Deployment Guide

Oracle Application Server 10g R2

Deploying the BIG-IP System v11 with Oracle Application Server 10g R2

What's Inside:

Welcome to the F5 and Oracle® Application Server 10g Release 2 (R2) Deployment Guide. When deployed with Oracle AS 10g R2, the BIG-IP system v11 ensures secure, fast and always available access for applications running on Oracle.

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy and accurate way to configure the BIG-IP system for Oracle Application Server 10g.

Oracle AS 10g R2 meets customers' demand for up-to-date business information with reliable, scalable and cost-effective grid computing. With grid computing, organizations can leverage the use of many low-cost, modular servers acting as one computer, making their applications more scalable and less expensive to deploy and manage.

Why F5?

F5's Application Ready Solution for Oracle Application Server 10g R2 provides a unique and comprehensive application delivery platform that helps align IT agility with business agility. F5 greatly enhances the efficiency and productivity of both the Oracle applications and the organizations who rely on these devices. Oracle is one of F5's largest customers, providing application delivery networking to Oracle.com, and all of their internal and external enterprise applications for Oracle employees worldwide.

- F5 WAN optimization technologies can dramatically increase Oracle AS 10g performance across the WAN.
- Extend server capacity by offloading tasks like compression and SSL processing onto F5's unified, simple to manage platform.
- Achieve 20 to 30 times bandwidth reduction for remote office users.
- F5's Oracle AS 10g-specific iApp templates, acceleration and security policies, and step-by-step configuration guidance help dramatically reduce deployment cycles.
- F5 gives peace of mind with comprehensive application-level security.

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com.*

Important: *Make sure you are using the most recent version of this guide, available at http://www.f5.com/pdf/deployment-guides/oracle-as-10g-iapp-dg.pdf.*

Document Version

1.0

Products and versions tested

Product	Version
BIG-IP LTM	v11
Oracle Application Server 10g	10g Release 2 (10.1.2.0.2)

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for Oracle AS 10g acts as the single-point interface for building, managing, and monitoring Oracle AS 10g Portal and SSO.

For more information on iApp, see the *F5 iApp: Moving Application Delivery Beyond the Network* White Paper: *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- The Oracle installation should be running Oracle AS 10g Release 2 (10.1.2.0.2).
- This document is written with the assumption that you are familiar with both F5 devices and Oracle AS 10g. For more information on configuring these devices, consult the appropriate documentation.
- For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.
- This deployment guide provides detailed guidance for using the iApp for Oracle AS 10g found in version 11.0 and later. For advanced users extremely familiar with the BIG-IP, there is a manual configuration table at the end of this guide. However, we strongly recommend using the iApp template.
- If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, and it is installed on the BIG-IP LTM system. When you configure the iApp, you are asked for the SSL Certificate and Key you imported for Oracle AS 10g R2.
- There are important changes for the Oracle configuration, be sure to see *Modifying the Oracle AS 10g R2 configuration on page 13* after running the iApp.
- This deployment guide contains guidance on optional modules, including Application Visibility Reporting, WebAccelerator, and Application Security Manager (ASM). To take advantage of these modules, they must be licensed and provisioned before starting the iApp template. For more information on licensing modules, contact your sales representative. Note that AVR is licensed on all systems, but must be provisioned before beginning the iApp template.

Configuration example

The BIG-IP system provides intelligent traffic management and fail-over for Oracle AS 10g R2 Web and Application servers. Through advanced health checking capabilities, the BIG-IP product recognizes when resources are unavailable or under-performing and directs traffic to another resource.

The BIG-IP product can also track Oracle Application Server 10g R2 end-user sessions, enabling the application server to maintain client session data. The following diagram shows an example deployment with Oracle AS 10g R2 and the BIG-IP system.

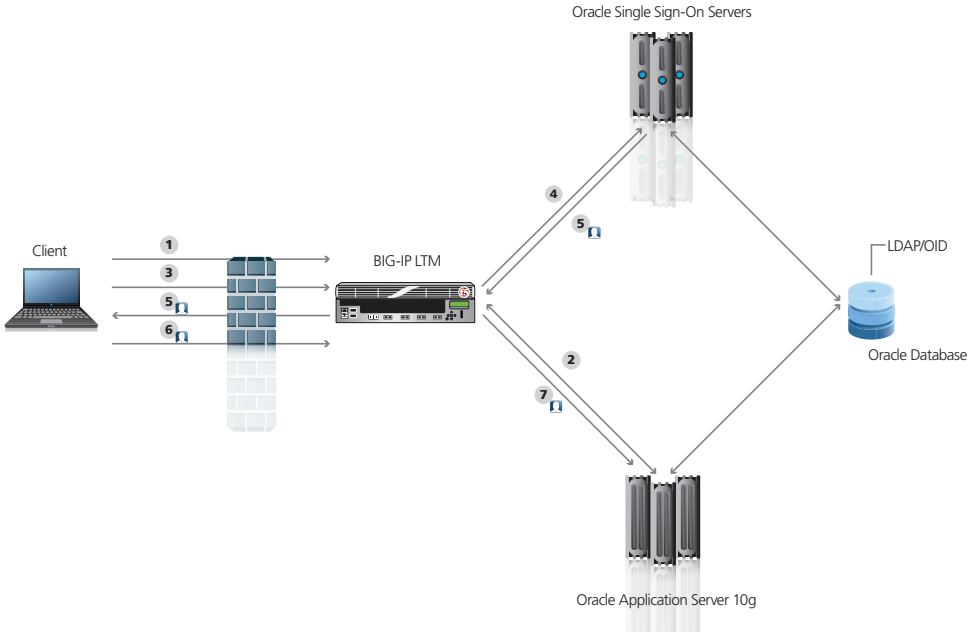


Figure 1: *Logical configuration example*

Traffic Flow:

