover Cluster only

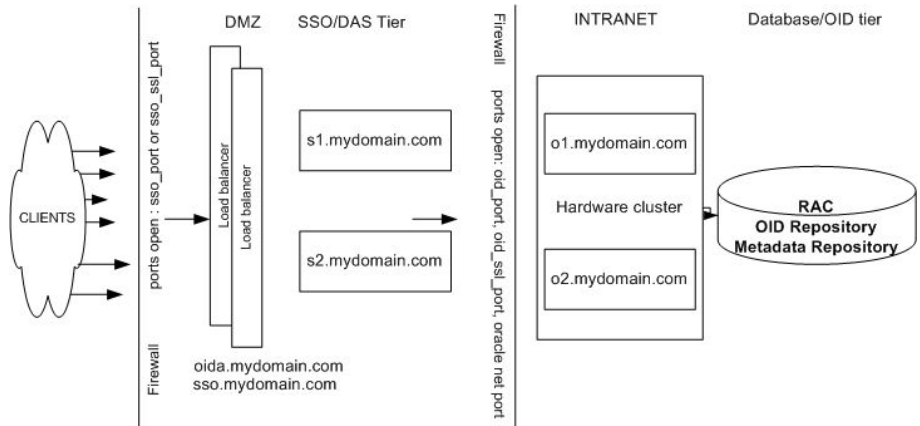
- Process redundancy is provided by OID processes running on each node of the hardware cluster and by the SSO/DAS instances running on multiple servers. RAC provides database process redundancy. This ensures that outages of any one of these instances or servers can be tolerated.
- OPMN (Oracle Process Management and Notification) provides death detection and restart capabilities on each node of the above architecture. It automatically detects death of the individual IM processes (OID, Apache, OC4J instances) on the current node and restarts them if necessary. This provides additional protection against accidental process deaths. OPMN has a built-in watchdog monitoring mechanism which guards against OPMN process death itself.
- Oracle Internet Directory built-in monitoring mechanism (oidmon) provides additional process death detection for OID processes and restarts these either locally or on the other nodes.
- Built-in HA features avoid cascading failures. There is no need to restart a component if another component it depends on fails. OID automatically reestablishes connections to surviving database instances in case a database outage occurs. SSO automatically reestablishes connections to surviving OID and the database instances, in case of outage of any of these components or node failures.

## INSTALL

In the following sections, we describe the install procedure for the above two architecture. The Database/OID tier install is different for the two architectures and has been described individually. Since the SSO/DAS tier install is common to both, this has been described in a single section.

### AFC Database/OID Tier Install

The layout assumed for the install to be illustrated in this document is –



Active Failover Cluster

oida.mydomain.com & sso.mydomain.com are two virtual servers defined in the redundant load balancers deployed in the DMZ.

#### A. Pre-Install Tasks

A.1 Please refer to the Oracle Application Server 10g Installation Guide 10g (9.0.4) for your operating system to get an understanding of the pre-install requirements. In particular the following sections of the guide are of interest,

- Requirements
- Requirements for High Availability Environments
- Setting Up the OracleAS Active Failover Cluster Environment

Make sure that these requirements are met.

A.2 Decide on the install node. A single install session deploys the software and configures the component on all nodes of the cluster. Let this be the node o1.mydomain.com in our case.

A.3 Set up the load balancer

- Decide on a load balancer virtual server hostname for the Database/OID tier load balancer. This is oida.mydomain.com in our case. Obtain an IP address for this virtual server and ensure that it is part of your DNS.

- If a firewall separates the hardware cluster and the load balancer (as in our case), add the following to the /etc/hosts file of both nodes of your cluster–

```
n.n.n.n <fully qualified virtual server name> <virtual server hostname>
```

For example,

```
123.45.67.89 oida.mydomain.com oid
```

n.n.n.n is the IP address of the install node (o1.mydomain.com)

This step is not required if there is no firewall between the cluster and the load balancer used for this tier.

- Create the OID virtual server configuration in the load balancer and associate the two nodes of the cluster (o1.mydomain.com & o2.mydomain.com) with this virtual server. The load balancer should be configured to forward all LDAP traffic to the two cluster nodes with a suitable load balancing mechanism. However, for the duration of the install, it is required that the OID virtual server should direct traffic to only the install node. Please refer to your load balancer guide for information on setting this up.
- There is no stickiness (persistence) requirement for the OID traffic.
- Many load balancers disconnect connections that have been idle for certain time. It is recommended that the load balancer should be configured to not reap idle connections associated with the OID virtual server or should be configured with a very high timeout for the same. Please refer to your load balancer guide for information on setting this up.

