Configuring Highly Available OracleAS Identity Management with F5 BIG-IP® v9 Local Traffic Manager

OracleAS Maximum Availability Architecture White Paper
November 2006

Maximum Availability Architecture

Oracle Best Practices For High Availability

Configuring Highly Available OracleAS Identity Management with F5 BIG-IP v9 Local Traffic Manager

Configuring Highly Available OracleAS Identity Management with F5 BIG-IP v9 Application Traffic Manager

INTRODUCTION

Oracle Application Server includes security and identity management features to provide a combination of flexibility and security across enterprise applications and infrastructures. The availability of the entire system directly affects business processes, user productivity, and cost. OracleAS Identity Management 10g (10.1.4.0.1) is an integrated, standards-based Identity Management solution. OracleAS Identity Management consists of different components that are deployed on multiple tiers. The availability of each component has a direct impact on the availability of the system.

A highly available OracleAS Identity Management Solution deployment requires a highly available database, Identity Management services, and Middle Tier Applications. Oracle Identity Management 10g Release (10.1.4.01) consists of the following Identity Management components in various HA Topologies:

- Oracle Internet Directory (OID)
- Oracle Directory Integration & Provisioning (DIP)
- Oracle Single Sign On (SSO)
- Oracle Delegated Administrative Service (DAS)
- Oracle Identity Server
- Oracle Access Server
- Oracle Access Manager
- WebGate
- WebPass
- Oracle Identity Federation Server

The hardware load balancer is an integral component for providing high availability.

F5's BIG-IP v9 provides the necessary load balancer features for Oracle Identity Management high availability, load balancing and monitoring

Oracle Identity Management 10g Release (10.1.4.0.1) provides a high availability foundation and architecture, which can be suited to different customer requirements. The primary OracleAS Identity Management High Availability architecture solutions are:

- OracleAS Cluster (Identity Management) Topology
- Distributed OracleAS Cluster (Identity Management) Topology
- OracleAS Cold Failover Cluster (Infrastructure) Topology
- Distributed OracleAS Cold Failover Cluster (Infrastructure) Topology

- OracleAS Cold Failover Cluster (Identity Management) Topology
- Distributed OracleAS Cold Failover Cluster (Identity Management) Topology
- Oracle Access Manager Active-Active Topology
- Oracle Access Manager Active-Active Topology with Active-Passive OID
- OracleAS Cold Failover Cluster Topology for Oracle Identity Federation

For additional details on the specific Identity Management Features please reference http://download-west.oracle.com/docs/cd/B28196_01/index.htm and for or High Availability options please reference http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28186/toc.htm

For this paper, we will be discussing following two Identity Management High Availability architecture solutions:

- Oracle Access Manager Active-Active Topology

  The Oracle Access Manager Active-Active Topology includes multiple active OID instances and a corresponding RAC database for the OID repository. In this high availability deployment, a hardware load balancer distributes the incoming WebGate requests, incoming WebPass requests, and Oracle Internet Directory (OID) requests across simultaneously active instances of each of the respective servers. Failure of any one of the instances causes the load balancer to direct the subsequent requests to the remaining active instances.

- Distributed OracleAS Cluster (Identity Management) Topology

  In this high availability deployment, a hardware load balancer distributes the incoming Oracle Internet Directory (OID) and Directory Integration & Provisioning (DIP), the Single Sign On (SSO) and Delegated Administrative Service (DAS) requests across simultaneously active instances of each of the respective servers. Failure of any one of the instances causes the load balancer to direct the subsequent requests to the remaining active instances.

It’s also recommended that the F5 BIG-IP v9 Local Traffic Manager is deployed redundantly for a more robust HA implementation.

This implies that the hardware load balancer is an integral part of the architecture and provides load balancing as well as failover capabilities. The F5 BIG-IP Local Traffic Management (LTM) system offers several features that can be used to intelligently control SSL traffic as well. This will be briefly discussed in this paper. For high availability purposes, the load balancer is always deployed redundantly.

This paper has been jointly written by Oracle Corporation and F5 Networks and describes the configuration and operational best practices for using F5 BIG-IP as the load balancer with an OracleAS Identity Management 10g HA deployment.

F5 BIG-IP LOCAL TRAFFIC MANAGER TERMS

This document assumes familiarity with F5 BIG-IP v9, however this section does include the basic terminology referenced in this paper in order to help with further discussions. For a detailed description of these terms, please refer to the F5 BIG-IP Solutions Guide and the BIG-IP Reference Guide http://www.f5.com/solutions/.

The version of BIG-IP assumed for the rest of the discussion is BIG-IP Kernel 9.2.3 Build 107.0.

Load Balancing Pool

A ***load balancing pool*** is a set of devices, such as web servers, that are grouped together to receive and process traffic. Instead of sending client traffic to the destination IP address specified in the client request, the LTM system sends the request to any of the servers that are members of that pool.

When creating a pool, you assign servers (known as pool members) to the pool, and then associate the pool with a virtual server in the LTM system. The LTM system then directs traffic coming into the virtual server to a member of that pool. An individual server can belong to one or multiple pools, depending on how you want to manage your network traffic.

The specific pool member to which the LTM system chooses to send the request is determined by the load balancing method that you have assigned to that pool. A ***load balancing method*** is an algorithm that the LTM system uses to select a pool member for processing a request. For example, the default load balancing method is ***Round Robin***, which causes the LTM system to send each incoming request to the next available member of the pool, thereby distributing requests evenly across the servers in the pool.

Virtual server

Virtual servers are the most important component of any BIG-IP® local traffic management (LTM) configuration. A ***virtual server*** receives a client request, and instead of sending the request directly to the destination IP address specified in the packet header, sends it to any of several content servers that make up a load balancing pool. Virtual servers increase the availability of resources for processing client requests.

Not only do virtual servers distribute traffic across multiple servers, they also treat varying types of traffic differently, depending on your traffic-management needs. For example, a virtual server can enable compression on HTTP request data as it passes through the LTM system, or decrypt and re-encrypt SSL connections and verify SSL certificates. For each type of traffic, such as TCP, UDP, HTTP, SSL, and FTP, a virtual server can apply an entire group of settings, to affect the way that the LTM system manages that traffic type.

A given load balancer device may contain one or more virtual servers.

Profiles

The BIG-IP® local traffic management (LTM) system can manage application-specific network traffic in a variety of ways, depending on the protocols and services being used. For example, you can configure the LTM system to compress HTTP response data, or you can configure the system to authenticate SSL client certificates before passing requests on to a target server.

For each type of traffic that you want to manage, the LTM system contains configuration tools that you can use to intelligently control the behavior of that traffic. These tools are called profiles. A ***profile*** is a system-supplied configuration feature that enhances your capabilities for managing application-specific traffic. More specifically, a profile is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections.

Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Monitor

An important feature of the BIG-IP® local traffic management (LTM) system is a load-balancing tool called monitors. ***Monitors*** verify connections on pool members and nodes. A monitor can be either a health monitor or a performance monitor, designed to check the status of a pool, pool member, or node on an ongoing basis, at a set interval. If a pool member or node being checked does not respond within a specified timeout period, or the status of a pool member or node indicates that performance has degraded, the LTM system can redirect the traffic to another pool member or node.

Some monitors are included as part of the LTM system, while other monitors are user-created. Monitors that the LTM system provides are called ***pre-configured monitors***. User-created monitors are called ***custom monitors***.

ORACLE ACCESS MANAGER ACTIVE-ACTIVE TOPOLOGY

Architecture Overview

The primary HA Architecture focused on for this paper is the Oracle Access Manager in an Active-Active Topology, with multiple active OID instances and a corresponding RAC database. In this high availability deployment, a hardware load balancer distributes the incoming WebGate requests, incoming WebPass requests, and Oracle Internet Directory (OID) requests across simultaneously active instances of each of the respective servers. Failure of any one of the instances causes the load balancer to direct the subsequent requests to the remaining active instances. Following are the details for the Oracle Access Manager HA configuration with a load balancer as depicted in Figure below.

One point not clearly visible in Figure below is that the F5 BIG-IP Local Traffic Manager should also be redundant for a more robust HA implementation.