1. The client machine makes a connection to the LTM virtual server IP of the Application Server to access a resource.
2. The BIG-IP establishes a connection to an Application Server, translating the destination port, based on the selected Load Balancing algorithm. The resource the client has requested requires authentication, so the Application Server redirects the client to log in via SSO (via the BIG-IP).
3. The client machine makes a connection to the LTM virtual server IP of the Oracle AS 10g Server to log on.
4. The BIG-IP establishes a connection to the SSO Server, translating the destination port, to allow the client to proceed with authentication. Depending on the configuration, the BIG-IP may terminate the SSL connection.
5. After successful authentication, the SSO Server redirects the client back to the resource that was originally requested, along with a SSO token to permit access.
6. The client machines makes a connection to the LTM virtual server IP of the Application Server and re-requests the resource.
7. The BIG-IP passes along the SSO token so the Application Server will allow them through. The BIG-IP persists the now authenticated session to the same Application Server while optimizing the connection and providing compression and caching as necessary.

Note: *Although we show space for 7 pool members for each application, you may have more or fewer members in each pool.*

Preparation Worksheets

In order to use the iApp for Oracle AS 10g, you need to gather some information, such as Oracle server IP addresses and domain information. There are two worksheets, one for Oracle AS 10g Portal server, and another if you are using Oracle AS 10g Single Sign-On server. Use these worksheets to gather the information you will need while running the template. The worksheets do not contain every question in the template, but rather include the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages. You might find it useful to print these tables and then enter the information.

Oracle AS 10g Portal Server

IP Addresses/FQDN	SSL Offload	Pool Members	Sync/Failover Groups	TCP request queuing	WAN or LAN clients
IP address for the Oracle Portal LTM virtual server: FQDN that will resolve to the virtual server address:	*Offloading SSL?* Yes | No If offloading SSL, import a certificate and key into the BIG-IP LTM before running the template. Certificate: Key:	Oracle Portal IP addresses: 1: 2: 3: 4: 5: 6: 7: Port used by Oracle Portal:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node. Request queue length: Timeout: Node Connection limit:	Most clients connecting through BIG-IP to Oracle AS 10g are coming over a: LAN WAN
Optional Modules (you must have provisioned modules before running the template)					
Application Visibility Reporting (AVR)		*WebAccelerator*		*Application Security Manager (ASM)*	
If using AVR, we strongly recommend you first create an custom Analytics profile before running the template. Analytics profile name:		All FQDNs for Oracle AS 10g: 1: 2: 3:		Language encoding the application uses (the default is Unicode (utf-8):	

Oracle AS 10g Single Sign-On Server

IP Addresses/FQDN	SSL Offload	Pool Members	Sync/Failover Groups	TCP request queuing	WAN or LAN clients
IP address for the Oracle SSO LTM virtual server: FQDN that will resolve to the virtual server address:	*Offloading SSL?* Yes | No If offloading SSL, import a certificate and key into the BIG-IP LTM before running the template. Certificate: Key:	Oracle SSO IP addresses: 1: 2: 3: 4: 5: 6: 7: Port used by Oracle SSO:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node. Request queue length: Timeout: Node Connection limit:	Most clients connecting through BIG-IP to Oracle AS 10g are coming over a: LAN WAN
Optional Modules (you must have provisioned modules before running the template)					
Application Visibility Reporting (AVR)		*WebAccelerator*		*Application Security Manager (ASM)*	
If using AVR, we strongly recommend you first create an custom Analytics profile before running the template. Analytics profile name:		All FQDNs for Oracle SSO: 1: 2: 3:		Language encoding the application uses (the default is Unicode (utf-8):	

Configuring the BIG-IP iApp for Oracle AS 10g

Use the following guidance to help you configure the BIG-IP system for Oracle AS 10g using the BIG-IP iApp template.

Getting Started with the iApp for Oracle AS 10g

To begin the Oracle AS 10g Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **Oracle-10g_**.
5. From the **Template** list, select **f5.oracle_as_10g**.
   The Oracle Application Server 10g template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. If you enable sync and failover, you can select a device group that synchronizes BIG-IP configuration data among devices and a traffic group of related objects that fail over to another device if the current device becomes unavailable.

Important → *If you plan on using Device and Traffic Groups with the iApp for Oracle AS 10g R2, you must have configured the Device Group and Traffic Group before beginning the iApp. For more information on Device Management, see the Online help or product documentation.*

1. **Configure Device and Traffic Groups?**
   If you want to configure the Application for Device and Traffic groups, select **Advanced** from the **Template Selection** list.
   a. **Device Group**
      If you select Advanced from the list, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.
   b. **Traffic Group**
      If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

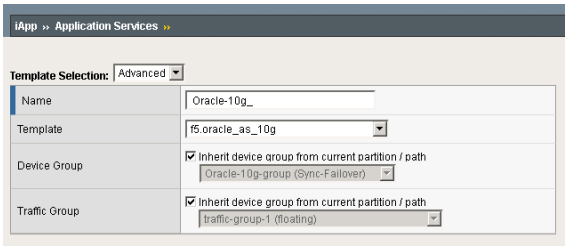


Figure 2: *Oracle AS 10g R2 iApp Advanced options*

Tip
If using AVR, create a new Analytics profile before beginning the iApp for more specific reporting

Analytics

This section of the template asks questions about Analytics. The Application Visibility Reporting (AVR) module allows you to view statistics specific to your Oracle AS 10g implementation. AVR is available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. Note that these are only for application visibility reporting, you can view object-level statistics from the BIG-IP without provisioning AVR.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile before beginning the template. To create a new profile, from the Main tab, select Profiles and then click Analytics. Click New and then configure the profile as applicable for your configuration. See the online help or product documentation for specific instructions.