A.4 Create raw devices required for the infrastructure repository and spfile. If this is the first Real Application Clusters install on this cluster, create a raw device for the SRVM repository as well. Please refer Active Failover Cluster section to the Oracle Application Server 10g Installation guide for the size of the raw devices.

A.5 Create the dbca\_raw\_config file to be used. This should be inline with the raw devices created above. A template dbca\_raw\_config file is listed in the Appendix of this document.

A.6 Decide on the ports to be used for the install in this tier. These ports should be free on both nodes of the cluster.

A.7 Create the staticports.ini.oid file with the ports numbers decided above. A template for this tier is listed in the Appendix. The ports of particular interest

are the **Oracle Internet Directory port** and **Oracle Internet Directory (SSL) port** (**oid\_port** and **oid\_ssl\_port** respectively).

A.8 Set up environment variables –

```
DBCA_RAW_CONFIG=/path/to/dbca_raw_config
export DBCA_RAW_CONFIG
```

If required,

```
SRVM_SHARED_CONFIG=/path/to/srvm_raw_device
export SRVM_SHARED_CONFIG
```

A.9 Complete any other pre-install task for your platform. For e.g. on Linux this includes the install of the Oracle Cluster Manager.

## B. Install

From the install node (o1.mydomain.com),

B.1 From the install media, start the install with the following command –

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

B.2 Follow the install instructions for an AFC install viz. **Active Failover Cluster Installation** → **Oracle Infrastructure** → **Identity Management and Metadata Repository** type install.

B.3 In Step 12 (**Select Configuration Options**) of the install, select just **Oracle Internet Directory** and **Oracle Directory Integration and Provisioning**. Deselect all other options (SSO, DAS, OCA). Make sure **High Availability Addressing** is selected (it is by default).

B.4 On the **High Availability Addressing** screen, enter the virtual server for this tier viz. oida.mydomain.com.

B.5 Let the install continue to the end.

## C. Post-Install Tasks

C.1 On each node of the cluster, shutdown the Web server

- Set the ORACLE\_HOME environment variable.
- Stop the Web server on this tier -