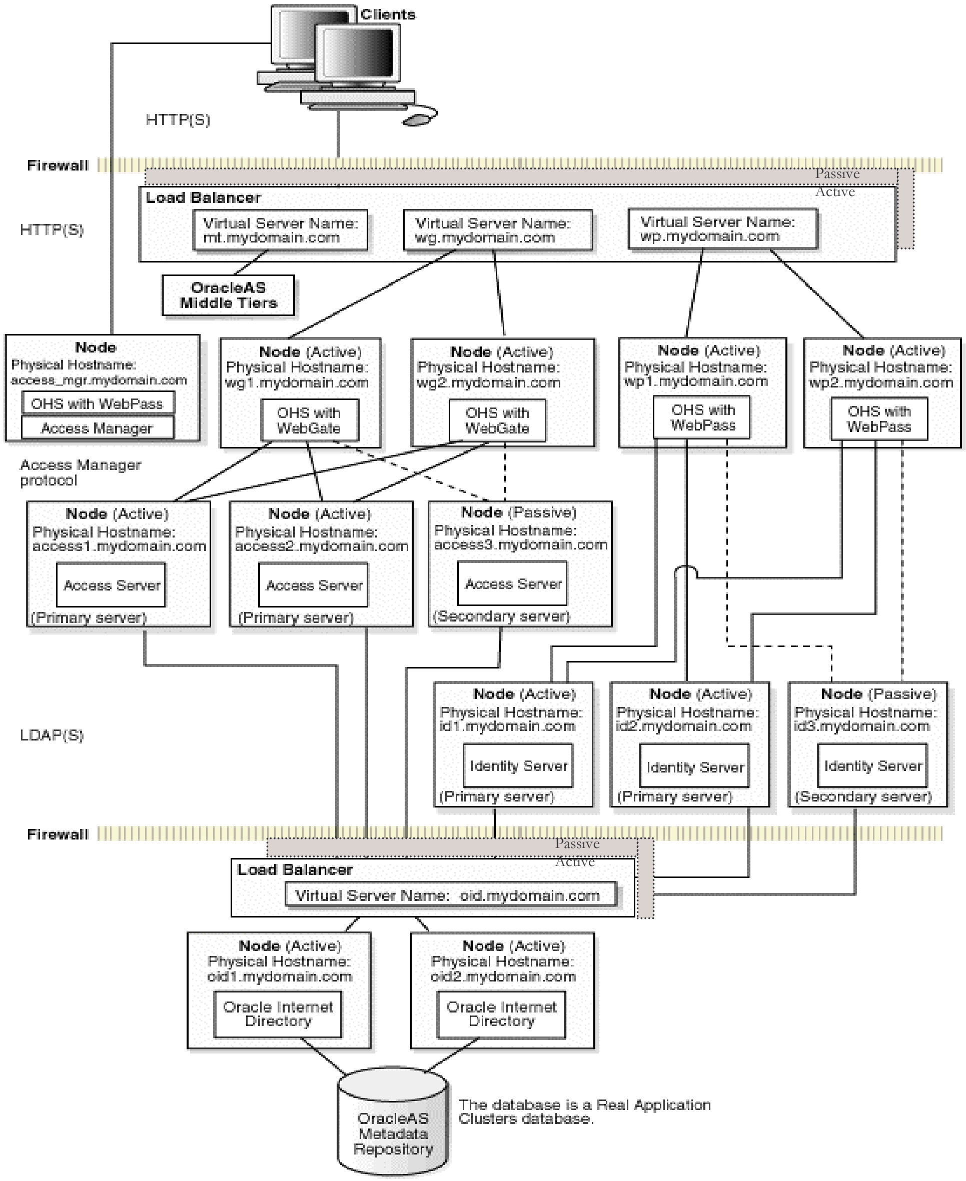
The load balancer configuration should not vary much between these different architectures other than the port numbers and the F5 BIG-IP pool members. Regardless of which Oracle Identity Management HA architecture you use, the same general configuration of F5 virtual servers is required. The primary virtual server names required for the architecture currently discussed are:

- oid.mydomain.com
- wg.mydomain.com
- wp.mydomain.com
- mt.mydomain.com

Each of the "root" virtual server names could be associated with multiple ports, and the same virtual server name is allowed with different ports.

Additional details about the Oracle Access Manager HA architectures are in the Oracle Application Server Identity Management 10g (10.1.4.0.1) HA Guide http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28186/toc.htm

and Oracle Application Server Identity Management 10g (10.1.4.0.1) Enterprise Deployment Guide http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28184/toc.htm.


Clients
HTTP(S)
Firewall
Passive
Active
Load Balancer
HTTP(S)
Virtual Server Name: mt.mydomain.com
Virtual Server Name: wg.mydomain.com
Virtual Server Name: wp.mydomain.com
OracleAS Middle Tiers
Node
Physical Hostname: access_mgr.mydomain.com
OHS with WebPass
Access Manager
Node (Active)
Physical Hostname: wg1.mydomain.com
OHS with WebGate
Node (Active)
Physical Hostname: wg2.mydomain.com
OHS with WebGate
Node (Active)
Physical Hostname: wp1.mydomain.com
OHS with WebPass
Node (Active)
Physical Hostname: wp2.mydomain.com
OHS with WebPass
Access Manager protocol
Node (Active)
Physical Hostname: access1.mydomain.com
Access Server
(Primary server)
Node (Active)
Physical Hostname: access2.mydomain.com
Access Server
(Primary server)
Node (Passive)
Physical Hostname: access3.mydomain.com
Access Server
(Secondary server)
LDAP(S)
Node (Active)
Physical Hostname: id1.mydomain.com
Identity Server
(Primary server)
Node (Active)
Physical Hostname: id2.mydomain.com
Identity Server
(Primary server)
Node (Passive)
Physical Hostname: id3.mydomain.com
Identity Server
(Secondary server)
Firewall
Passive
Active
Load Balancer
Virtual Server Name: oid.mydomain.com
Node (Active)
Physical Hostname: oid1.mydomain.com
Oracle Internet Directory
Node (Active)
Physical Hostname: oid2.mydomain.com
Oracle Internet Directory
OracleAS Metadata Repository
The database is a Real Application Clusters database.

For purposes of the Oracle Access Manager HA configuration with the F5 BIG-IP, it's not necessary to discuss the Database tier because it does not require a load balancer. The focus will be on the Oracle Access Manager HA configuration.

For the following discussions and examples, here is the high-level Oracle Access Manager configuration of the physical nodes:

Server type	Hostname
Hosts for the database tier Not Shown in Figure 1	d1.mydomain.com d2.mydomain.com
Hosts for the OID tier	oid1.mydomain.com oid2.mydomain.com
Hosts for WebGate tier	wg1.mydomain.com wg2.mydomain.com
Hosts for WebPass tier Same tier as WebGate. Requires different OHS.	wp1.mydomain.com wp2.mydomain.com
Hosts for Access Servers WebGate used for failover and load-balancing.	access1.mydomain.com access2.mydomain.com access3.mydomain.com
Hosts for Identity Servers WebPass used for failover and load-balancing.	id1.mydomain.com id2.mydomain.com id3.mydomain.com
Hosts for Access Manager (Requires it's own OHS)	access_mgr.mydomain.com

Install Overview

The load balancer setup must be done prior to the Oracle Access Manager HA install. Then during the Oracle Access Manager HA install use the same ports as specified in the load balancer setup for subsequent installs, which will be part of the same active-active configuration. This can be enforced by using either the staticports.ini file or manually entering the same port number information. In this manner you can ensure that the ports agree with the load balancer configuration and are consistent across multiple nodes.

Here is a high-level view of the steps involved in setting up an Oracle Access Manager HA installation that will use the F5 BIG-IP Application Traffic Manager.

1. Complete the prerequisites for the installation
2. Configure the F5 BIG-IP configuration.
   - Create pools
   - Create profiles
   - Create virtual servers and associate them with pools
   - Associate virtual servers with profiles, if required

- Create monitors and associate them with the pools and/or nodes
- Propagate information to the redundant BIG-IP

3. Note all the ports information and, wherever required, use these details for each Oracle Access Manager HA install step based on the load balancer configuration.
4. If a firewall separates your load balancer and the servers, then ensure that appropriate ports are open for the two way traffic across the firewall. For more details, reference the Oracle Application Server Identity Management 10g (10.1.4.0.1) Enterprise Deployment Guide http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28184/toc.htm.
5. Mark the non-installed node(s) as down in the load balancer configuration as required. This will ensure clients are not yet routed to additional nodes included as part of the pool, but not yet fully installed or configured. This will be detailed in the HA Install section.
6. Perform the Oracle Access Manager HA installs using the ports information that was noted earlier.

The details of these steps follow.

Load Balancer Setup - Prerequisites

Understanding the load balancer components, planning out the deployment, and walking through it are key to a successful implementation.

1. Decide on the virtual server names and ports (ensure the ports are free on the appropriate hosts). For this paper example we will use the following virtual server names:
   - oid.mydomain.com
   - wg.mydomain.com
   - wp.mydomain.com
   - mt.mydomain.com

   The ports are summarized in Table 1
2. Get the IP addresses assigned to the virtual servers and ensure that they are part of your Domain Name Server (DNS).
3. Plan the load balancer configuration described in Table 1.

Virtual Server:port	Pool	Pool Nodes	Persistence	Purpose / *staicports.ini setting*
oid.mydomain.com:389	oid_pool	oid1.mydomain.com:389 oid2.mydomain.com:389	No persistence	IMHA OiD *Oracle Internet Directory port*
oid.mydomain.com:636	oidssl_pool	oid1.mydomain.com:636 oid2.mydomain.com:636	No persistence	IMHA OiD SSL *Oracle Internet Directory (SSL) port*
wp.mydomain.com:7777	wp_pool	wp1.mydomain.com:7777 wp2.mydomain.com:7777	Cookie persistence	WebPass tier 7777 should match the *Oracle HTTP Server port*
wg.mydomain.com:7778	wg_pool	wg1.mydomain.com:7778 wg2.mydomain.com:7778	Cookie persistence	WebGate tier 7778 should match the *Oracle HTTP Server port*

Table 1 Load Balancer Configuration Summary

Configure Load Balancer

The following subsections describe the steps to configure a load balancer in detail.

