

OracleAS 10g (9.0.4) Infrastructure Highly Available Architectures

An Oracle White Paper
May 2004

OracleAS 10g (9.0.4) Infrastructure Highly Available Architectures

Introduction	3
Architecture Components.....	3
Architecture Types and Deployment Scenarios	4
Decision FlowChart.....	17
Considerations.....	18
Flow Chart.....	20
References	22

OracleAS 10g (9.0.4) Infrastructure Highly Available Architectures

INTRODUCTION

The Infrastructure provides such critical services as Identity Management, Metadata repository and Management services. With 902 Oracle Internet Application Server, Cold failover cluster was the only HA deployment available. With Oracle Application Server 10g 904, the Oracle infrastructure database can be deployed in a variety of High Availability (HA) Architectures. This paper is intended to provide System architects an overview of the various HA architectures and a method to arrive at architecture suitable to their requirements.

ARCHITECTURE COMPONENTS

The OracleAS Infrastructure is primarily made of three tiers – the database tier, Oracle Internet Directory (OID) service tier and a SSO tier comprising Single Sign-On (SSO) & Delegated Administration Service (DAS) service tier. The OID tier and the SSO tier together provide the Identity Management (IM) service. A given deployment architecture is a unique supported combination of the three tiers and provides specific level of availability, scalability and operational manageability and an associated level of installation and configuration complexity. A brief description of the three tiers is given below. Please look at the references for further information.

Tier	Description	Components
Database Tier	<p>This is an Oracle RDBMS that serves as the metadata repository. The default version of the RDBMS when installed from the Application server is 9.0.1.5. It is also possible to create a database of version 9.2.0.4 or 10g and then create the metadata repository schema in this database using the repCA.</p> <p>The same database may have the metadata repository schemas as well as schemas to hold the application data.</p> <p>The processes in this tier are the database instance processes and the database listener.</p> <p>For High Availability, Oracle recommends that this database be deployed as a Real Application Cluster (RAC) database or as a Cold Failover Cluster (CFC) database.</p>	Oracle database to store the OID repository, Application Server Components metadata repository and DCM repository
OID tier	This is a service tier that provides the Oracle Internet Directory services. Typically, this includes directory services, directory	Oracle Internet Directory

	<p>integration services to integrate OID with third-party directories, etc. The tier may be co-located with the database tier or the SSO tier or may be deployed separately. The co-location can be in terms of their being on the same machine and in many cases, sharing the same Oracle Home.</p> <p>The main processes in this tier are the OID and DIP processes.</p> <p>For High Availability, Oracle recommends that multiple instances of this tier be deployed or that the deployment be designed to failover the service to any available machine. An active-active deployment of this tier requires a hardware load balancer.</p>	<p>Directory</p> <p>Oracle Directory Integration and Provisioning</p>
SSO tier	<p>This is a service tier that provides Single Sign on and Delegation Administration services. The service is assessed using HTTP requests, a vast majority of which originate from the client browser. Typically, this tier is co-located with the OID tier or may be deployed separately. The co-location can be in terms of their being on the same machine and in many cases, sharing the same Oracle Home. Also, typically, the SSO and DAS services are deployed together.</p> <p>The main processes in this tier are the Oracle HTTP server and the OC4J instances hosting the SSO and DAS applications.</p> <p>For High Availability, Oracle recommends that multiple instances of this tier be deployed or that the deployment be designed to failover the service to any available machine. An active-active deployment of this tier requires a hardware load balancer.</p>	<p>Oracle Single Sign On</p> <p>Oracle Delegated Administrative Service.</p>

Besides the above, the OID tier and the SSO tier, have such common OracleAS components as Oracle Process Management and Notification (OPMN), Application Server Control, etc. When deployed in the same Oracle Home, the two tiers share these common processes.

ARCHITECTURE TYPES AND DEPLOYMENT SCENARIOS

The High Availability architectures described in this paper are either **Manual HA** or **Managed HA** configurations. In Manual HA architectures, the architecture is capable of failing over a service (and thus ensure its availability) to an alternate location (machine), but the failover process (detection, recovery and service relocation) itself is manual. In case of Managed HA, Oracle automatically manages the failover process and this results in faster failover and reduced outage times.