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=HTTP_Server
```

C.2 If a /etc/hosts entry was created in step A.3 of the pre-install tasks for the AFC Database/OID tier, remove the entry from both nodes of the cluster. (Check step D.2 in the validation section before doing this)

- C.3 Re-configure the load balancer to have the virtual server oida.mydomain.com point to both nodes of the cluster.
- C.4 Turn on archiving for the database.
- C.5 Disable listener cross registration for the database instances by executing the following commands:
- Set the ORACLE\_HOME. & ORACLE\_SID environment variable.
  - Login into sqlplus as sysdba to any one of the database instances.
  - Execute the following SQL command:  
SQL> alter system set remote\_listener=" scope=spfile;
  - Restart the database instances.
- C.6 The above install creates a minimal database. For production use, this database needs to be resized for the usage envisaged. For high availability, it is important to conduct a proper capacity planning exercise and pre-create raw devices/tablespaces of appropriate size to avoid database out-of-space conditions that can compromise service availability. Please refer to the Oracle Internet Directory Admin guide 10g (9.0.4) on sizing guidelines for OID.

#### D. Validation

- D.1 At this stage, the following processes should be up on both nodes of the cluster
- Database instance processes and listener process
  - OID processes
  - OPMN processes
  - Application Server Control console daemon and Oracle Management daemon.
- D.2 To do a basic validation of the OID install on the cluster nodes, run the following commands from both nodes of the cluster as well as from a machine outside the cluster and in the DMZ. The command ORACLE\_HOME/bin/ldapbind should be available and executable on such a machine –

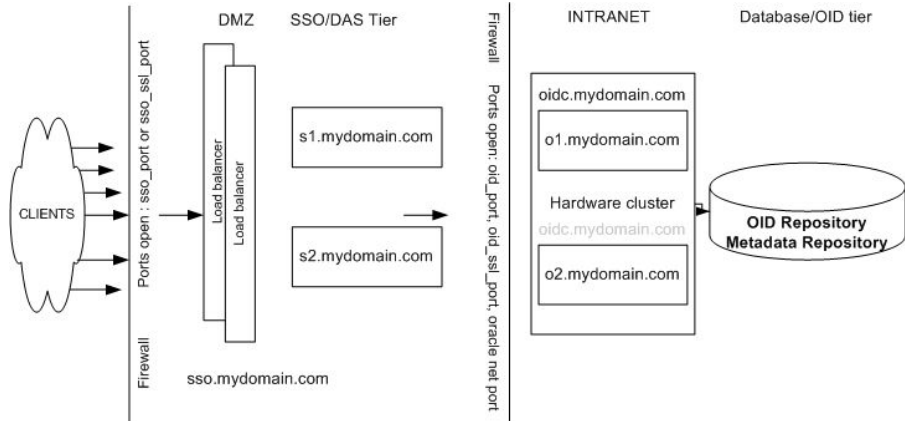
```
ldapbind -h oida.mydomain.com -p oid_port  
ldapbind -h oida.mydomain.com -p oid_ssl_port -U 1
```

If the install was done by creating load balancer virtual server related entries in /etc/hosts of the cluster nodes (in A.3 for the AFC Database/OID tier), the above validation on the cluster nodes should be done before removing these entries.



## CFC Database/OID Tier Install

The layout assumed for the install to be illustrated in this document is –



Cold Failover Cluster

oidc.mydomain.com is a virtual hostname associated with one node of the hardware cluster at a time .  
sso.mydomain.com is a virtual server defined in the redundant load balancers deployed in the DMZ.

### A. Pre-Install Tasks

A.1 Please refer to the Oracle Application Server 10g Installation Guide 10g (9.0.4) for your operating system to get an understanding of the pre-install requirements. In particular the following sections of the guide are of interest,

- Requirements
- Requirements for High Availability Environments
- Setting Up the OracleAS Cold Failover Cluster Environment

Make sure that these requirements are met.

A.2 Decide on the install node. Let this be the node o1.mydomain.com in our case.

A.3 Set up the virtual hostname

- Decide on a virtual hostname for the Database/OID tier. This is oidc.mydomain.com in our case. Obtain an IP address for this virtual server and ensure that it is part of your DNS.
- Enable the virtual hostname on the install node of the cluster e.g. for Solaris this is done by executing the following command as root.  

```
# /usr/sbin/ifconfig interface addif xxx.xxx.xxx.xxx up
```
- The Oracle Home, database and related inventory files for the install on this tier should be on a disk that can be mounted by any

node of the cluster. At any given time, only one node has it mounted. At install time, the install node should have it mounted. The exact commands to do this are operating system as well as volume manager specific. For Solaris with Veritas volume manager, the steps are –

- Have your system administrator create the necessary logical volume and file system for you. This should be large enough to hold the oracle home, the infrastructure database, oraInventory and the jre/1.1.8 directory.
- Have your System Administrator create the necessary file system mount\_point on both nodes of the cluster.
- On the install node, as root,

```
# vxdg -C import DiskgroupName
```

```
# vxvol -g DiskgroupName startall
```

```
# mount /dev/vx/dsk/DiskgroupName /VolumeName mount_point
```

A.4 Decide on the ports to be used for the install in this tier. These ports should be free on both nodes of the cluster.

A.5 Create the staticports.ini.oid file with the ports numbers decided above. A template for this tier is listed in the Appendix. The ports of particular interest are the **Oracle Internet Directory port** and **Oracle Internet Directory (SSL) port** (**oid\_port** and **oid\_ssl\_port** respectively).

A.6 Complete any other pre-install task for your platform.

## B. Install

From the install node (o1.mydomain.com),

B.1 From the install media, start the install with the following command –

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

B.2 Follow the install instructions for a CFC install, viz. **Single Node or Cold Failover Cluster Installation** → **Oracle Infrastructure** → **Identity Management and Metadata Repository** type install.

B.3 In Step 12 (**Select Configuration Options**) of the install, select just **Oracle Internet Directory** and **Oracle Directory Integration and Provisioning**. Deselect all other options (SSO, DAS, OCA). Make sure **High Availability Addressing** is selected (it is by default).

B.4 On the **High Availability Addressing** screen, enter the virtual hostname for this tier viz. oidc.mydomain.com.

B.5 Let the install continue to the end.

### C. Post-Install Tasks

C.1 On the install node of the cluster, shutdown the Web server

- Set the ORACLE\_HOME environment variable.
- Stop the Web server on this tier -

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=HTTP_Server
```

C.2 Turn on archiving for the database.