Create Pools

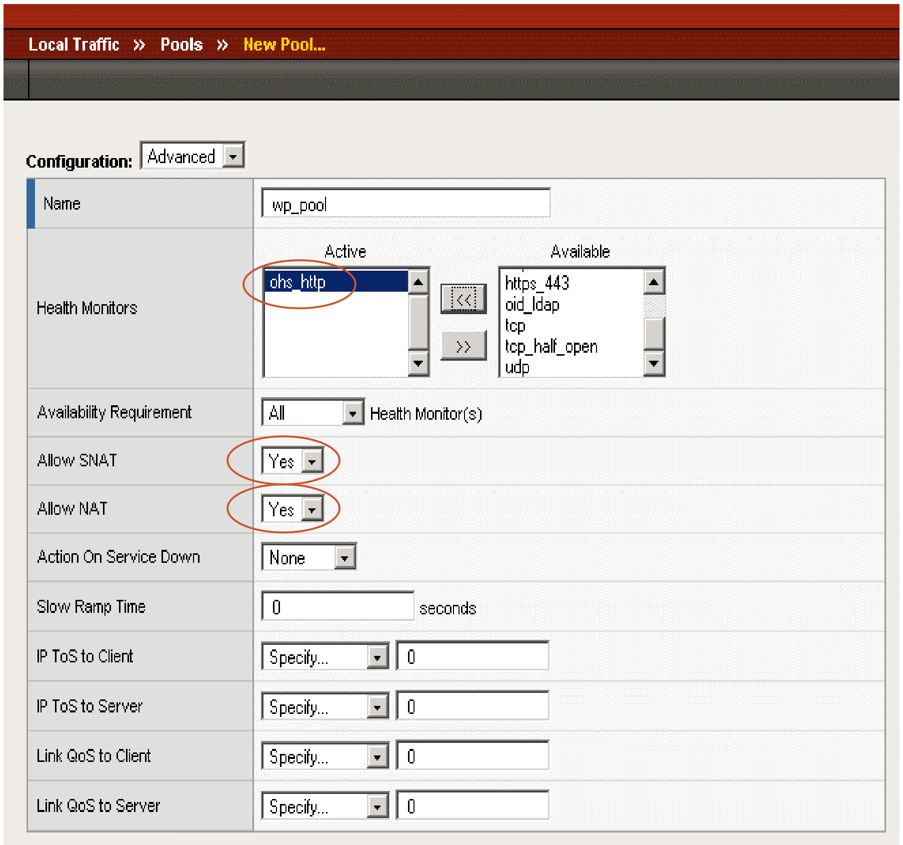
To create a new pool using the BIG-IP configuration tool, connect to the active device of the redundant load balancer configuration and click **Pools** and then click the **+**. Each pool has to be created separately. The characteristics of these pools are described in the Table 2.

Pool Name	Pool Members	Monitor
oid_pool	oid1.mydomain.com:389 Oid2.mydomain.com:389	oid_ldap
oidssl_pool	oid1.mydomain.com:636 oid2.mydomain.com:636	oid_ldapssl
wp_pool	wp1.mydomain.com:7777 wp2.mydomain.com:7777	ohs_http
wg_pool	wg1.mydomain.com:7778 wg2.mydomain.com:7778	ohs_http

Table 2 Load Balancer Pool Summary

In addition, for each pool the following should be allowed (they are allowed by default),

- Allow SNAT
- Allow NAT



Local Traffic » Pools » New Pool...

Configuration: Advanced

Name	wp_pool
Health Monitors	Active: ohs_http Available: https_443, oid_ldap, tcp, tcp_half_open, udp
Availability Requirement	All Health Monitor(s)
Allow SNAT	Yes
Allow NAT	Yes
Action On Service Down	None
Slow Ramp Time	0 seconds
IP ToS to Client	Specify... 0
IP ToS to Server	Specify... 0
Link QoS to Client	Specify... 0
Link QoS to Server	Specify... 0

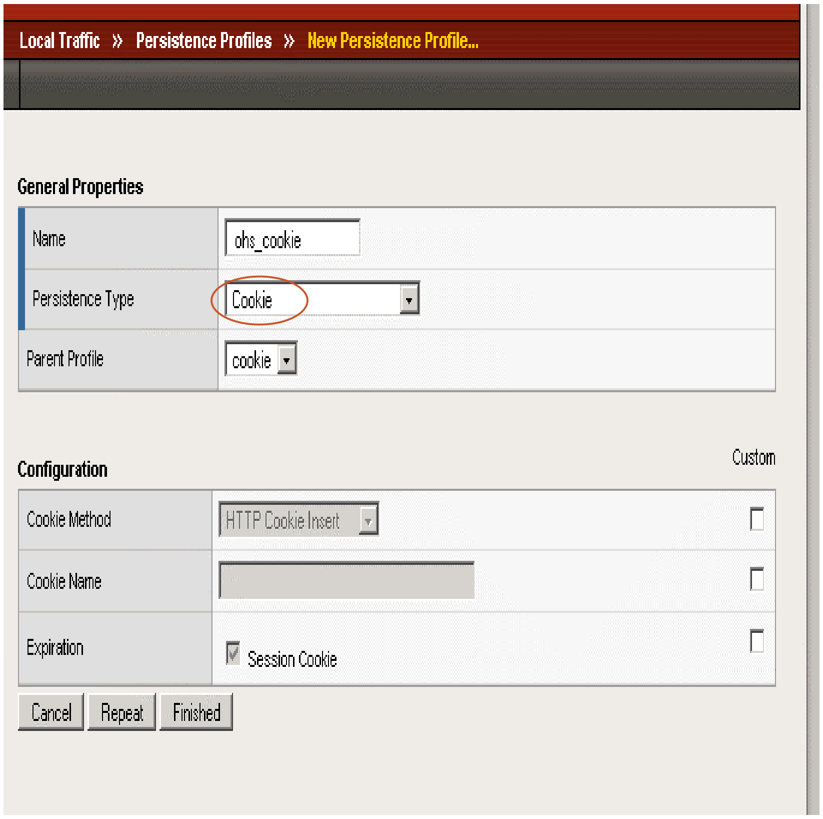
If custom Health Monitor is not created at this time, it can be associated later with the pool or individual members of the pool.

Create Profiles

To create a profile, click Profiles and then click the + to add a new profile. Select the type of profile you want to create. Each of the profile has to be created separately. The characteristics of these profiles are described in the Table 3.

Profile Name	Parent Profile	Virtual Server
ohs_cookie	Persistence - Cookie	wp.mydomain.com:7777 wg.mydomain.com:7778
ws_http	http	wp.mydomain.com:7777 wg.mydomain.com:7778

Table 3 Load Balancer Pool Summary



Local Traffic » Persistence Profiles » New Persistence Profile...

General Properties

Name	ohs_cookie
Persistence Type	Cookie
Parent Profile	cookie

Configuration

		Custom
Cookie Method	HTTP Cookie Insert	□
Cookie Name		□
Expiration	☑ Session Cookie	□

Create Virtual Servers and Associate them with Pools and Profiles

Create the virtual servers and associate each with its respective pool, and if required with the appropriate profile.

To create a virtual server, click on **Virtual Servers** and then click on **+** to add a new virtual server.

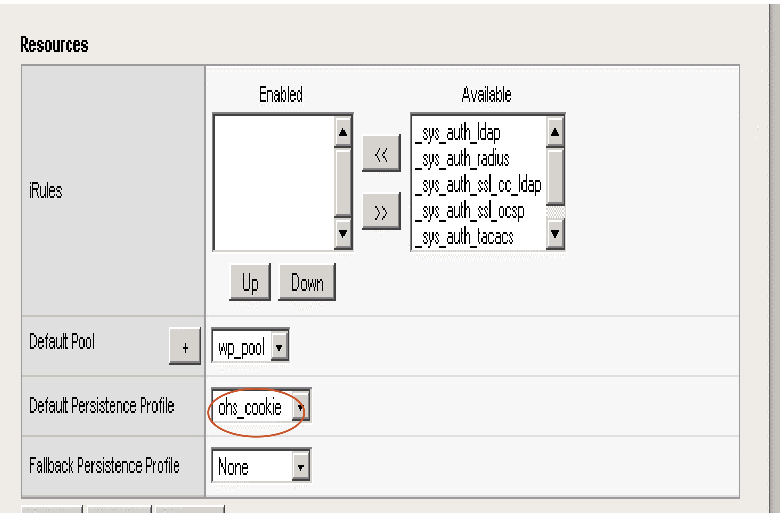
There are three primary steps for creating a virtual server:

1. Configure General Properties Virtual IP Address and Service – Here, you enter the virtual host name and the port (service).
2. Configure Basic/Advanced Properties – Here, accept the default settings and do not change anything for most pools..
3. Select Physical Resources – Here, select the pool and Persistence profiles.