Managed HA architectures itself can be categorized as **Active-Passive** architecture or **Active-Active** architecture. In the former, only one instance of the service is active at any time but this can failover to alternate locations, if necessary. In the later, more than one instance of the service can be active at any time. Even if one of the three tiers is active-active in a given architecture, we have classified the

architecture as active-active. Active-Active architectures, by their very nature, provide added scalability as well. The Active-Passive architectures considered are -

- Basic Cold failover Cluster
- Cold failover Cluster IM against a repCA database.

The Active-Active architectures considered are -

- Distributed Cold failover Cluster
- Distributed Cold failover Cluster IM against a repCA database.
- Basic Active Failover Cluster
- Distributed Active Failover Cluster
- Basic Multi-Box
- Distributed Multi-Box (various scenarios)
- Replicated IM
- Distributed Replicated IM

The factors which result in distributed versions of the base architectures include such things as the need to deploy the three tiers in a in difference security zones, the need to access SSO/DAS services from the intranet as well as the internet, the need to deploy the three tiers separately due to machine resource constraints, the need to accommodate the varied scalability of these three tiers, etc.

Even with these architectures, other factors may influence the exact installation, configuration and operational issues. These can be issues like enabling SSL for the HTTP and/or OID traffic between components; use of SSL accelerators for the SSO/DAS traffic; use of a single load balancer device with multiple virtual servers (which is usually the case) or multiple load balancer devices in architectures with more than one load balancer; etc. The variations caused by these are considered to be marginal and have largely been ignored. Also, this paper describes just the local site high availability architectures.

This paper describes the most typical manual and managed HA architectures. Other combinations are possible and some of these may be valid and supported by Oracle but have not been considered. A high level description of the architectures is followed a flow chart to help decide on an appropriate architecture.

Architecture		
Manual HA	This architecture relies on the ability of the OracleAS installer to do a virtual hostname based IM+MR install. The failover process is completely manual. The IM+MR software resides on a NAS that can be mounted on any machine. The database and AS processes run on any machine that has the virtual hostname enabled and has the network drive mounted.	
	Database Tier	Active Passive; 9.0.1.5
	OID Tier	Active Passive

	SSO tier	Active Passive
	Hardware Requirements	NAS drive; any server that can mount the NAS drive.
	Load Balancer Required	None
	Firewall Ports opened	Not Applicable
	Oracle Homes	Oracle home with the default CFC IM+MR install
	Install Method	Install IM+MR infrastructure on a non-clustered hardware with virtual hostname (HA Addressing option enabled)
	Characteristic	Manageability: very low; Scalability: low; Availability: low; Install complexity: Low
Manual IM HA	This architecture relies on the ability of the OracleAS installer to do a virtual hostname based IM only install. The failover process is completely manual. The IM software resides on a NAS that can be mounted on any machine. The AS processes run on any machine that has the virtual hostname enabled and has the network drive mounted. The database is created using the repCA option or an MR only option. HA for database tier is managed independently. It can be CFC or RAC.	
	Database Tier	Active Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active Passive
	SSO tier	Active Passive
	Hardware Requirements	NAS drive, any server that can mount the NAS drive.
	Load Balancer Required	None
	Firewall Ports opened	Not Applicable
	Oracle Homes	Oracle home for the database software Oracle home with the CFC IM only install
	Install Method	Create database and seed it using repCA or do an MR only install. Do a CFC IM only install on a non-clustered hardware with virtual hostname (HA Addressing option enabled) against the above MR database
	Characteristic	Manageability: very low; Scalability: low; Availability: low; Install complexity: Low
Cold Failover Cluster (CFC)	This architecture is an out-of-the-box cold failover cluster solution for the infrastructure. The failover process is automated and managed by the cluster manager.	
	Database Tier	Active Passive (CFC); 9.0.1.5