C.3 The above install creates a minimal database. For production use, this database needs to be resized for the usage envisaged. For high availability, it is important to conduct a proper capacity planning exercise and pre-create raw devices/tablespaces of appropriate size to avoid database out-of-space conditions that can compromise service availability. Please refer to the Oracle Internet Directory Admin guide 10g (9.0.4) on sizing guidelines for OID.

### D. Validation

D.1 At this stage, the following processes should be up on the install node of the cluster

- Database instance processes and listener process
- OID processes
- OPMN processes
- Application Server Control console daemon and Oracle Management daemon.

D.2 To do a basic validation of the OID install on the cluster nodes, run the following commands from both nodes of the cluster as well as from a machine outside the cluster and in the DMZ. The command ORACLE\_HOME/bin/ldapbind should be available and executable on such a machine –

```
ldapbind -h oidc.mydomain.com -p oid_port  
ldapbind -h oidc.mydomain.com -p oid_ssl_port -U 1
```

## SSO/DAS Tier Install for Distributed Identity Management

This section is common to both distributed AFC as well as distributed CFC architectures. In fact, it applies to any topology where the SSO/DAS services have been pulled out of the infrastructure and are deployed in an active-active configuration on multiple machines.

### A. Pre-Install Tasks

- A.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.
- A.2 Ensure that the database instances, database listener and the OID processes are up in the database/OID tier. For AFC, these should be up on both nodes of the Database/OID tier.
- A.3 For AFC, the load balancer virtual server `oid.mydomain.com` has been correctly set up to point to these nodes.
- A.4 Decide on the ports to be used for the install in this tier. These ports should be free on both the servers.
- A.5 Create `staticports.ini.sso` with the ports numbers decided above. A template for this tier is listed in Appendix of this document. The ports of particular interest are the **Oracle HTTP Server port** and **Oracle HTTP Server SSL port** (`sso_port` and `sso_ssl_port` respectively). The `staticports.ini.sso` file should be available on both the servers in this tier.
- A.6 The DMZ to intranet firewall should be configured to allow only expected traffic from specific DMZ IP addresses to specific intranet IP:port addresses using the correct protocols. This includes the Oracle Net traffic from SSO to the database instances as well as the LDAP traffic from SSO & DAS to OID.

The DMZ to intranet firewall should be opened up to allow incoming traffic for the OID ports (`oid_port` and `oid_ssl_port`) defined in the Database/OID tier install. It should also be opened up for the Oracle Net Listener port. This port can be determined from the `ORACLE_HOME/install/portslist.ini` file (Oracle Net Listener) on the install node of the Database/OID tier or from `ORACLE_HOME/network/admin/listener.ora` file from any node of the Database/OID tier. Typically, it is 1521. Note that we are implicitly assuming that the database instances have been deployed in the dedicated server mode, which is true by default.

- A.7 Set up load balancer
  - o Decide on the virtual server hostname for the SSO/DAS tier. This is `sso.mydomain.com` in our case. Obtain an IP address for this virtual server and ensure that it is part of your DNS.

Active Failover Cluster only

- Create the virtual server configuration in the load balancer and associate the two servers (s1.mydomain.com & s2.mydomain.com) with this virtual server. The load balancer should be configured to load balance all HTTP traffic across the two servers. Please refer to your load balancer guide for information on setting this up.
- Ensure that the SSO/DAS servers and the load balancer in the DMZ can resolve the SSO virtual server hostname (sso.mydomain.com).
- For AFC, ensure that the SSO/DAS servers and the load balancer in the DMZ can resolve the OID virtual server hostname (oida.mydomain.com).
- For CFC, ensure that the SSO/DAS servers and the load balancer in the DMZ can resolve the OID virtual hostname (oidc.mydomain.com).
- Set up Cookie Persistence for the HTTP traffic associated with the SSO virtual server. 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 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.

**Active Failover Cluster only**

**Cold Failover Cluster only**

## **B. Install**

This tier requires one install for each of the SSO/DAS instances. Ensure the following for the two installs so that they are equivalent in all respects,

- a) Provide the same oracle home location for both the installs.
- b) Provide the same Oracle Application server instance name for both the installs.
- c) Use of the same staticports.ini.sso ensures that both the installs use the same port numbers.
- d) The system clocks are synchronized on all the servers.

To perform the install, do the following on **each** server.