1. **Enable Analytics**
   Choose whether you want to enable AVR for Analytics.
2. **Analytics Profile**
   You must decide whether to use the default Analytics profile, or create a new one. As mentioned previously, we recommend creating a new profile to get the most flexibility and functionality out of AVR. If you choose to create a new profile after starting the template, you must exit the template, create the profile, and then restart the template.

   To use the default Analytics profile, choose Use **Default Profile** from the list.

   To choose a custom profile, leave the list set to **Select a Custom Profile**, and then from the Analytics profile list, select the custom profile you created.

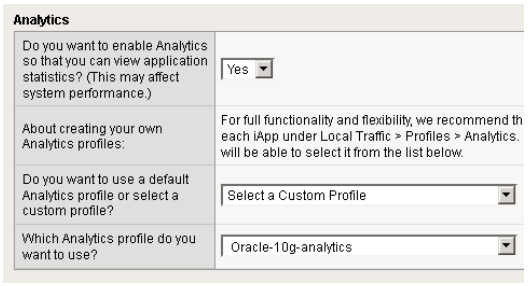


Figure 3: *Analytics options*

Oracle AS 10g Portal Pool, Load Balancing, and Service Monitor questions

The next section of the template asks questions about the Oracle AS 10g Portal configuration.

1. **SSL Offload**
   Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

   For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the ***Configuration Guide for BIG-IP Local Traffic Manager*** *available at http://support.f5.com/kb/en-us.html.*

   To configure the BIG-IP to offload SSL, select **Yes** *from the list.*

   a. **Certificate**
      Select the certificate for you imported for Oracle Portal from the certificate list.

   b. **Key**
      Select the associated key from the list.

2. **IP address for the virtual server**
   This is the address clients use to access Oracle Portal (or a FQDN will resolve to this address).

3. **Routes or secure network address translation**
   If the Oracle Portal servers do not have a route back for clients through the BIG-IP, (i.e. if they do not use the BIG-IP as the default gateway), the BIG-IP uses Secure Network Address Translation (SNAT) Automap (one exception, see #4) to translate the client's source address to an address configured on the BIG-IP.

   If you indicate that the Oracle Portal servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the Portal servers.

   We recommend choosing **No** from the list because it does not require you to configure routing manually.

   If you are configuring your BIG-IP LTM in a "one-armed" configuration with your Oracle Portal servers -- where the BIG-IP virtual server(s) and the Portal server have IP addresses on the same subnet – you must choose No.

   If you do select Yes from the list, the following question about 64,000 connections does not appear.

4. **More than 64,000 simultaneous connections**
   If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #5.

   If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat with an additional IP address for each multiple of 64,000 simultaneous connections.

5. **New Pool**
   Choose **Create New Pool** unless you have already made a pool on the LTM for the Oracle Portal devices.

6. **Load balancing method**
   While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

7. **Address/Port**
   Type the IP Address and Port for each Oracle AS 10g Portal server. The default port for Oracle AS 10g is **7778**, so you must change the port box from 80. You can optionally add a Connection Limit. Click **Add** to include additional servers to the pool.

8. **TCP Request Queuing**
   TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *New Features Guide for BIG-IP Version 11*, available on Ask F5.

   If you want the BIG-IP to queue TCP requests, select Yes from the list. Additional options appear.

   a. Type a queue length in the box.

   b. Type a number of milliseconds for the timeout value.

➲ **Important**
If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port

9. **Health Monitor**
   Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the Oracle Portal devices.
10. **Interval**
    Specifies how often the system checks the health of the servers. We recommend the default of 30 seconds.
11. **HTTP Request**
    This is optional. You can configure the template to retrieve a specific page by typing the path. Leaving the default (GET /) marks the node up if anything is returned from the web page.
12. **HTTP version**
    Unless the majority of your users are using HTTP 1.0, we recommend selecting **Version 1.1** from the list.
    - FQDN: When you select Version 1.1, a new row appears asking for the FQDN the clients use to access Oracle AS 10g Portal. Type it here.
13. **Monitor response string**
    Optional. If you configured a unique HTTP Request, type the expected response.