Address	Pool	Profile
oid.mydomain.com:389	oid_pool	Not applicable
oid.mydomain.com:636	oidssl_pool	Not applicable

Address	Pool	Profile
wp.mydomain.com:7777	wp_pool	ohs_cookie ws_http
wg.mydomain.com:7777	wg_pool	ohs_cookie ws_http

Table 4 Load Balancer Pool Profile Summary



Resources

iRules

Default Pool: wp_pool

Default Persistence Profile: ohs_cookie

Fallback Persistence Profile: None

For virtual servers associated with OHS pools, select appropriate HTTP Profile In our configuration, for the virtual server wp.mydomain.com, and wg.mydomain.com, we will select HTTP Profile as “ws_http”. These two virtual servers require persistence as well and “ohs_cookie” will be selected as Default Persistence Profile.

Create Monitors and Associate them with the Nodes

Create the monitors listed in Table 5.

To create a monitor, click **Monitors** and then click **+** to add a new monitor.

Monitor name	**Configuration**
oid_ldap	Import Settings from LDAP **Interval:** 30 **Timeout:** 95 **Username:** <a username full directory name (DN) > **Password:** <username password> **Filter:** cn=***databasename*** ***Note:*** *It is recommended that a dedicated account be used to monitor the LDAP service to prevent operational conflicts with other uses of the account. In particular, administrative accounts such as orcladmin should* ***not*** *be used for the username.*
oid_ldapssl	Import Settings from tcp **Interval:** 30 **Timeout:** 95
ohs_http	Import Settings from http **Interval:** 30 **Timeout:** 95

Table 5 Monitor Summary

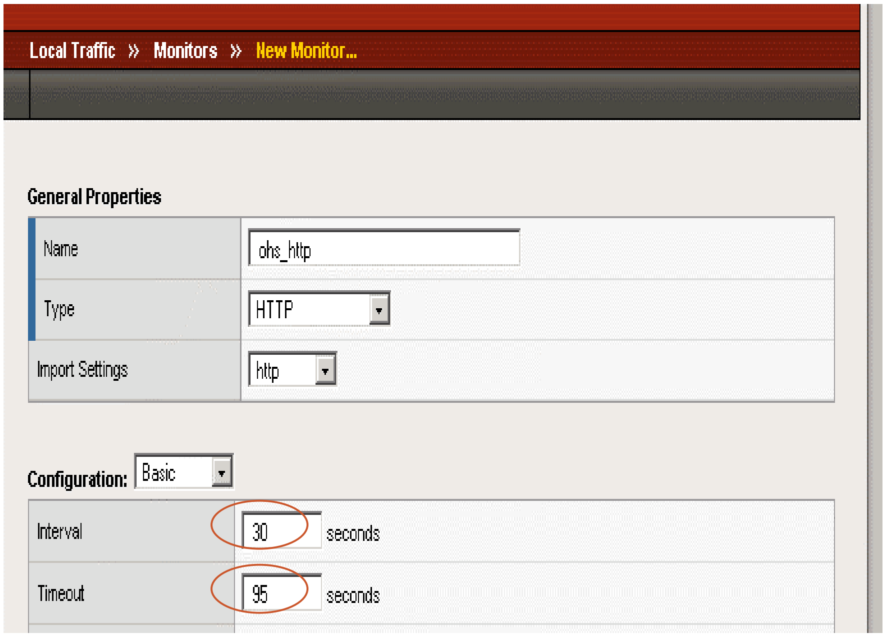
For the oid_ldap monitor, it is recommended that a dedicated account be used to monitor the LDAP service to prevent operational conflicts with other uses of the account. In particular, administrative accounts such as orcladmin should not be used for the monitor username. The username field should be similar to:

```
cn=ldapmUser,cn=Users,dc=mydomain,dc=com
```

where `ldapmUser` is an ldap account that was provisioned with minimum privileges. The validity of the user DN can be verified at the operating system level by executing an `ldapbind` command for the user DN as follows:

```
ldapbind  -h ldap.mydomain.com -p 389 -D \
"cn=ldapmUser,cn=Users,dc=mydomain,dc=com" -w welcome1
```

The interval and timeout for the monitors should be adjusted according to your requirements.



General Properties

Name: ohs_http

Type: HTTP

Import Settings: http

Configuration: Basic

Interval: 30 seconds

Timeout: 95 seconds

Interval is the frequency at which BIG-IP pings the service and ***timeout*** is the maximum time it waits each time before determining whether the service is down.

A low interval time implies frequent pings but faster automatic failover in case of the service going down.

The timeout value should be a minimum of interval*3+1. For slow backend servers or servers with higher load, it should be adjusted higher to prevent false alarms. The values in Table 5 are the recommended default values.

After the monitors have been created, associate the monitors to the nodes as Table 6 indicates.

Monitor Name	Nodes	Purpose
oid_ldap	oid1.mydomain.com:389 oid2.mydomain.com:389	*Oracle Internet Directory port*
oid_ldapssl	oid1.mydomain.com:636 oid2.mydomain.com:636	*Oracle Internet Directory (SSL) port*
ohs_http	wp1.mydomain.com:7777 wp2.mydomain.com:7777	*Oracle HTTP Server port*
ohs_http	wg1.mydomain.com:7778 wg2.mydomain.com:7778	*Oracle HTTP Server port*

Table 6 Monitor Node Association Summary

Propagate Information to the Redundant BIG-IP

Because a redundant load balancer is highly recommended for the deployment, the preceding configuration done performed on the active load balancer should be propagated to the standby load balancer in the redundant configuration. To do so using the BIG-IP Configuration Utility, click **Redundant Properties** on the home page and then click **Synchronize Configuration**.

This will propagate the newly created configuration to the redundant load balancer, which will then be ready to service the new configuration in the event of a failure of the active load balancer.

Oracle Access Manager High Availability Installation

Here, we describe the pre-install and install steps for the Oracle Access Manager HA deployment. These steps are relevant to the BIG-IP Local Traffic Manager usage in this configuration. For other detailed install steps refer to the Installation Guide, High Availability Guide and Enterprise Deployment Guide of Oracle Application Server 10g (10.1.4.0.1).

Pre-Installation Tasks

The following sections describe the pre-installation steps for installing Oracle Access Manager in a high availability environment.

Validate that ports are not in use

Before proceeding with the installation and using the load balancer ports as previously described, you should ensure that the ports are free on the appropriate nodes. This can be done by using the `netstat` command or by verifying with your network or system administrator. A simple netstat command to verify port 7777 is not in use would be as follows:

```
netstat –a | grep 7777
```

The preceding command should not return any line in response. If it returns a line with a "tcp … *:7777 LISTEN" then the queried port is in use.

Static Ports Files

Instead of using default ports, you can assign custom port numbers for Oracle Access Manager components during the installation. For this, you must create a file containing the component names and port numbers. This file is referred to as the static ports file or staticports.ini.

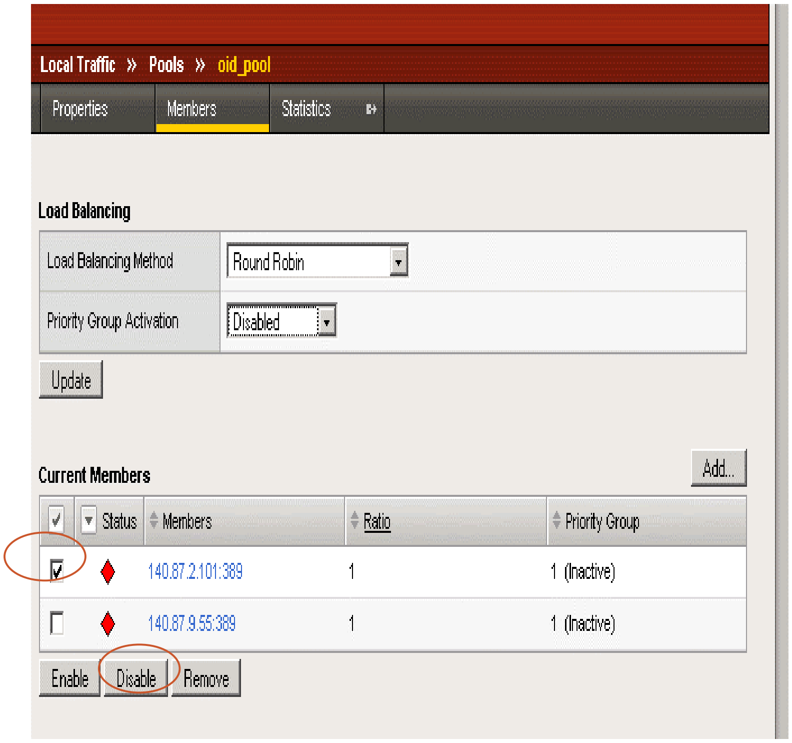
The static ports feature of Oracle Universal Installer (OUI) ensures that the only specific ports will be used for the install. However, for this, these ports must be free on all the relevant nodes. Your planning process should take this into account while deciding the various ports. Some installs do not all use staticports.ini file. In such installs manually provide the port numbers to be used during install, otherwise configure your load balancer using the ports available at the install time.