B.1 From the install media, start the install with the following command –

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

B.2 Follow the install instructions for an **Oracle Infrastructure → Identity Management** type install.

B.3 In Step 2 (**Select Configuration Options**) of the install, just select **Single Sign-On & Delegated Administration Services**. Deselect all the other options including OID, DIP, OCA and High Availability.

B.4 In Step 3 (**Register with Oracle Internet Directory**) of the install,

For AFC, enter the OID hostname as oida.mydomain.com (the OID virtual server name defined in the load balancer) and the port as oid\_port.

For CFC, enter the OID hostname as oidc.mydomain.com (the OID virtual hostname) and the port as oid\_port.

B.5 Let the install continue to the end.

B.6 Consult the Release Notes in the Documentation to check for known issues and workarounds. Be sure to complete these steps. Specifically,

To facilitate clean failover of SSO in case of database outages, install JDBC patches 2513420 and 3444173. These two patches are available at <http://metalink.oracle.com>. The patches should be applied on top of all the Oracle Homes where the SSO/DAS tier resides.

**Active Failover Cluster only**

**Cold Failover Cluster only**

## C. Post-Install Tasks

### 1. For Oracle Single Sign-On

C.1.1 On both the servers (s1.mydomain.com AND s2.mydomain.com), change the Web server configuration as follows -

- 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 s1.mydomain.com (or s2.mydomain.com)	ServerName <i>sso.mydomain.com</i>
Port <i>sso_port</i>	Port <i>sso_port_new</i>

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.sso file at the time of install. Let us assume

sso\_port\_new is the same as sso\_port and use sso\_port for the rest of the commands.

- Update the Distributed Configuration Management (DCM) schema

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

- C.1.2 Configure the Identity Management infrastructure database by running the following on any one of the servers (s1.mydomain.com or s2.mydomain.com),

```
$ORACLE_HOME/sso/bin/ssocfg.sh http sso.mydomain.com sso_port
```

- C.1.3 Re-Register mod\_osso on the first server in this tier (s1.mydomain.com)

- Set the ORACLE\_HOME environment variable.
- Include \$ORACLE\_HOME/lib in LD\_LIBRARY\_PATH environment variable (SHLIB\_PATH on HPUX)

- Run the following command

```
$ORACLE_HOME/jdk/bin/java -jar \  
  $ORACLE_HOME/sso/lib/ossoreg.jar \  
  -oracle_home_path $ORACLE_HOME \  
  -site_name sso.mydomain.com \  
  -config_mod_osso TRUE \  
  -mod_osso_url http://sso.mydomain.com:sso\_port \  
  -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 10g (9.0.4) for additional changes required for running Oracle HTTP Server as root.

- Restart the SSO Tier on all the servers (s1.mydomain.com & s2.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
```

- C.1.4 For the rest of the servers (s2.mydomain.com, in this case)

- From any browser, Login to [http://sso.mydomain.com:sso\\_port/pls/orasso](http://sso.mydomain.com:sso_port/pls/orasso) & delete any entry corresponding to that server (s2.mydomain.com, in this case)

- From the command line on s2.mydomain.com,
  - Backup  
\$ORACLE\_HOME/Apache/Apache/conf/osso/osso.conf to osso.conf.old.
  - Copy  
\$ORACLE\_HOME/Apache/Apache/conf/osso/osso.conf from s1.mydomain.com to the same location on s2.mydomain.com.
- Run the following command on s2.mydomain.com
 

```
$ORACLE_HOME/Apache/Apache/bin/ssotransfer \  
$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf
```
- Restart SSO on this server

```
$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
```

## 2. For Oracle Delegated Administration Services

C.2.1 Change the operation URL for DAS as follows,

- Login to the active node of the Database/OID tier 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.
- Login as cn=orcladmin
- Go to the entry containing the **orcldasurlbase** by navigating through, **Entry Management** → **cn=OracleContext** → **cn=Products** → **cn=DAS** → **cn=OperationURLs**.
- Change the **orcldasurlbase** attribute value to as below and click on Apply.

```
http://sso.mydomain.com:sso_port/
```

C.2.2 An alternative to the above is to run the following command from any node of the cluster,

```
echo "dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext  
changetype:modify  
replace:orcldasurlbase
```

```
orclbaseurlbase:http://sso.mydomain.com:sso_port/" |
$ORACLE_HOME/bin/ldapmodify -h o1.mydomain.com -p oid_port -D
cn=orcladmin -w orcladmin_password
```

Replace the sso.mydomain.com, sso\_port, o1.mydomain.com, oid\_port and orcladmin\_password with values appropriate to your install.