(CFC)	OID Tier	Active Passive (CFC)
	SSO tier	Active Passive (CFC)
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS/SAN)
	Load Balancer Required	None
	Firewall Ports opened	Not Applicable
	Oracle Homes	Oracle home with the default CFC IM+MR install
	Install Method	Install IM+MR infra on a clustered hardware with virtual hostname (HA Addressing option enabled)
	Characteristic	Manageability: High; Scalability: Low; Availability: High; Install complexity: Low
Distributed Cold Failover Cluster (CFC)	This architecture is based on CFC but pulls out the SSO tier into the DMZ (typically). The database tier and the OID tier are co-located on a hardware cluster and deployed in CFC. The SSO tier is deployed on multiple non-clustered boxes. The failover process on the cluster is automated and managed by the cluster manager.	
	Database Tier	Active Passive (CFC); 9.0.1.5
	OID Tier	Active Passive (CFC)
	SSO tier	Active-Active
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN) Multiple non-clustered servers for SSO tier
	Load Balancer Required	Yes (for the SSO tier)
	Firewall Ports opened	Oracle Net; OID Port; OID SSL Port
	Oracle Homes	Oracle home on hardware cluster with the default CFC IM+MR install Oracle home on each server in the SSO tier with an IM install
Install Method	Install infrastructure (IM+MR) on a clustered hardware with virtual hostname (HA Addressing option enabled). OID and DIP are the only components installed. Install (on each server separately) of the SSO tier (infrastructure IM only) pointing to the above install. Components installed in this tier as SSO and DAS. Configure Load balancer for SSO tier appropriately.	

	Characteristic	Manageability: Average; Scalability: Average; Availability: High; Install complexity: Average
Active Failover Cluster (AFC)		This architecture is an out-of-the-box active failover cluster solution for the infrastructure. Multiple active instances provide continued availability in case of failure of one instance. The Database instance processes and AS processes run on both the nodes of a hardware cluster. The cluster is front-ended by a load balancer.
	Database Tier	Active-Active (RAC); 9.0.1.5
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/ SA
	Load Balancer Required	Yes (fronts the OID and SSO tier on the cluster)
	Firewall Ports opened	Not Applicable
	Oracle Homes	Oracle home on hardware cluster with the default AFC IM+MR install
	Install Method	Install AFC IM+MR infra on a clustered hardware (HA Addressing option enabled)
	Characteristic	Manageability: High; Scalability: Very High; Availability: Very High; Install complexity: High
Distributed Active Failover Cluster (AFC)		This architecture is based on AFC but pulls out the SSO tier into the DMZ (typically). The database tier and the OID tier are co-located on a hardware cluster and deployed in AFC (active-active). A load balancer front-ends this tier. The SSO tier is deployed on multiple non-clustered boxes. A load balancer front-ends this tier as well.
	Database Tier	Active-Active (RAC); 9.0.1.5
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/SAN) Multiple non-clustered servers for SSO tier
	Load Balancer Required	Yes (for the SSO tier)
	Firewall Ports opened	Oracle Net; OID Port; OID SSL Port

	Oracle Homes	Oracle home on hardware cluster with the default AFC IM+MR install Oracle home on each server in the SSO tier with an IM install
	Install Method	Install AFC IM+MR on a clustered hardware (HA Addressing option enabled). OID and DIP are the only components installed. Configure Load balancer for DB/OID tier appropriately. Install (on each server separately) of the SSO tier pointing to the above install. Components installed in this tier as SSO and DAS. Configure Load balancer for SSO tier appropriately.
	Characteristic	Manageability: Average; Scalability: Very High; Availability: Very High; Install complexity: High
Cold Failover Cluster (CFC) IM only	This architecture splits the database tier and the IM tier. The database tier is typically created using repCA or it may be an MR only install. It may be CFC or RAC (repCA only). The IM tier is installed separately against the MR created above using the CFC IM only option.	
	Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active Passive (CFC)
	SSO tier	Active Passive (CFC)
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN)
	Load Balancer Required	None
	Firewall Ports opened	Not Applicable
	Oracle Homes	Oracle home with the database install Oracle home with the default CFC IM Only install
	Install Method	Create database and seed it using repCA or do an MR only install. Do a CFC IM only install on a clustered hardware with virtual hostname (HA Addressing option enabled) against the above MR database
Characteristic	Manageability: High; Scalability: low; Availability: High; Install complexity: Average	