Please refer to the Appendix A for the template and sample files that go with the install steps.

Oracle Internet Directory Virtual Server Load Balancer Configuration

A requirement for the OID/DIP install is to point the load balancer to only one OID node during the install. This is because the load balancer must direct traffic to only the first node until all OID nodes are installed.

To disable traffic to non-install node(s), click **Members** and then check the non-install node(s) and "***Disable***" for the non-install OID node oid2.mydomain.com:389 and the SSL node oid2.mydomain.com:636, as illustrated in Figure below.



Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Disabled

Current Members

☑	Status	Members	Ratio	Priority Group
☑	◆	140.87.2.101:389	1	1 (Inactive)
□	◆	140.87.9.55:389	1	1 (Inactive)

Installation Tasks

During the installation one or more installation sessions may be required. In each case, make sure that you start the installation process with the arguments required for it to use the correct staticports.ini file.

Table 7 summarizes the installation step and the command to use to initiate the installation process.

Install Step	Install Command
OID / DIP	`./runInstaller`
OHS for WebPass	`./runInstaller`
Identity Server	`./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server`
WebPass	`./Oracle_Access_Manager10_1_4_0_1_linux_OHS_WebPass`
Policy Manager	`./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_Policy_Manager`
Access Server	`./Oracle_Access_Manager10_1_4_0_1_linux_Access_Server`
WebGate	`./Oracle_Access_Manager10_1_4_0_1_linux_OHS_WebGate`

Table 7 Installation Steps and Commands

Post-Installation Tasks

The post-installation tasks described here are relevant only to the BIG-IP Local Traffic Manager usage in this configuration and common to all installations.

Verify Port Settings

After each installation, verify the port settings match your load balancer configuration. To verify, check the `$ORACLE_HOME/install/portlist.ini` file.

Enable Oracle Internet Directory Traffic to Both Nodes

Following the installation of both OID/DIP, enable OID traffic to all nodes. To enable traffic to all node(s), click **Members** and then check the disabled node(s) and "***Enable***" for the disabled OID node oid2.mydomain.com:389 and the SSL node oid2.mydomain.com:636.

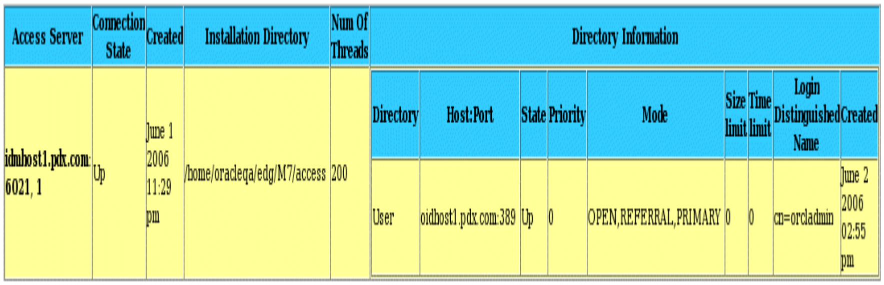
Validation Step

Perform the following tasks to validate if the installation was successful:

- Ensure that the Identity Server, WebPass, and Access Server are running.
- Access this URL:

```
https://WEBHOST1:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
```

The WebGate page appears as shown below:



Access Server	Connection State	Created	Installation Directory	Num Of Threads	Directory Information								
					Directory	Host:Port	State	Priority	Mode	Size limit	Time limit	Login Distinguished Name	Created
idmhost1.pdx.com:6021, 1	Up	June 1 2006 11:29 pm	/home/oracleqa/edg/M7/access	200	User	oidhost1.pdx.com:389	Up	0	OPEN,REFERRAL,PRIMARY	0	0	cn=orcladmin	June 2 2006 02:55 pm

Configuring SSL for Access Server

A common security requirement is to SSL encrypt the traffic from the client browser to the load balancer. The load balancer then acts as an SSL accelerator and directs the converted http traffic to the web tier HTTP listener. This provides the required security but does not burden the web tier machines with the overhead of SSL. The following are the post-install steps to configure the web tier and the BIG-IP load balancer for this.

Configuration for Load Balancer

For Load Balancer configuration, use the procedure as detailed above.

- Create pool

Pool Name	Pool Members	Monitor
wgssl_pool	wg1.mydomain.com:7778 wg2.mydomain.com:7778	ohs_https

- Create profiles

Profile Name	Parent Profile	Virtual Server
httpssl	clientssl	wg.mydomain.com:7779

- Create virtual servers and associate them with pools

Address	Pool	Profile
wg.mydomain.com:7779	wgssl_pool	ohs_cookie ws_http httpssl

For virtual servers associated with SSL pools, based on the configuration, select appropriate SSL Profile (Client) and SSL Profile (Server).

Client SSL: clientssl is used from Client – [HTTPS] → Load Balancer

Server SSL: serverssl is used from Load Balancer – [HTTPS] → Oracle HTTP Server

In our configuration,

Client – [HTTPS] → Load Balancer – [HTTP] → Oracle HTTP Server

for the virtual server wg.mydomain.com, we will select SSL Profile (Client) as “httpssl”.

- Create monitors and associate them with the pools and/or nodes

Monitor name	Configuration
ohs_https	Import Settings from https **Interval:** 30 **Timeout:** 95 **Send String:** GET /sso/status **Receive String:** OC4J_SECURITY is running

Configuration for Access Server

If the Load Balancing Router is configured for SSL acceleration, and Oracle HTTP Server is listening on a non-SSL port, you must perform the following steps to make the Access Server function properly:

- Access the Access System Console at this URL:

  http://ADMINHOST:port/access/oblix

- Click the Access System Console link.
- Log in as an administrator.
- Click the Access System Configuration tab.
- Navigate to the WebGate entries section.
- Add the user-defined parameter ProxySSLHeaderVar, providing a header variable name, for example:

  Name: ProxySSLHeaderVarVal: IS_SSL

- Modify the Load Balancing Router (reverse proxy web server) settings to insert an HTTP header string that sets the `IS_SSL` value to `ssl`. For example, in the F5 load balancer, in Advanced Proxy Settings, you add the HTTP header string `IS_SSL:ssl`.

DISTRIBUTED ORACLEAS CLUSTER (IDENTITY MANAGEMENT) TOPOLOGY

Architecture Overview

There are many OracleAS Cluster HA architectures that are described in detail in the Oracle Application Server Identity Management 10g (10.1.4.0.1) HA Guide http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28186/toc.htm.

For this example we will describe the Distributed OracleAS Cluster (Identity Management) configuration with a load balancer as depicted in Figure 2.

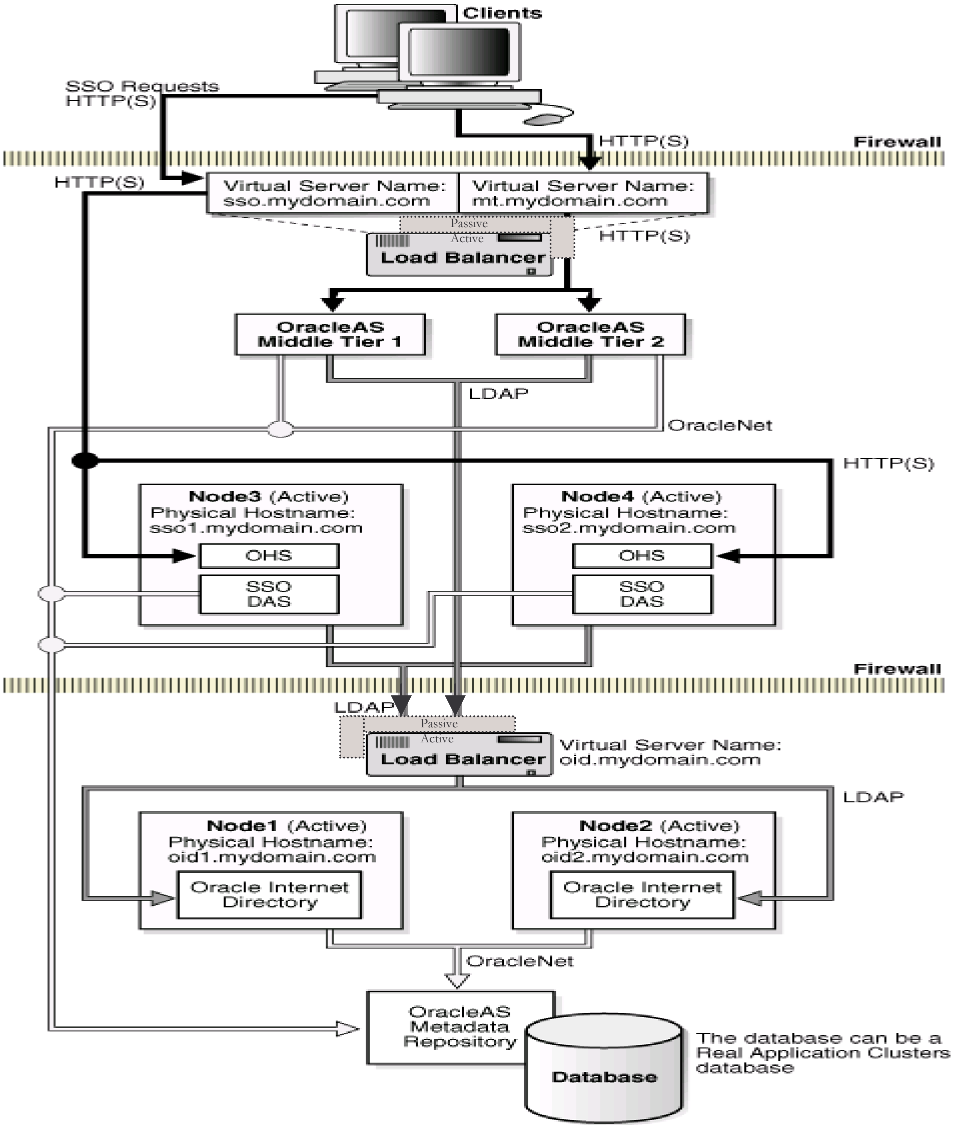
One point not clearly visible in Figure 2 is that the F5 BIG-IP Local Traffic Manager should also be redundant for a more robust HA implementation.