## D. Validation

D.1 At this stage, the following processes should be up on the servers.

- Web server Apache processes
- OC4J\_SECURITY instance
- OPMN processes
- Application Server Control console daemon and Oracle Management daemon.

D.2 Access [http://sso.mydomain.com:sso\\_port/oiddas](http://sso.mydomain.com:sso_port/oiddas) multiple times and validate that everything is working.

D.3 Access [http://sso.mydomain.com:sso\\_port/pls/orasso](http://sso.mydomain.com:sso_port/pls/orasso) multiple times and validate that everything is working.

## RUN TIME CONSIDERATIONS

Some of the run time management considerations for this environment are described in the following sections.

### Active Failover Cluster only

### Load Balancer Management

For the distributed AFC deployment, the load balancer should be configured to automatically detect failure of a node or a process in a tier and disable traffic to the failed node or service. This is true for the OID service in the Database/OID tier as well as the SSO and DAS service in the SSO/DAS tier. Besides node death detection, most load balancers provide a mechanism to detect OID failure as well as HTTP failure (for SSO/DAS) and stop traffic to the failed node. The details of doing this should be available in your vendor load balancer guide.

### Cold Failover Cluster only

### Virtual Hostname Management

For distributed CFC deployment, the load balancer should be configured to automatically detect failure of a node or a process in the SSO/DAS tier and disable traffic to the failed node or service. The details of doing this should be available in your vendor load balancer guide.

On the Database/OID tier, the hardware cluster should be configured to automatically detect node failure or process (database, OID, Apache and OC4J) failure and then failover the service to the surviving node. Cluster Manager software normally provides cluster agent packages that monitor nodes as well as services (e.g. `opmnctl` status for the infrastructure) and failovers as appropriate. The typical steps involved in doing this are (examples are for Solaris and Veritas volume manager) –

- Shutdown the entire infrastructure processes on current node. This includes OPMN, OID, Application server console and agent processes.
- Shutdown the database and listener processes on this node.
- Unmount the file system and deport the diskgroup on current node (as root).

```
# umount mount_point
```

```
# vxdg deport DiskgroupName
```

- Bring down the virtual IP on the current node

```
# /usr/sbin/ifconfig interface removeif
```

- On the new node, import and mount the file system ( as root)

```
# vxdg -C import DiskgroupName
```

```
# vxvol -g DiskgroupName startall
```

```
# mount /dev/vx/dsk/DiskgroupName /VolumeName mount_point
```

- Bring up the virtual IP on the new node

```
# /usr/sbin/ifconfig interface addif xxx.xxxx.xxx.xxx up
```

- Bring up the database and the listener process on the new node
- Startup the infrastructure process (OPMN, OID, Application Server control and EM agent) on the new node.

## Backup & Recovery

It is recommended that the Oracle Application Server backup and recovery tool be used for backing up both the database and the configuration files of the Database/OID tier as well as the SSO/DAS tier.

Configuration file backup must be done at the same time as the database backup to make sure that the infrastructure repository and the configuration files on the file system are in sync.

Please refer to the backup & recovery section of Oracle Application Server Administrator's Guide 10g (9.0.4) for more information on installing, configuring and using the tool.

Some best practices recommended are -

## Backup

### *For the Database/OID tier*

- For AFC,
  - Please refer to the Oracle Application Server 10g Release Notes (section 6.1.10) for details about setting up the backup and recovery tool for an AFC install.
  - Also refer to the Oracle Application Server 10g Administrator's Guide 10g (9.0.4) for details of the backup and recovery tool and its usage in an AFC or CFC environment.
  - Ensure archive destinations are the same on all nodes for the database instances.
  - Execute backup of the configuration files and metadata repository using the backup/recovery tool from one node.
  - Execute backup of just the configuration files from the other node.
  - Once the metadata repository and configuration files have been backed up on one AFC node, ensure that no administrative operations or changes take place until the configuration files on the additional AFC nodes have also been backed up.

Active Failover Cluster only

Cold Failover Cluster and Active Failover Cluster

### *For the SSO/DAS tier*

- Execute backup of only the configuration files using the backup/recovery tool on each server in this tier.