Distributed Cold Failover Cluster (CFC) IM only	This is similar to the CFC IM only architecture above but additionally has the SSO tier pulled out. The database tier is typically created using repCA or it may be an MR only install. It may be CFC or RAC. The OIF tier is installed separately against the MR created above using the CFC IM only option. The SSO tier is deployed on multiple non-clustered boxes. A load balancer front-ends this tier	
	Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active-Passive (CFC)
	SSO tier	Active-Active
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN) Multiple non-clustered servers for SSO tier
	Load Balancer Required	Yes (for the SSO tier)
	Firewall Ports opened	Oracle Net; OID Port; OID SSL Port
	Oracle Homes	Oracle Home on hardware cluster for the database install. Oracle home on hardware cluster with the default CFC IM only install. OID and DIP are the only components installed. Oracle home on each server in the SSO tier with an IM install. SSO and DAS are the only components installed.
	Install Method	Create database and seed it using repCA or do an MR only install. Do a CFC IM only install on a clustered hardware with virtual hostname (HA Addressing option enabled) against the above MR database. OID and DIP are the only components installed. Install (on each server separately) of the SSO tier pointing to the above install. Components installed in this tier as SSO and DAS. Configure Load balancer for SSO tier appropriately.
Characteristic	Manageability: Average; Scalability: Average; Availability: High; Install complexity: Average	

Multi Box IM HA I	<p>This architecture splits the database tier and the IM tier. The database tier is typically created using repCA or it may be an MR only install. It may be CFC or RAC but typically will be RAC. The IM tier is installed separately against the MR created above but is co-located on the same hardware cluster as the database (in a separate oracle home). One IM install is done on each node of the cluster.</p> <p>A hardware load balancer front-ends the cluster and load balances the IM traffic.</p>	
Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)	
OID Tier	Active-Active	
SSO tier	Active-Active	
Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN)	
Load Balancer Required	Yes (for the IM (OID and SSO/DAS tier))	
Firewall Ports opened	Not Applicable	
Oracle Homes	Oracle Home for the database install. May be CFC or RAC Oracle home on each node of hardware cluster with the default IM only install.	
Install Method	<p>Create database and seed it using repCA or do an MR only install.</p> <p>Do an IM only install on multiple nodes of the hardware cluster against the above MR database.</p> <p>Configure Load balancer for IM tier appropriately.</p>	
Characteristic	Manageability: Average; Scalability: Very High; Availability: Very High; Install complexity: High	
Multi Box IM HA II	<p>It is similar to Multi Box IM HA I but has the SSO tier pulled to multiple non-clustered hardware in the DMZ.</p> <p>A hardware load balancer front-ends the cluster and load balances the OID traffic. Similar a load balancer front-ends the SSO tier and load balances the HTTP traffic.</p>	
Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)	
OID Tier	Active-Active	
SSO tier	Active-Active	

	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN) Multiple non-clustered servers for SSO tier
	Load Balancer Required	Yes (for the SSO tier)
	Firewall Ports opened	Oracle Net; OID Port; OID SSL Port
	Oracle Homes	Oracle Home on hardware cluster for the database install. May be CFC or RAC Oracle home on each node of hardware cluster with the IM only install. (OID & DIP) Oracle home on multiple non-clustered hardware with the IM only install (SSO & DAS)
	Install Method	Create database and seed it using repCA or do an MR only install. Do an IM only install on multiple nodes of the hardware cluster against the above MR database. OID and DIP are the components installed. Configure Load balancer for OID tier appropriately Do an IM only install on multiple non-clustered machines against the above OID and MR database. SSO and DAS are the components installed. Configure Load balancer for SSO tier appropriately.
	Characteristic	Manageability: Average; Scalability: Very High; Availability: Very High; Install complexity: High
Multi Box IM HA III	This is a variation on the multi-box IMHA I that has the IM tier pulled out. The IM tier (OID and Web) is separate from the DB tier and is installed on multiple non-clustered hardware. A hardware load balancer front-ends the IM machines and load balances the IM traffic.	
	Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN) Multiple non-clustered servers for IM tier