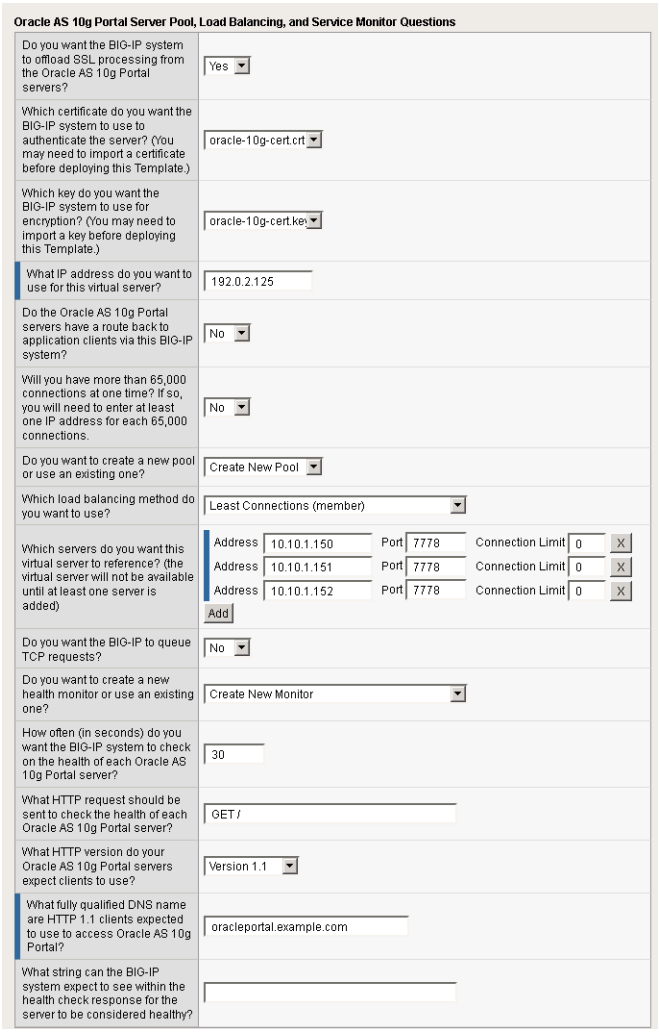


Figure 4: *Portal Server Pool options*

Oracle AS 10g Single Sign-On Pool, Load Balancing, and Service Monitor questions

The next section of the template asks questions about the Oracle AS 10g Single Sign-On configuration. If you are not deploying Oracle AS 10g Single Sign-On, continue with *Protocol Optimization and Security Questions on page 11*.

1. **Deploying Single Sign-On?**
   If you are using Oracle AS 10g Single Sign-On, select **Yes** from the list. The Single Sign-On questions appear.
   If you are not using Single Sign-On, leave the list at **No** and continue with the following section.

2. **SSL Offload**
   Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

   For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the ***Configuration Guide for BIG-IP Local Traffic Manager*** *available at http://support.f5.com/kb/en-us.html*.

   To configure the BIG-IP to offload SSL, select **Yes** *from the list.*

   a. **Certificate**
      Select the certificate for you imported for Oracle SSO from the certificate list.

   b. **Key**
      Select the associated key from the list.

3. **IP address for the virtual server**
   This is the address clients use to access Oracle SSO (or a FQDN will resolve to this address).

4. **Routes or secure network address translation**
   If the Oracle SSO servers do not have a route back for clients through the BIG-IP, (i.e. if they do not use the BIG-IP as the default gateway), the BIG-IP uses Secure Network Address Translation (SNAT) Automap (one exception, see #5) to translate the client's source address to an address configured on the BIG-IP.

   If you indicate that the Oracle SSO servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the Portal servers.

   We recommend choosing **No** from the list because it does not require you to configure routing manually.

   If you are configuring your BIG-IP LTM in a "one-armed" configuration with your Oracle SSO servers -- where the BIG-IP virtual server(s) and the SSO server have IP addresses on the same subnet – you must choose No.

   If you do select Yes from the list, the following question about 64,000 connections does not appear.

5. **More than 64,000 simultaneous connections**
   If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #6.

   If you have a very large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need

one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat with an additional IP address for each multiple of 64,000 simultaneous connections.

6. **New Pool**
   Choose **Create New Pool** unless you have already made a pool on the LTM for the Oracle SSO devices.
7. **Load balancing method**
   While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.
8. **Address/Port**
   Type the IP Address and Port for each Oracle AS 10g SSO server. The default port for Oracle AS 10g is **7778**, so you must change the port box from 443. You can optionally add a Connection Limit. Click **Add** to add additional servers to the pool.
9. **TCP Request Queuing**
   TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *New Features Guide for BIG-IP Version 11*, available on Ask F5.

   If you want the BIG-IP to queue TCP requests, select Yes from the list. Additional options appear.

   a. Type a queue length in the box. Leave the default of 0 for unlimited.

   b. Type a number of milliseconds for the timeout value.

10. **Health Monitor**
    Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the Oracle SSO devices.
11. **Interval**
    Specifies how often the system checks the health of the servers. We recommend the default of 30 seconds.
12. **HTTP Request**
    This is optional. You can configure the template to retrieve a specific page by typing the path. Leaving the default (GET /) marks the node up if anything is returned from the web page.
13. **HTTP version**
    Unless the majority of your users are using HTTP 1.0, we recommend selecting **Version 1.1** from the list.

    - FQDN: When you select Version 1.1, a new row appears asking for the FQDN the clients use to access Oracle SSO. Type it here.

14. **Monitor response string**
    Optional. If you configured a unique HTTP Request, this is where you enter the expected response.

➲ **Important**
If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port

Protocol Optimization and Security Questions

In this section, you configure security and protocol optimizations for Oracle AS 10g.

1. **WAN or LAN**
   Specify whether most clients are connecting over a WAN or LAN. Because most Oracle AS 10g clients are likely to be coming over the WAN, we recommend selecting WAN (the default).

2. **WebAccelerator**
   If you have licensed and provisioned the WebAccelerator module, you have the option of using it for Oracle AS 10g. The WebAccelerator provides application acceleration for remote users.

   a. *DNS names*
   If you select Yes, an additional row appears in the template asking for the fully qualified domain names used for Oracle AS 10g. The BIG-IP system uses these entries for the Requested Hosts field, allowing the WebAccelerator module to accelerate the traffic to these virtual hosts.