The load balancer configuration should not vary much between these different architectures other than the port numbers and the F5 BIG-IP pool members. Regardless of which Oracle Identity Management HA architecture you use, the same general configuration of F5 virtual servers is required. However, the pool and pool member configurations will vary among the different architectures. The primary virtual server names required are:

- oid.mydomain.com
- sso.mydomain.com
- mt.mydomain.com

Each of the "root" virtual server names could be associated with multiple ports, and the same virtual server name is allowed with different ports.

Additional details about the OracleAS Cluster (Identity Management) HA architectures are in the Oracle Application Server Identity Management 10g (10.1.4.0.1) HA Guide.



For purposes of the Distributed OracleAS Cluster (Identity Management) HA configuration with the F5 BIG-IP, it’s not necessary to discuss the Database tier because it does not require a load balancer. The focus will be on the OracleAS (Identity Management) HA configuration.

For purposes of discussion and example, here is the high-level Distributed IM configuration of the physical nodes:

Server type	Hostname
Hosts for the database tier	Not shown in Figure 2
Hosts for the OID tier	oid1.mydomain.com oid2.mydomain.com
Hosts for SSO/DAS tier	sso1.mydomain.com sso2.mydomain.com

Install Overview

The load balancer setup must be done prior to the Distributed OracleAS Cluster (Identity Management) install. Then during the Distributed OracleAS Cluster (Identity Management) HA install use the same ports as specified in the load balancer setup for subsequent installs, which will be part of the same active-active configuration. This can be enforced by using either the staticports.ini file or manually entering the same port number information. In this manner you can ensure that the ports agree with the load balancer configuration and are consistent across multiple nodes.

Here is a high-level view of the steps involved in setting up a Distributed OracleAS Cluster (Identity Management) HA installation that will use the F5 BIG-IP Application Traffic Manager.

1. Complete the prerequisites for the installation
2. Configure the F5 BIG-IP configuration.
    - Create pools
    - Create profiles
    - Create virtual servers and associate them with pools
    - Associate virtual servers with profiles, if required
    - Create monitors and associate them with the pools and/or nodes
    - Propagate information to the redundant BIG-IP
3. Note all the ports information and, wherever required, use these details for each Distributed OracleAS Cluster (Identity Management) HA install step based on the load balancer configuration.
4. If a firewall separates your load balancer and the servers, then ensure that appropriate ports are open for the two way traffic across the firewall. Refer Oracle Application Server Identity Management 10g (10.1.4.0.1) Enterprise Deployment Guide for more details.

5. Mark the non-installed node(s) as down in the load balancer configuration as required. This will ensure clients are not yet routed to additional nodes included as part of the pool, but not yet fully installed or configured. This will be detailed in the HA Install section.
6. Perform the Distributed OracleAS Cluster (Identity Management) HA installs using the ports information that was noted earlier.

The details of these steps follow.

Load Balancer Setup – Prerequisites

1. Decide on the virtual server names and ports (ensure the ports are free on the appropriate hosts). For this paper example we will use the following virtual server names:
   - oid.mydomain.com
   - sso.mydomain.com
   - mt.mydomain.com
2. The ports are summarized in Table 8
3. Get the IP addresses assigned to the virtual servers and ensure that they are part of your Domain Name Server (DNS).
4. Plan the load balancer configuration described in Table 8.

Understanding the load balancer components, planning out the deployment, and walking through it are key to a successful implementation.

Virtual Server:port	Pool	Pool Nodes	Persistence	Purpose / *staicports.ini setting*
oid.mydomain.com:389	oid_pool	oid1.mydomain.com:389 oid2.mydomain.com:389	No persistence	IMHA OiD *Oracle Internet Directory port*
oid.mydomain.com:636	oidssl_pool	oid1.mydomain.com:636 oid2.mydomain.com:636	No persistence	IMHA OiD SSL *Oracle Internet Directory (SSL) port*
sso.mydomain.com:7777	sso_pool	sso1.mydomain.com:7777 sso2.mydomain.com:7777	No persistence	IMHA SSO / DAS *Oracle HTTP Server port*

Table 8 Load Balancer Configuration Summary

Configure Load Balancer

The following subsections describe the steps to configure a load balancer in detail.

Create Pools

To create a new pool using the BIG-IP configuration tool, connect to the active device of the redundant load balancer configuration and click **Pools** and then click the **+**. Each pool has to be created separately. The characteristics of these pools are described in the Table 9.

Pool Name	Pool Members	Monitor
oid_pool	oid1.mydomain.com:389 Oid2.mydomain.com:389	oid_ldap
oidssl_pool	oid1.mydomain.com:636 oid2.mydomain.com:636	oid_ldapssl
sso_pool	sso1.mydomain.com:7777 sso2.mydomain.com:7777	ohs_http

Table 9 Load Balancer Pool Summary

In addition, for each pool the following should be allowed (they are allowed by default),

- Allow SNAT
- Allow NAT

If custom Health Monitor is not created at this time, it can be associated later with the pool or individual members of the pool.

Create Profiles

To create a profile, click Profiles and then click the + to add a new profile. Select the type of profile you want to create. Each of the profile has to be created separately. The characteristics of these profiles are described in the Table 10.

Profile Name	Parent Profile	Virtual Server
ws_http	http	sso.mydomain.com:7777

Table 10 Load Balancer Pool Summary

Create Virtual Servers and Associate them with Pools and Profiles

Create the virtual servers and associate each with its respective pool, and if required with the appropriate profile.

To create a virtual server, click on **Virtual Servers** and then click on **+** to add a new virtual server.

There are three primary steps for creating a virtual server:

1. Configure General Properties Virtual IP Address and Service – Here, you enter the virtual host name and the port (service).
2. Configure Basic/Advanced Properties – Here, accept the default settings and do not change anything for most pools.
3. Select Physical Resources – Here, select the pool.

Address	Pool	Profile
oid.mydomain.com:389	oid_pool	Not applicable
oid.mydomain.com:636	oidssl_pool	Not applicable
sso.mydomain.com:7777	sso_pool	ws_http

Table 11 Load Balancer Pool Profile Summary

For virtual servers associated with OHS pools, select appropriate HTTP Profile In our configuration, for the virtual server sso.mydomain.com, we will select HTTP Profile as “ws_http”.

Create Monitors and Associate them with the Nodes

Create the monitors listed in Table 12.

To create a monitor, click **Monitors** and then click **+** to add a new monitor.