	Load Balancer Required	Yes (for the IM tier)
	Firewall Ports opened	Not Applicable
	Oracle Homes	Oracle Home on hardware cluster for the database install. May be CFC or RAC Oracle home on multiple non-clustered hardware with the IM only install
	Install Method	Create database and seed it using repCA or do an MR only install. Do a IM only install on multiple non-clustered machines against the above MR database. Configure Load balancer for IM tier appropriately.
	Characteristic	Manageability: Average; Scalability: Very High; Availability: Very High; Install complexity: High
Multi Box IM HA IV	This is a variation on the multi-box IMHA II. OID is deployed on multiple non-clustered servers in DMZ and SSO is installed on multiple non-clustered servers in the DMZ. A hardware load balancer front-ends the OID tier machines and load balances the OID traffic. A hardware load balancer front-ends the SSO tier machines and load balances the HTTP traffic.	
	Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	Hardware cluster with clusterware; Shared storage (direct attached/NAS /SAN) Multiple non-clustered servers for OID tier Multiple non-clustered servers for SSO tier
	Load Balancer Required	Yes (for the IM tier)
	Firewall Ports opened	Oracle Net
	Oracle Homes	Oracle Home on hardware cluster for the database install. May be CFC or RAC Oracle home on multiple non-clustered hardware with the IM only install (OID and DIP) Oracle home on multiple non-clustered hardware with the IM only install (SSO and DAS)

	Install Method	<p>Create database and seed it using repCA or do an MR only install.</p> <p>Do a IM only install on multiple non-clustered machines against the above MR database. (OID and DIP)</p> <p>Configure Load balancer for OID tier appropriately.</p> <p>Do a IM only install on multiple non-clustered machines against the above OID and MR database. (SSO and DAS)</p> <p>Configure Load balancer for SSO tier appropriately.</p>
	Characteristic	<p>Manageability: Average; Scalability: Very High;</p> <p>Availability: Very High; Install complexity: High</p>
Multi Box IM HA V		<p>This is a variation on the multi-box IMHA II. OID is deployed on multiple non-clustered servers inside the DMZ and SSO is installed on multiple non-clustered servers in the DMZ.</p> <p>A hardware load balancer front-ends the OID tier machines and load balances the OID traffic. A hardware load balancer front-ends the SSO tier machines and load balances the HTTP traffic.</p>
	Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	<p>Hardware cluster with clusterware;</p> <p>Shared storage (direct attached/NAS /SAN)</p> <p>Multiple non-clustered servers for OID tier</p> <p>Multiple non-clustered servers for SSO tier</p>
	Load Balancer Required	Yes (for the IM tier)
	Firewall Ports opened	Oracle Net; OID Port; OID SSL Port
	Oracle Homes	<p>Oracle Home for the database install. May be CFC or RAC</p> <p>Oracle home on multiple non-clustered hardware with the IM only install (OID and DIP)</p> <p>Oracle home on multiple non-clustered hardware with the IM only install (SSO and DAS)</p>

	Install Method	<p>Create database and seed it using repCA or do an MR only install.</p> <p>Do an IM only install on multiple non-clustered machines against the above MR database. (OID and DIP)</p> <p>Configure Load balancer for OID tier appropriately.</p> <p>Do an IM only install on multiple non-clustered machines against the above OID and MR database. (SSO and DAS)</p> <p>Configure Load balancer for SSO tier appropriately.</p>
	Characteristic	<p>Manageability: Average; Scalability: Very High;</p> <p>Availability: Very High; Install complexity: High</p>
Multi Box IM HA VI	<p>This is a variation on the multi-box IMHA III. The IM tier is deployed in the DMZ</p> <p>A hardware load balancer front-ends the IM tier machines and load balances the IM traffic.</p>	
	Database Tier	Active-Passive (CFC) or Active-Active (RAC); 9.2.0.4 or 10g (or 9.0.1.5)
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	<p>Hardware cluster with clusterware;</p> <p>Shared storage (direct attached/NAS /SAN)</p> <p>Multiple non-clustered servers for IM tier</p>
	Load Balancer Required	Yes (for the IM tier)
	Firewall Ports opened	Oracle Net
	Oracle Homes	<p>Oracle Home for the database install. May be CFC or RAC</p> <p>Oracle home on multiple non-clustered hardware with the IM only install (OID and DIP)</p> <p>Oracle home on multiple non-clustered hardware with the IM only install (SSO and DAS)</p>