   In the **Host** box, type the **FQDN**. If you have additional FQDNs, click the **Add** button.

   b. *X-WA-info Header*
   By default, the WebAccelerator X-WA-info header is not included in the response from the BIG-IP. This header is useful for debugging WebAccelerator behavior. There are two additional options:
   - Standard: If you choose Standard, the BIG-IP inserts a HTTP header that includes numeric codes which indicate if and how each object was cached.
   - Debug: If you choose Debug, the BIG-IP includes extended information which may help for extended troubleshooting.

   c. *WebAccelerator Performance monitor*
   While the BIG-IP Dashboard provides statistics and performance graphs related to WebAccelerator, you can choose to enable the WebAccelerator performance monitor for legacy WebAccelerator performance monitoring for debugging purposes. The results can be found in the Main tab of the navigation page, under WebAccelerator, by clicking Traffic Reports.
   In our example, we leave the performance monitor **Disabled**.

   d. *WebAccelerator policy*
   For this template, F5 recommends the **Oracle AS 10g Portal** policy to achieve the best results for Web acceleration of Oracle traffic. Should F5 publish an updated policy to DevCentral that you have downloaded and imported, or if a custom policy is created for your environment (locally), you can select that custom policy from the list. In our example, we leave the default, **Oracle AS 10g Portal**.

3. **Application Security Manager**
   If you have licensed and provisioned the Application Security Manager (ASM), you have the option of using it to protect Oracle AS 10g. The ASM module is an advanced web application firewall that significantly reduces and mitigates the risk of loss or damage to data, intellectual property, and web applications.

Important → *If you choose to use ASM, the iApp template sets the policy enforcement mode to transparent. In this mode, violations are logged but not blocked. Before changing the mode to blocking, review the log results and adjust the policy for your deployment if necessary.*

a. If you select Yes, an additional row appears asking for the language encoding. Select the proper language from the list.

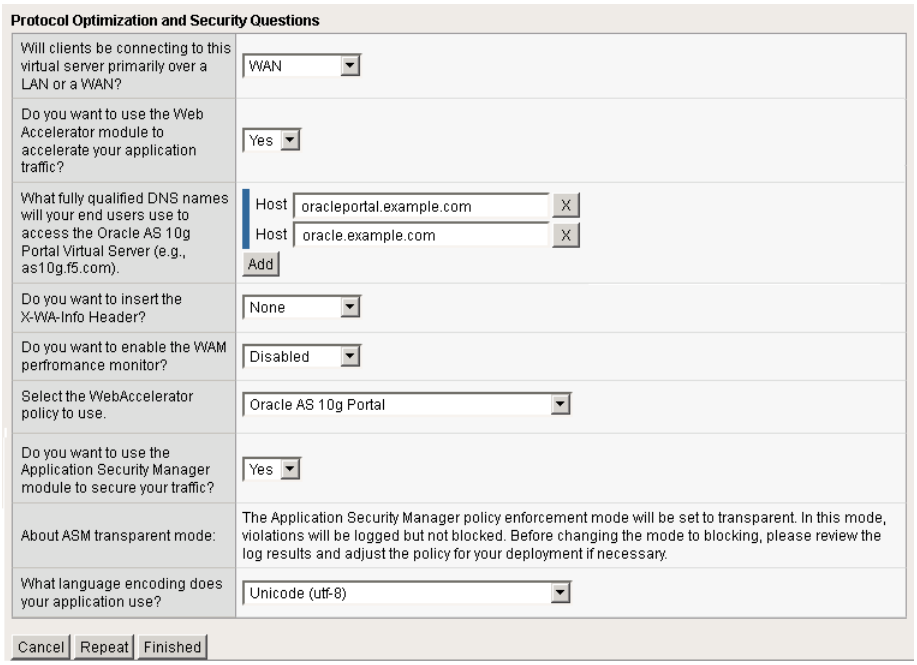


Figure 5: *Protocol and Security Questions*

Finished

Review your answers to the questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Be sure to continue to the following section, *Modifying the Oracle AS 10g R2 configuration on page 13*.

When you are finished with the Oracle modifications, see *Next Steps on page 21* for more information.

Modifying the Oracle AS 10g R2 configuration

With the BIG-IP LTM configuration complete, there are now modifications to the Oracle AS 10g R2 configuration that need to be made in order for traffic to resolve and flow properly.

Modifying the Oracle Portal configuration

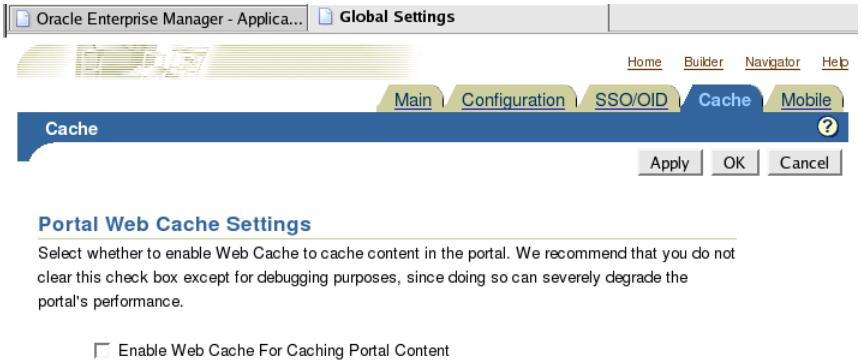
The first task is to modify the Oracle AS 10g R2 Portal configuration. You must perform the following four procedures on each Oracle AS 10g R2 Portal server.

Disabling Web Cache

Because the caching duties in this configuration are handled by the BIG-IP LTM system, we disable the Oracle AS 10g R2 Web Cache. This frees the servers you would normally use for the Web Cache devices to run other Oracle applications.

To disable the Oracle Web Cache

1. Log on to your Oracle Application Server Portal GUI as an administrator.
2. Click the *Administer* tab.
3. Under the Services portlet, click **Global Settings**.
4. Click the *Cache* tab.
5. Clear the **Enable Web Cache For Caching Portal Content** box to disable the Web Cache.
6. Click the **Apply** button.