Monitor name	**Configuration**
oid_ldap	Import Settings from LDAP **Interval:** 30 **Timeout:** 95 **Username:** <a username full directory name (DN) > **Password:** <username password> **Filter:** cn=***databasename*** ***Note:*** *It is recommended that a dedicated account be used to monitor the LDAP service to prevent operational conflicts with other uses of the account. In particular, administrative accounts such as orcladmin should* ***not*** *be used for the username.*
oid_ldapssl	Import Settings from tcp **Interval:** 30 **Timeout:** 95
ohs_http	Import Settings from http **Interval:** 30 **Timeout:** 95

Table 12 Monitor Summary

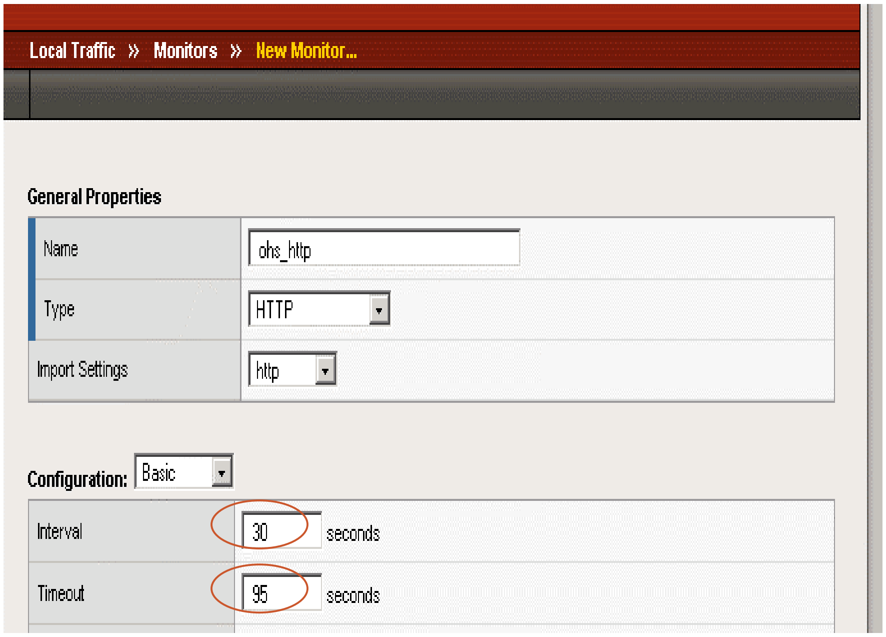
For the oid_ldap monitor, it is recommended that a dedicated account be used to monitor the LDAP service to prevent operational conflicts with other uses of the account. In particular, administrative accounts such as orcladmin should not be used for the monitor username. The username field should be similar to:

```
cn=ldapmUser,cn=Users,dc=mydomain,dc=com
```

where `ldapmUser` is an ldap account that was provisioned with minimum privileges. The validity of the user DN can be verified at the operating system level by executing an `ldapbind` command for the user DN as follows:

```
ldapbind  -h ldap.mydomain.com -p 389 -D \
"cn=ldapmUser,cn=Users,dc=mydomain,dc=com" -w welcome1
```

The interval and timeout for the monitors should be adjusted according to your requirements.



General Properties

Name	ohs_http
Type	HTTP
Import Settings	http

Configuration: Basic

Interval	30 seconds
Timeout	95 seconds

Interval is the frequency at which BIG-IP pings the service and ***timeout*** is the maximum time it waits each time before determining whether the service is down.

A low interval time implies frequent pings but faster automatic failover in case of the service going down.

The timeout value should be a minimum of interval*3+1. For slow backend servers or servers with higher load, it should be adjusted higher to prevent false alarms. The values in Table 5 are the recommended default values.

After the monitors have been created, associate the monitors to the nodes as Table 13 indicates.

Monitor Name	Nodes	Purpose
oid_ldap	oid1.mydomain.com:389 oid2.mydomain.com:389	*Oracle Internet Directory port*
oid_ldapssl	oid1.mydomain.com:636 oid2.mydomain.com:636	*Oracle Internet Directory (SSL) port*
ohs_http	sso1.mydomain.com:7777 sso2.mydomain.com:7777	*Oracle HTTP Server port*

Table 13 Monitor Node Association Summary

Propagate Information to the Redundant BIG-IP

Because a redundant load balancer is highly recommended for the deployment, the preceding configuration done performed on the active load balancer should be propagated to the standby load balancer in the redundant configuration. To do so using the BIG-IP Configuration Utility, click **Redundant Properties** on the home page and then click **Synchronize Configuration**.

This will propagate the newly created configuration to the redundant load balancer, which will then be ready to service the new configuration in the event of a failure of the active load balancer.

Distributed OracleAS Cluster (Identity Management) High Availability Installation

Here, we describe the pre-install and install steps for the Distributed OracleAS Cluster (Identity Management) HA deployment. These steps are relevant to the BIG-IP Local Traffic Manager usage in this configuration. For other detailed install steps refer to the Installation Guide and High Availability Guide of Oracle Application Server 10g (10.1.4.0.1).

Pre-Installation Tasks

The following sections describe the pre-installation steps for installing Distributed OracleAS Cluster (Identity Management) in a high availability environment.

Validate that ports are not in use

Before proceeding with the installation and using the load balancer ports as previously described, you should ensure that the ports are free on the appropriate nodes. This can be done by using the `netstat` command or by verifying with your network or system administrator. A simple netstat command to verify port 7777 is not in use would be as follows:

```
netstat –a | grep 7777
```

The preceding command should not return any line in response. If it returns a line with a "tcp … *:7777 LISTEN" then the queried port is in use.

Static Ports Files

Instead of using default ports, you can assign custom port numbers for Oracle Identity Management components during the installation. For this, you must create a file containing the component names and port numbers. This file is referred to as the static ports file or staticports.ini.

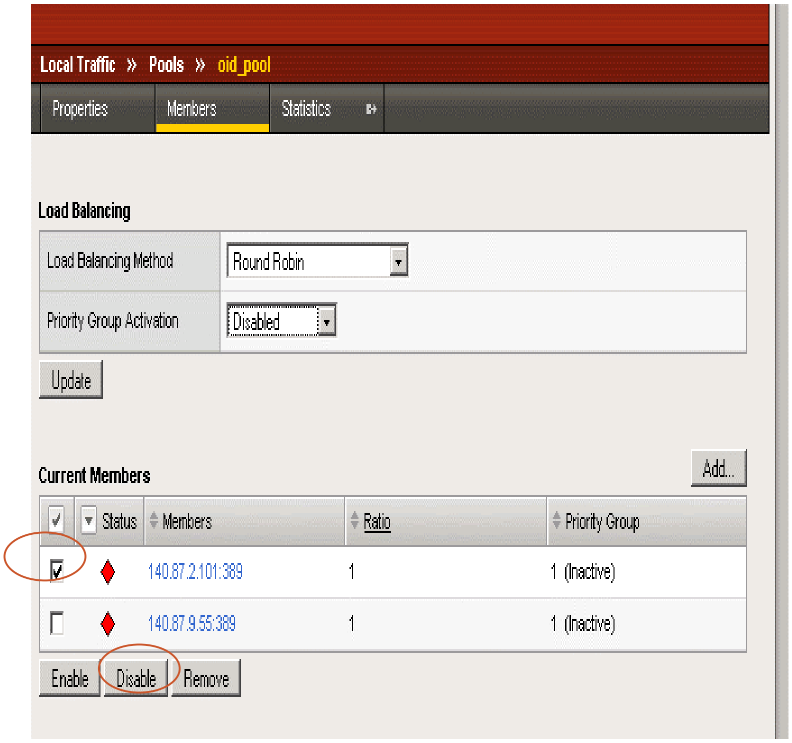
The static ports feature of Oracle Universal Installer (OUI) ensures that the only specific ports will be used for the install. However, for this, these ports must be free on all the relevant nodes. Your planning process should take this into account while deciding the various ports.

Please refer to the Appendix A for the template and sample files that go with the install steps.

Oracle Internet Directory Virtual Server Load Balancer Configuration

A requirement for the OID/DIP install is to point the load balancer to only one OID node during the install. This is because the load balancer must direct traffic to only the first node until all OID nodes are installed.

To disable traffic to non-install node(s), click **Members** and then check the non-install node(s) and "***Disable***" for the non-install OID node oid2.mydomain.com:389 and the SSL node oid2.mydomain.com:636, as illustrated in Figure below.



Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Disabled

Current Members

☑	Status	Members	Ratio	Priority Group
☑	♦	140.87.2.101:389	1	1 (Inactive)
□	♦	140.87.9.55:389	1	1 (Inactive)

Installation Tasks

During the installation one or more installation sessions may be required. In each case, make sure that you start the installation process with the arguments required for it to use the correct staticports.ini file.

Table 14 summarizes the installation step and the command to use to initiate the installation process.

Install Step	Install Command
OID	`./runInstaller`
SSO/DAS	`./runInstaller`

Table 14 Installation Steps and Commands

Post-Installation Tasks

The post-installation tasks described here are relevant only to the BIG-IP Local Traffic Manager usage in this configuration and common to all installations.

Verify Port Settings

After each installation, verify the port settings match your load balancer configuration. To verify, check the `$ORACLE_HOME/install/portlist.ini` file.

Enable Oracle Internet Directory Traffic to Both Nodes

Following the installation of both OID/DIP, enable OID traffic to all nodes. To enable traffic to all node(s), click **Members** and then check the disabled node(s) and "***Enable***" for the disabled OID node oid2.mydomain.com:389 and the SSL node oid2.mydomain.com:636.

Validation Step

Perform the following tasks to validate if the installation was successful:

1. Access http://sso.mydomain.com:7777/oiddas multiple times and validate that everything is working.
2. Access http://sso.mydomain.com:7777/pls/orasso multiple times and validate that everything is working.