	Install Method	<p>Create database and seed it using repCA or do an MR only install.</p> <p>Do an IM only install on multiple non-clustered machines against the above MR database. (OID and DIP)</p> <p>Configure Load balancer for OID tier appropriately.</p> <p>Do an IM only install on multiple non-clustered machines against the above OID and MR database. (SSO and DAS)</p> <p>Configure Load balancer for SSO tier appropriately.</p>
	Characteristic	<p>Manageability: Average; Scalability: Very High;</p> <p>Availability: Very High; Install complexity: High</p>
Replicated IM	<p>This architecture provides HA for the IM related data of the Metadata repository. It provides additional benefits of protection from Media failures, rolling upgrade of the IM software, support geographically distributed instances of IM for localized access, etc.</p> <p>Two instances of the IM repository and the IM services are deployed and these are master-master replicas of each other. Replication for the IM data is provided through setting up the OID replication and SSO replication and post-install steps.</p> <p>High Availability of the metadata repository is not addressed by this architecture and has to be managed separately outside of this solution. Each instance of the replicated architecture is single instance (i.e. cannot be AFC or CFC by itself). Failover in case of failure of one of the instance is not completely automated and has to be managed manually.</p> <p>Please contact the HA or OID Product Managers for further information on implementing this architecture.</p>	
	Database Tier	Active-Active (replicated); 9.0.1.5
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	Two servers for each site.
	Load Balancer Required	No
	Firewall Ports opened	Not applicable
	Oracle Homes	Oracle Home for the default IM+MR install on each site
	Install Method	Please contact the HA or OID Product Managers for further information on implementing this architecture.
	Characteristic	<p>Manageability: low; Scalability: High;</p> <p>Availability: High; Install complexity: High</p>

Distributed and Replicated IM	<p>This is similar to the replicated IM above but has the SSO tier pulled out.</p> <p>This architecture provides HA for the IM related data of the Metadata repository. It provides additional benefits of protection from Media failures, rolling upgrade of the IM software, support geographically distributed instances of IM for localized access, etc.</p> <p>Two instances of the IM repository and the IM services are deployed and these are master-master replicas of each other. Replication for the IM data is provided through setting up the OID replication and SSO replication and post-install steps.</p> <p>High Availability of the metadata repository is not addressed by this architecture and has to be managed separately outside of this solution. Each instance of the replicated architecture is single instance (i.e. cannot be AFC or CFC by itself)</p>	
	Database Tier	Active-Active (replicated); 9.0.1.5
	OID Tier	Active-Active
	SSO tier	Active-Active
	Hardware Requirements	Two servers for each site for the database and OID tier Two servers for each site for the SSO tier
	Load Balancer Required	No
	Firewall Ports opened	Oracle Net; OID Port; OID SSL Port
	Oracle Homes	Oracle Home for the default IM+MR install on each site Oracle Home for the IM only install on each site.
	Install Method	Please contact the HA or OID Product Managers for further information on implementing this architecture.
	Characteristic	Manageability: low; Scalability: High; Availability: High; Install complexity: High

DECISION FLOWCHART

The flow chart described in this section is intended as an aid in arriving at the right kind of architecture. These flow charts are also available in dynamic format to facilitate the decision flow.

Dynamic flow chart for out-of-the-box installs:

http://www.oracle.com/technology/products/ias/hi_av/animated-flow-chartI.pps

Dynamic flow chart for repCa based installs:

http://www.oracle.com/technology/products/ias/hi_av/animated-flow-chartII.pps

The considerations section provides further information on the questions asked in the flow chart.

Considerations

Do you plan the DB tier to co-exist with OID and/or SSO or will it be separate?

Each of the three tiers in the infrastructure (DB, OID and SSO) can be deployed together in one install out-of-the-box or can be deployed separately. Also, the High Availability for each of these can be managed separately as well. The reason why database tier may be separate for the other two tiers may be -

- The customer wants to use a pre-existing database for the Meta data repository
- The customer plans to use 9.2.x or 10g as the database repository instead of the default 9015 which comes by default.

Does the DB tier already exist?

This is true if the database intended for the Meta data already exists before the install begins.

Do you plan an Active-Active or Active-Passive IM service?