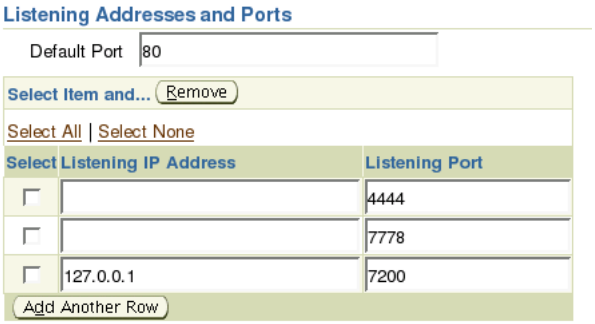


Changing the default port

The next step is to change the default port for the Oracle AS 10g R2 Portal server to 80. If you are using the BIG-IP LTM to offload SSL traffic, change the default port to 443.

To change the default port

1. Log on to your Oracle Application Server Portal GUI through Enterprise Manager as an administrator.
2. Under System Components, click **HTTP Server**.
3. Click the *Administration* Tab.
4. Click the **Server Properties** link.
5. In the **Listening Addresses and Ports** section, change the default port to **80**. If you are using the BIG-IP LTM for SSL offload, change the port to **443**.



6. Click the **Apply** button
7. At the prompt, click to restart the service.

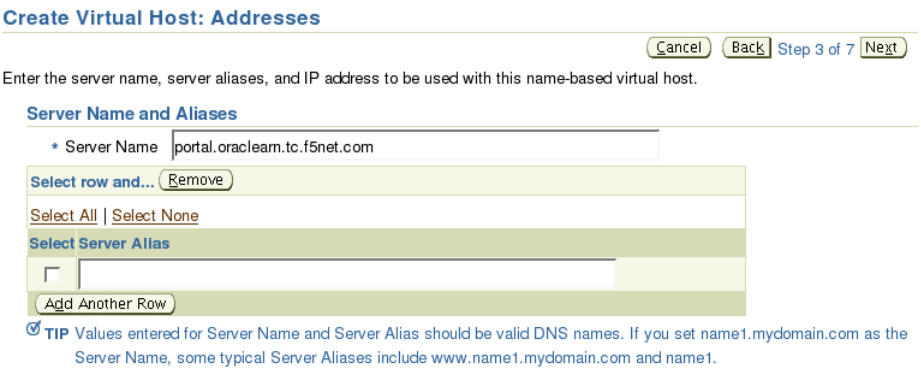
Adding the virtual host entry for the BIG-IP LTM virtual server

The next step is to add a virtual host entry on the Oracle device for the BIG-IP LTM virtual server. This ensures that traffic is properly routed to the BIG-IP LTM system.

To add a virtual host entry

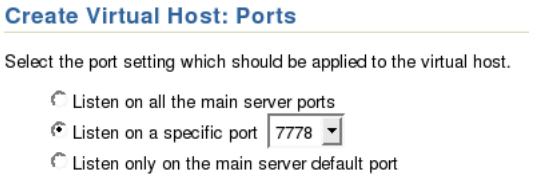
1. Log on to your Oracle Application Server Portal GUI through Enterprise Manager as an administrator.
   (If you are already logged in, return to the **HTTP Server** page).
2. Under System Components, click **HTTP Server**.
3. Click the *Virtual Hosts* tab.
4. Click the **Create** button. The Create Virtual Host wizard opens.
   a. In Step One of the virtual Host wizard, click **Next**.
   b. In Step 2, make sure that the Virtual Host is set to **Name-based** (this is the default setting).
   c. In Step 3, in the **Server Name** box, type the DNS name that resolves to the Oracle AS 10g R2 Portal virtual server on the BIG-IP LTM system, and then click the **Next** button.

Important → *This is not the name of the virtual server itself, it is the name that resolves to the virtual server in DNS; check with your DNS administrator.*



   d. In Step 4, make sure that **Listen on a specific port** is selected. From the list, select

7778. Click the **Next** button.



e. In Step 6 (Step 5 does not appear), click **Next**.

f. In Step 7, click **Finish**.

5. Restart the service by clicking **Yes** at the prompt.

Making sure the server responds on port 80

The next step is to configure the Oracle HTTP Server (OHS) so that it returns the correct URLs to the user on port 80. If you are using the BIG-IP LTM for SSL offload of the Portal servers, this is port 443.

This procedure must be performed from the command line.

To configure the Oracle service to respond on port 80

1. Log on to the Oracle AS 10g R2 Portal Server from the command line as the Oracle user.
2. Open the **httpd.conf** file (**$ORACLE_HOME/Apache/Apache/conf/httpd.conf**) in a text editor, such as VI or PICO.
3. Find the **Virtual Host** entry at the bottom of the file.
4. Create a Port Directive for the virtual host by adding Port 80 to the entry (port 443 if the BIG-IP LTM system is offloading SSL from the Portal devices). Add the following:

   ```
   Port 80
   ```

   The entry should look like the following when you are finished:

   ```
   <VirtualHost *:7778>
       ServerName portal.oraclearn.tc.f5net.com
       Port 80
   </VirtualHost>
   ```

   Note that the **ServerName** example above will be different in your deployment.

5. ***Optional***: If you are using the BIG-IP LTM system to offload SSL from the Oracle AS 10g R2 Portal device, you need to add another line immediately following the line you just entered:

   ```
   SimulateHttps on
   ```

   So the final result of the Virtual Host entry for offloading SSL should look like:

   ```
   <VirtualHost *:7778>
       ServerName portal.oraclearn.tc.f5net.com
       Port 443
       SimulateHttps on
   </VirtualHost>
   ```

You must also add the following LoadModule line at the end of the LoadModule entries in the httpd.conf file:

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

6. Save and close the **httpd.conf** file.
7. Restart your web server. For simplicity, we recommend you restart the web server through the Oracle Enterprise Manager.