Configuring SSL for SSO and DAS

A common security requirement is to SSL encrypt the traffic from the client browser to the load balancer. The load balancer then acts as an SSL accelerator and directs the converted http traffic to the web tier HTTP listener. This provides the required security but does not burden the web tier machines with the overhead of SSL. Out of the box install provides this deployment. Following are the steps to configure the BIG-IP load balancer for this.

Configuration for Load Balancer

For Load Balancer configuration, use the procedure as detailed above.

- Create pool

Pool Name	Pool Members	Monitor
ssossl_pool	sso1.mydomain.com:7777 sso2.mydomain.com:7777	ohs_https

- Create profiles

Profile Name	Parent Profile	Virtual Server
httpssl	clientssl	sso.mydomain.com:7778

- Create virtual servers and associate them with pools

Address	Pool	Profile
sso.mydomain.com:7778	ssossl_pool	ohs_cookie ws_http httpssl

For virtual servers associated with SSL pools, based on the configuration, select appropriate SSL Profile (Client) and SSL Profile (Server).

Client SSL: clientssl is used from Client – [HTTPS] → Load Balancer

Server SSL: serverssl is used from Load Balancer – [HTTPS] → Oracle HTTP Server

Based on the configuration we can select one or both the profiles.

In current configuration,

Client – [HTTPS] → Load Balancer – [HTTP] → Oracle HTTP Server

for the virtual server sso.mydomain.com, we will select SSL Profile (Client) as "httpssl".

- Create monitors and associate them with the pools and/or nodes

Monitor name	**Configuration**
ohs_https	Import Settings from https **Interval:** 30 **Timeout:** 95 **Send String:** GET /sso/status **Receive String:** OC4J_SECURITY is running

Validation Step

Perform the following tasks to validate if the installation was successful:

3. Access https://login.mydomain.com:7778/oiddas multiple times and validate that everything is working.
4. Access https://login.mydomain.com:7778/pls/orasso multiple times and validate that everything is working.

APPENDIX

A. Static Ports

Oracle Access Manager in Active-Active Topology

OID/DIP staticports.ini

```
Oracle Internet Directory port = 389
Oracle Internet Directory (SSL) port = 636
```

OHS for WebPass

```
Oracle HTTP Server port = 7777
```

OHS for WebGate

```
Oracle HTTP Server port = 7778
```

Distributed OracleAS Cluster (Identity Management) Topology

OID/DIP staticports.ini (static_oid.ini)

```
Oracle Internet Directory port = 389
Oracle Internet Directory (SSL) port = 636
```

SSO/DAS staticports.ini (static_sso.ini)

```
Oracle HTTP Server port = 7777
```

B. References

1. *Oracle Application Server Identity Management 10g (10.1.4.0.1) Documentation*
   http://download-west.oracle.com/docs/cd/B28196_01/index.htm

2. *Oracle Application Server Identity Management 10g (10.1.4.0.1) HA Guide*
   http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28186/toc.htm

3. *Oracle Application Server Identity Management 10g (10.1.4.0.1) Enterprise Deployment Guide*
   http://download-west.oracle.com/docs/cd/B28196_01/core.1014/b28184/toc.htm

4. *Oracle Application Server Identity Management 10g (10.1.4.0.1) Install Guide*
   http://download-west.oracle.com/docs/cd/B28196_01/getstart.htm

5. *BIG-IP Reference and Solution Manuals*
   http://www.f5.com/solutions/

C. Add LDAP User

Following script can be used for adding an ldap user:

Create a ldif file as follows:

File: ldapmuser.ldif

```
dn:cn=ldapmuser,cn=users,dc=us,dc=oracle,dc=com
cn:ldapmuser
sn:ldapmuser
userpassword:welcome1
objectclass:top
objectclass:person
objectclass:inetorgperson
```

```
objectclass:organizationalperson
objectclass:orcluser
objectclass:orcluserv2
uid:ldapmuser
title:engineer
```

Execute ‘ldapadd’ command as mentioned below:

```
$ ldapadd -h stbee19 -p 389  -D "cn=orcladmin" -w welcome1 -f a.ldif
```

```
adding new entry cn=ldapmuser,cn=users,dc=us,dc=oracle,dc=com
```

Execute ‘ldapsearch’ command to verify the ldap user you just created. System will list the details.

```
$ ldapsearch -h stbee19 -p 389  "cn=ldapmuser"
```

```
cn=ldapmuser,cn=users,dc=us,dc=oracle,dc=com
cn=ldapmuser
sn=ldapmuser
objectclass=top
objectclass=person
objectclass=inetorgperson
objectclass=organizationalperson
objectclass=orcluser
objectclass=orcluserv2
uid=ldapmuser
title=engineer
```

Validate using ‘ldapbind’ command as follows:

```
$ ldapbind -h stbee19 -p 389  -D "cn=ldapmuser,cn=users,dc=us,dc-oraclec,dc=com" –w welcome1
```

D. OID Connections being disconnected by Load Balancer

Problem

The load balancer or firewall terminates connections to Oracle Internet Directory, and further connections from OC4J to Oracle Internet Directory cannot be made.

Solution

To fix this, set the `orclLDAPConnTimeout` attribute (in the `"cn=dsaconfig, cn=configsets, cn=oracle internet directory"` entry) to a value smaller than the "idle connection timeout" value configured on the load balancer or firewall. This prevents the load balancer or firewall from terminating connections to Oracle Internet Directory.

The `orclLDAPConnTimeout` attribute is expressed in minutes.

Note that in this release and also in the 10.1.2.2.0 patch set, the `orclLDAPConnTimeout` attribute is independent of the `orclStatsPeriodicity` attribute when Oracle Internet Directory calculates the idle time of a connection.

However, in previous releases (releases 9.0.4.2, 9.0.4.3, 10.1.2.0, 10.1.2.0.2, and 10.1.2.1), Oracle Internet Directory takes into account the values for both attributes when it calculates the idle time. For these releases, you need to set the attributes as follows:

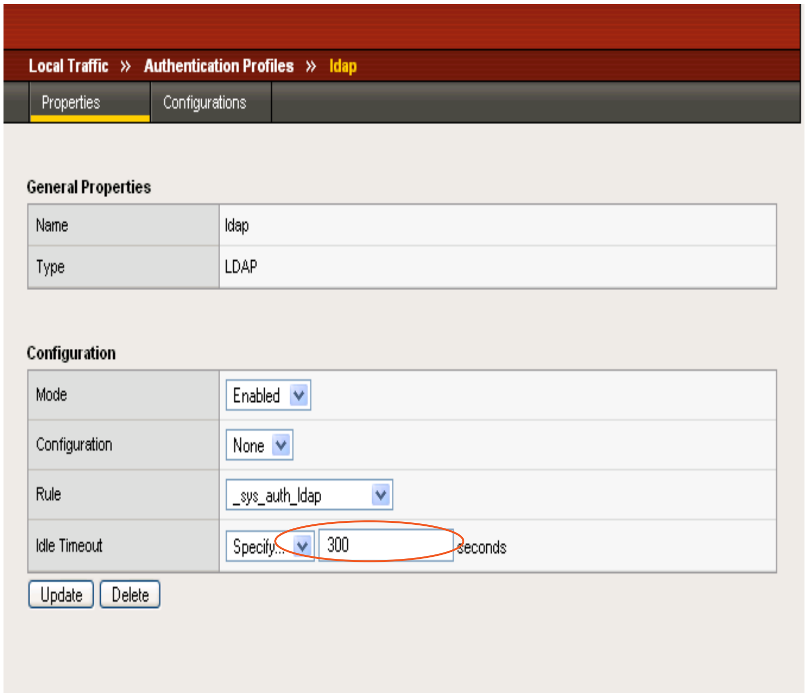
- Set the `orclStatsPeriodicity` attribute to a value less than half of the "idle connection timeout" value configured on the load balancer or firewall.
- Set the `orclLDAPConnTimeout` attribute to a value less than the "idle connection timeout" value configured on the load balancer or firewall.

The attribute values are expressed in minutes.

The values of the `orclStatsFlag` and `orclMaxTcpIdleConnTime` attributes are not used here.

For example, assume that the "idle connection timeout" value on the load balancer or firewall is set at 15. In this case, you can set the `orclStatsPeriodicity` attribute to 7 (which is less than half of 15) and the `orclLDAPConnTimeout` attribute to 12 (which is less than 15).

The `orclLDAPConnTimeout` attribute is in the "`cn=dsaconfig, cn=configsets, cn=oracle internet directory`" entry, while the other attributes are in the root DSE entry.



General Properties

Name	ldap
Type	LDAP

Configuration

Mode	Enabled
Configuration	None
Rule	_sys_auth_ldap
Idle Timeout	Specify... 300 seconds

Configuring Highly Available OracleAS Identity Management with F5 BIG-IP v9 Local Traffic Manager, November 2006
Author: Shashi Mohan, Oracle HA Systems Group; Randy Cleveland, F5 Networks

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
oracle.com