The IM service may be planned to be Active-Active or Active-Passive. At a high level, Active Passive provides adequate level of availability but very limited scalability. So if the demands on the infrastructure deployment are expected to grow, an Active-active solution may be the better option. Active-Active solutions also provide a higher level of availability and almost no downtime even in case of failures as compared to active-passive solutions. They are also higher cost.

Do you have load balancers?

A hardware load balancer is mandatory for any active-active solution. In case of infrastructure, the hardware load balancer is used to manage the OID (ldap) traffic and the SSO/DAS (http/https) traffic.

Will you use a hardware cluster for high availability?

Most of the HA architectures assume that the database tier is managed in a CFC or RAC deployment. A hardware cluster is required for this. However, in case a hardware cluster is not available, alternate solutions are possible. Chief among these is manual ha and replicated IM. Another option is to use local dataguard, but this has not been included in this discussion since the solution is not certified by Oracle.

External Internet access needed?

If an application is accessed from both the Internet and the intranet, the single sign-on facility needs to be accessible from the external network. Typically, this is accomplished by deploying SSO in the DMZ and by use of firewalls and restricted port access to control access to the internal network.

Is AFC possible?

In some case Active Failover Cluster solution may not be possible. The reasons for this include

- AFC is not supported on Windows platform for 9.0.4.
- On Solaris, it is possible for both 32-bit and 64-bit platforms. However, for 64-bit Solaris platform, if you already have a 64 bit RAC installed on the cluster or plan to have one soon, AFC may not be a good option. AFC is 32-bit and comes with a 32-bit RAC. On Solaris, this cannot co-exist with a 64-bit RAC.
- AFC in 904 need RAW devices for the Meta data repository. If you storage is a NAS (Network Attached Storage) environment, this is not supported. The storage has to be direct attached storage or on a SAN (Storage Area Network).

Do you plan a DR site?

If a DR site is being planned, then the only supported local HA solution in 904 is a Cold failover cluster solution. So in case a DR site is being planned, the current local HA options are limited to this. In the future, DR solution will be available for a larger set of architectures.

Will IM be co-located with the DB on the hardware cluster?

If this is an application that is designed primarily for intranet access and the Infrastructure deployment is specific to a particular application, it may be advantageous from a manageability standpoint to deploy the IM service along with the database on the same hardware cluster. This is assuming that the hardware cluster has the requisite specs and the capacity to handle the load.

Will OID be in the DMZ?