You must repeat all of these procedures for each Oracle AS 10g R2 Portal server in your configuration. Return to Modifying the Oracle AS 10g R2 Portal configuration, on page 10 to start again.

There is an additional procedure necessary if you are using the BIG-IP LTM for offloading SSL from the Oracle AS 10g R2 Portal devices, after completing the following section for Oracle Single Sign-On.

Modifying the Oracle AS 10g R2 Single Sign-On configuration

In the following procedures, we configure the Oracle AS 10g R2 SSO service to use the BIG-IP LTM system.

Deleting the SSO Partner Application

The first procedure in this configuration is to delete the SSO Partner Application, before adding it back. It is necessary to delete the SSO Partner application because the Site ID field is not editable, and the login URL will change.

To delete the SSO Partner Application

1. Log on to the Oracle AS 10g R2 Single Sign-On Server as an administrator.
2. Click the **Single Sign-On Server Administration** link.
3. Click the **Administer Partner Applications** link.
4. In the **Edit/Delete Partner Application** section, click the **Delete** button for the SSO Partner Application (**SSO Server (orasso)**.
5. On the Delete Partner Application confirmation page, click **OK**.

Configuring a new Single Sign-On URL for partner applications

The next step is to configure a new Single Sign-On URL for partner applications. This procedure requires a manual command line entry on Single Sign-On server.

The following procedure is also a manual command line entry, so you can remain logged on to the command line after you complete this procedure.

To configure a new Single Sign-On URL

1. Log on to the Oracle Single Sign-On device from the command line as the Oracle user.
2. Type the following command to change directories:

   ```
   cd $ORACLE_HOME/sso/bin
   ```

3. Use the following syntax to create the new URL:

   ```
   ./ssocfg.sh https <DNS name of LTM SSO virtual server> 443
   ```

   For example:

   ```
   ./ssocfg.sh https login.oraclearn.tc.f5net.com 443
   ```

Registering the SSO server as a Partner Application

The next step is to register the Single Sign-On server as a Partner Application. This procedure also requires a manual command line entry on Single Sign-On server. If you are already logged on from the previous procedure, you can skip to Step 3.

For more information on this command, see Oracle MetaLink article ID#315053.1

To register the SSO server as a partner application

1. Log on to the Oracle Single Sign-On device from the command line as the Oracle user.
2. Type the following command to change directories:

   ```
   cd $ORACLE_HOME/sso/bin
   ```

3. Use the following syntax to create the new URL:

   ```
   ./ssoreg.sh -site_name 'SSO Server orasso' -mod_osso_url <DNS name of LTM SSO
   virtual server> -config_mod_osso TRUE -oracle_home_path $ORACLE_HOME -config_
   file $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf -admin_info 'cn=orcladmin'
   -virtualhost
   ```

   For example:

   ```
   ./ssoreg.sh -site_name 'SSO Server orasso' -mod_osso_url https://login.oraclearn.
   tc.f5net.com -config_mod_osso TRUE -oracle_home_path $ORACLE_HOME -config_
   file $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf -admin_info 'cn=orcladmin'
   -virtualhost
   ```

Changing the default port to port 443

The next procedure is to change the default port of the Single Sign-On Server to port 443. For more information on this procedure, see Oracle MetaLink ID #315200.1.

To change the default port

1. Log on to your Oracle Application Server SSO Infrastructure GUI through Enterprise Manager as an administrator.
2. Under System Components, click **HTTP Server**.
3. Click the *Administration* Tab.
4. Click the **Server Properties** link.
5. In the Listening Addresses and Ports section, change the default port to **443**.
6. Click the **Apply** button
7. At the prompt, click to restart the service.

Adding the virtual host entry for the BIG-IP LTM virtual server

The next step is to add a virtual host entry on the Oracle device for the BIG-IP LTM virtual server.

To add a virtual host entry

1. Log on to your Oracle SSO GUI through Enterprise Manager as an administrator.
   If you are already logged in, return to the HTTP Server page.
2. Under System Components, click **HTTP Server**.
3. Click the *Virtual Hosts* tab.
4. Click the **Create** button. The Create Virtual Host wizard opens.

a. In Step One of the virtual Host wizard, click **Next**.

b. In Step 2, make sure that the Virtual Host is set to **name-based** (this is the default setting).

c. In Step 3, in the **Server Name** box, type the DNS name that resolves to the virtual server on the BIG-IP LTM system for Single Sign-On.

d. In Step 4, make sure that **Listen on specific port** is selected. From the list, select **7777**.

e. In Step 6 (Step 5 does not appear), click **Next**.

f. In Step 7, click **Finish**.

5. Restart the service by clicking Yes at the prompt.

Making sure the server responds on port 443

The next step is to configure the Oracle AS 10g R2 SSO device to respond on port 443. If you do not make this change, the URLs will retain the original port (such as 7777).

This procedure must be performed from the command line.