## Restore

### *For the Database/OID tier*

#### Active Failover Cluster only

- For AFC,
  - In case of media recovery, ensure archive logs from all cluster nodes are available in the archive log destination on the node where recovery is taking place.
  - Complete restore and recovery of the configuration files and metadata repository on one node first.
  - Restore only the configuration files (not the metadata repository) on the additional cluster nodes. Since in an Active Failover Cluster Infrastructure configuration the metadata repository is shared between all nodes, the database has already been restored and recovered. There is no need to do additional recovery from the other nodes. Just a restore of the configuration files from the same point in time is required.
  - All nodes must be restored irrespective of whether or not they require recovery.

#### Cold Failover Cluster and Active Failover Cluster

##### *For the SSO/DAS tier*

- Restore only the configuration files on all the servers in this tier.

### Runtime file change sync up

#### Active Failover Cluster only

For AFC, any change to the configuration file on one node of the Database/OID tier needs to be synced to other node/machine in that tier.

#### Cold Failover Cluster and Active Failover Cluster

For both CFC & AFC, any change to the configuration file on one machine of the SSO/DAS tier needs to be synced to other machine in that tier.

The tool to do this is **afctl**. Please refer to the Oracle Application Server 10g High Availability Guide 10g (9.0.4) for more information on installing, configuring and using the tool.

Some best practices recommended are –

- Install the tool on all nodes of the hardware cluster in the Database/OID and each server in the SSO/DAS tier.
- Always choose to update the Distributed Configuration Management (DCM) repository to keep the changes in the SSO/DAS tiers updated in the DCM repository.

### Middle tier association

#### **Active Failover Cluster only**

For AFC based infrastructure, at the time of a mid tier install, a mid-tier association with the OID repository should be done using the OID virtual server hostname. Before the mid-tier install, it is required that the load balancer configuration for the OID virtual server be changed to point to only one node of the cluster. After the mid tier install, this can be reset back to point to all nodes the Database/OID tier. On most load balancers, this can be accomplished with no down time and no loss of existing connections.

An alternative to the above is to turn on, for the duration of the mid-tier install; client IP based persistence (if available) in the load balancer for the connections associated with the OID virtual server. This also ensures that all the LDAP traffic from a given mid-tier node goes to only one node of the cluster. This too should be reset back to no persistence once the mid-tier install is done.

#### **Cold Failover Cluster only**

For CFC based infrastructure, at the time of a mid tier install, a mid-tier association with the OID repository should be done using the OID virtual hostname.

### **SUMMARY**

The architecture described above provides for identity management requirements of all enterprise class applications, which need to be accessed from the intranet and the Internet. This deployment is secure, scalable to grow with application demands and provides uninterrupted service to applications deployed with Oracle Application Server 10g.

### **ACKNOWLEDGEMENTS**

Grateful thanks to the following reviewers for their valuable comments, suggestions and corrections - Wei Hu, Shari Yamaguchi, Ashesh Parekh, David Saslav, Ganesh Kirti, Ajay Keni & Bill Loi.

## APPENDIX - TEMPLATES

### Template for Database/OID tier staticports.ini.oid file

Cold Failover Cluster & Active Failover Cluster

Oracle HTTP Server port = 7800  
Oracle HTTP Server Listen port = 7800  
Oracle HTTP Server SSL port = 4400  
Oracle HTTP Server Listen (SSL) port = 4400  
Oracle HTTP Server Diagnostic port = 7200  
Oracle Notification Server Request port = 6005  
Oracle Notification Server Local port = 6102  
Oracle Notification Server Remote port = 6202  
Log Loader port = 44002  
Java Object Cache port = 7002  
DCM Java Object Cache port = 7103  
Application Server Control RMI port = 1850  
Application Server Control port = 1810  
Oracle Management Agent port = 1832  
Oracle Internet Directory port = 3062  
Oracle Internet Directory (SSL) port = 3132

### Template for SSO/DAS tier staticports.ini.sso file

Cold Failover Cluster & Active Failover Cluster

Oracle HTTP Server port = 7801  
Oracle HTTP Server Listen port = 7801  
Oracle HTTP Server SSL port = 4401  
Oracle HTTP Server Listen (SSL) port = 4401  
Oracle HTTP Server Diagnostic port = 7201  
Oracle Notification Server Request port = 6006  
Oracle Notification Server Local port = 6103  
Oracle Notification Server Remote port = 6203  
Log Loader port = 44003  
Java Object Cache port = 7003  
DCM Java Object Cache port = 7104  
Application Server Control RMI port = 1851  
Application Server Control port = 1811  
Oracle Management Agent port = 1833