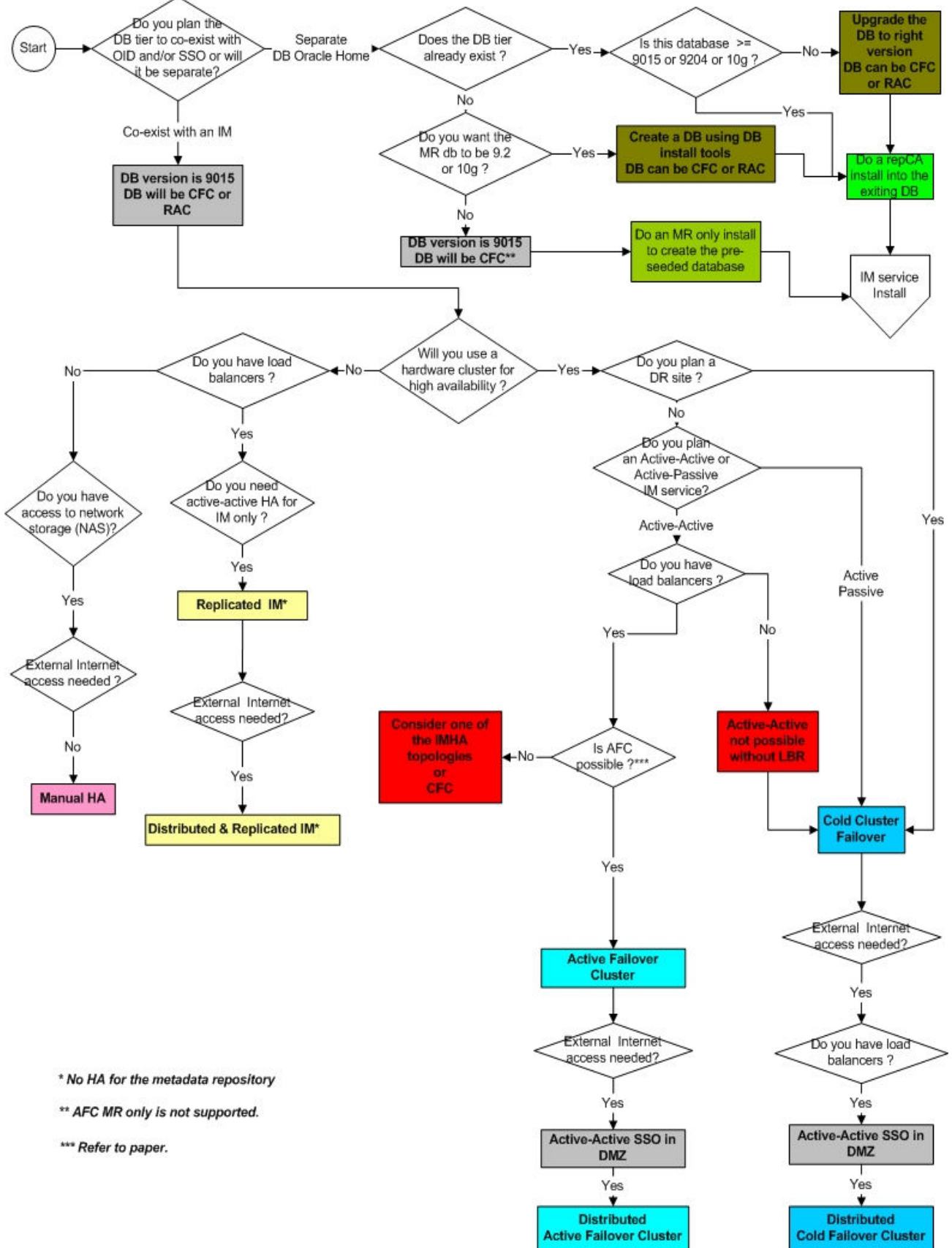
In case where the only the Oracle Net port can be opened in the DMZ, it may be necessary to locate OID in the DMZ as well along with SSO and DAS. In this case, SSO and DAS access to the OID is within the DMZ and there is not need to open the OID ports on the internal firewall.

Will OID process co-locate with SSO?

The IM service is made of the OID service and the SSO/DAS service. A customer may choose to separate these tiers on to different oracle homes, different boxes or different security zones. Typically, they are co-located if the customer expects the OID service demand to scale similarly to SSO. This is typically the case if an OID install will be used primarily by SSO and not much else. But if the OID service is used extensively by other mid-tier applications or collaboration suite and/or acts as the central directory service for the enterprise, it may be desirable to separate them out and deploy them as two tiers. This gives a better control over the two services, their deployment environment, ability to scale them and so on.

In many case, different groups in an IT department may manage the OID service and the single sign on service, In this case also, it may be desirable to separate them out.

Flow Chart



* No HA for the metadata repository
 ** AFC MR only is not supported.
 *** Refer to paper.

It is assumed that the database is either CFC or AFC and already has the MR seeded.



REFERENCES

- a) Oracle Application Server 10g Online Documentation 10g (9.0.4.0.0) for Microsoft Windows
- b) Oracle Application Server 10g Online Documentation 10g (9.0.4.0.0) for Solaris Operating System (SPARC)
- c) Oracle Application Server 10g Online Documentation 10g (9.0.4) for AIX-Based Systems, hp HP-UX PA-RISC (64-bit), hp Tru64 UNIX, and Linux x86
- d) Highly Available Distributed Identity Management, June 2004.
- e) Highly Available identity Management Deployment Example – Multi-box Identity Management, June 2004.
- f) Highly Available identity Management Deployment Example – Cold Failover Cluster Identity Management, June 2004.
- g) OracleAS 10g (9.0.4) (9.0.4) High Availability Certification Matrix, June 2004.



OracleAS 10g (9.0.4) Infrastructure Highly Available Architectures

May 2004

Author: Pradeep Bhat, Fermin Castro High Availability Systems Group, Oracle Corporation.

Contributing Authors:

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

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.