### Template for dbca\_raw\_config

Active Failover Cluster

system1=/dev/vx/rdisk/ias\_dg/infra\_system\_1024m  
spfile1=/dev/vx/rdisk/ias\_dg/infra\_raw\_spfile\_64m  
temp1=/dev/vx/rdisk/ias\_dg/infra\_raw\_temp\_128m  
undotbs1=/dev/vx/rdisk/ias\_dg/infra\_raw\_undotbs1\_256m  
undotbs2=/dev/vx/rdisk/ias\_dg/infra\_raw\_undotbs2\_256m  
drsys1=/dev/vx/rdisk/ias\_dg/infra\_raw\_drsys\_64m  
control1=/dev/vx/rdisk/ias\_dg/infra\_raw\_controlfile1\_64m  
control2=/dev/vx/rdisk/ias\_dg/infra\_raw\_controlfile2\_64m  
control3=/dev/vx/rdisk/ias\_dg/infra\_raw\_controlfile3\_64m  
redo1\_1=/dev/vx/rdisk/ias\_dg/infra\_raw\_1\_log1\_64m  
redo1\_2=/dev/vx/rdisk/ias\_dg/infra\_raw\_1\_log2\_64m  
redo1\_3=/dev/vx/rdisk/ias\_dg/infra\_raw\_1\_log3\_64m  
redo2\_1=/dev/vx/rdisk/ias\_dg/infra\_raw\_2\_log1\_64m

redo2\_2=/dev/vx/rdisk/ias\_dg/infra\_raw\_2\_log2\_64m  
redo2\_3=/dev/vx/rdisk/ias\_dg/infra\_raw\_2\_log3\_64m  
portal1=/dev/vx/rdisk/ias\_dg/infra\_raw\_portal\_128m  
portal\_doc1=/dev/vx/rdisk/ias\_dg/infra\_raw\_portaldoc\_64m  
portal\_idx1=/dev/vx/rdisk/ias\_dg/infra\_raw\_portalidx\_64m  
portal\_log1=/dev/vx/rdisk/ias\_dg/infra\_raw\_portallog\_64m  
dcm1=/dev/vx/rdisk/ias\_dg/infra\_raw\_dcm\_256m  
ocats1=/dev/vx/rdisk/ias\_dg/infra\_raw\_ocats\_64m  
disco\_ptm5\_cache1=/dev/vx/rdisk/ias\_dg/infra\_raw\_discoptm5cache\_64m  
disco\_ptm5\_meta1=/dev/vx/rdisk/ias\_dg/infra\_raw\_discoptm5meta\_64m  
dsgateway\_tab1=/dev/vx/rdisk/ias\_dg/infra\_raw\_dsgatewaytab\_64m  
wcrsys\_ts1=/dev/vx/rdisk/ias\_dg/infra\_raw\_wcrsys\_64m  
uddisys\_ts1=/dev/vx/rdisk/ias\_dg/infra\_raw\_uddisys\_64m  
olts\_attrstore1=/dev/vx/rdisk/ias\_dg/infra\_raw\_oltsattrstore\_128m  
olts\_battrstore1=/dev/vx/rdisk/ias\_dg/infra\_raw\_oltsbattrstore\_64m  
olts\_ct\_store1=/dev/vx/rdisk/ias\_dg/infra\_raw\_oltsctstore\_256m  
olts\_default1=/dev/vx/rdisk/ias\_dg/infra\_raw\_oltsdefault\_128m  
olts\_svrngstore1=/dev/vx/rdisk/ias\_dg/infra\_oltssvrngstore\_64m  
ip\_dt1=/dev/vx/rdisk/ias\_dg/infra\_raw\_ipdt\_128m  
ip\_rt1=/dev/vx/rdisk/ias\_dg/infra\_raw\_iprt\_128m  
ip\_lob1=/dev/vx/rdisk/ias\_dg/infra\_raw\_iplob\_128m  
ip\_idx1=/dev/vx/rdisk/ias\_dg/infra\_raw\_ipidx\_128m  
ias\_meta1=/dev/vx/rdisk/ias\_dg/infra\_raw\_iasmeta1\_256m



Highly Available Distributed Identity Management with Active Failover Cluster

December 2003

Author: Pradeep Bhat, High Availability Systems Group, Fermin Castro Product Management Oracle Application Server

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.