To configure the Oracle service to respond on port 443

1. Log on to the Oracle device from the command line as an administrator.
2. Open the httpd.conf file (**$ORACLE_HOME/Apache/Apache/conf/httpd.conf**) in a text editor, such as VI or PICO.
3. Find the end of the LoadModule entries, and add the following line:

   ```
   LoadModule certheaders_module libexec/mod_certheaders.so
   ```

   We load this file in order for the SimulateHttps on directive to work in the VirtualHost directive in the following step.
4. Find the Virtual Host entry at the bottom of the file, and add the following lines to the Virtual Host entry:

   ```
   Port 443

   SimulateHttps on
   ```

   So the final result if you are offloading SSL should look like:

   ```
   <VirtualHost *:7777>

       ServerName login.oraclearn.tc.f5net.com

       Port 443

       SimulateHttps on

   </VirtualHost>
   ```
5. Save and close the **httpd.conf** file.
6. Restart your web server. We recommend you restart the web server through the Oracle Enterprise Manager

Configuring the SSO URL for Oracle DAS

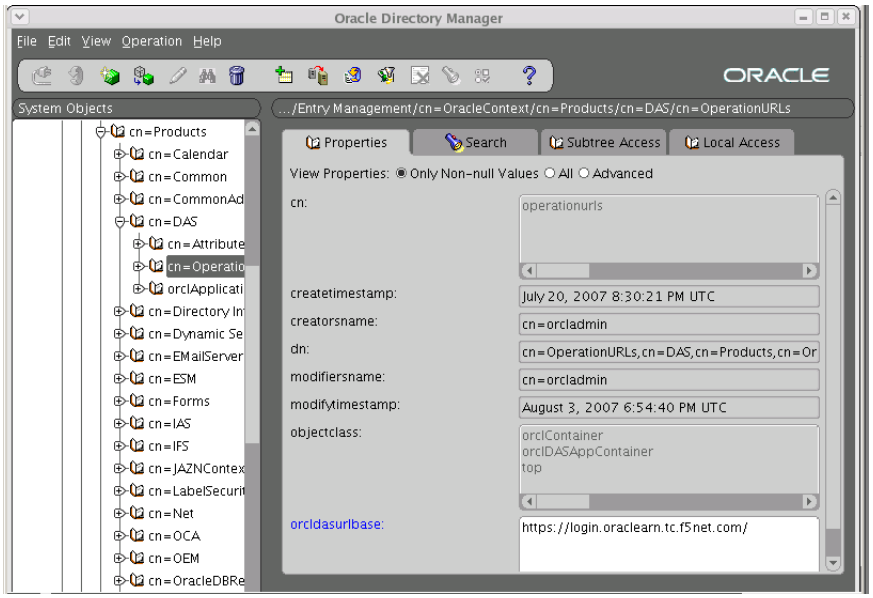
In this section, we configure the new SSO url for Oracle Directory Administration Server (DAS). You can find more information on this procedure in Oracle Metalink Article ID#302634.1

To configure the SSL URL for Oracle DAS

1. Login to Oracle Directory Manager (OID console).
2. Navigate to the following directory:

```
Oracle Internet Directory Servers
  cn=orcladmin@OID_hostname:OID_port
    Entry Management
      cn=OracleContext
        cn=Products
          cn=DAS
            cn=OperationalURLs
```

3. Under the property **orcldasurlbase**, replace the URL with the name that resolves to the SSO virtual server on the BIG-LTM in DNS.
4. Click **Apply**.
5. Restart the Single Sign-On server.



Configuring Oracle AS 10g R2 Portal to use the new SSO URL

Now that we have successfully configured Oracle AS 10g R2 Portal and Single Sign-On with URLs that are direct traffic through the BIG-IP LTM system, we need to configure the Oracle AS 10g R2 Portal servers to use the new SSL-enabled SSO URL (the name that resolves to the SSO virtual server on the BIG-LTM in DNS).

To add the SSO URL to the 10g R2 Portal configuration

1. Log on to your Oracle Single Sign-On server, using the new Single Sign-On URL (the URL that resolves to the SSO virtual server on the BIG-IP LTM.

2. Click the **Single Sign-On Server Administration** link.
3. Click the **Administer Partner Applications** link.
4. In the Edit/Delete Partner Application section, click the **Delete** button for the Portal Partner Application (**Oracle Portal (portal)**).
5. On the Delete Partner Application confirmation page, click **OK**.

Registering the Portal server as a Partner Application

The final procedure is to (re)register the Portal server as a Partner Application. This procedure also requires a manual command line entry on Single Sign-On server. If you are already logged on from the previous procedure, you can skip to Step 3.

To register the Portal server as a Partner Application

1. Log on to the Oracle Single Sign-On device from the command line as an administrator.
2. Type the following command to change directories:

   ```
   cd $ORACLE_HOME/portal/conf
   ```

3. Use the following syntax to create the new URL:

```
./ptlconfig -dad portal -sso -host <DNS name of BIG-IP LTM Portal virtual server> -port 80
```

   For example:

   ```
   ./ptlconfig -dad portal -sso -host portal.oraclearn.tc.f5net.com -port 80
   ```

4. *Optional*: If you configured the BIG-IP LTM system to offload SSL from the Portal devices, the port in the preceding command would be 443. For example:

   ```
   ./ptlconfig -dad portal -sso -host portal.oraclearn.tc.f5net.com -port 443
   ```

After completing the Oracle AS 10g R2 modifications, log on to Enterprise Manager for the Oracle AS 10g R2 Portal and restart all services. You must restart each Portal server, however you only need to run this command on one server.

Next Steps

After completing the iApp Template, the BIG-IP Application Services page opens for the Oracle AS 10g service you just created. To see the list of all the configuration objects created to support Oracle AS 10g, on the Menu bar, click **Components**. The complete list of all Oracle AS 10g related objects opens. You can click individual objects to see the settings. Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the Oracle AS 10g implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). As a safer option, the iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Oracle AS 10g Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the Oracle AS 10g configuration objects created by the iApp template. You can get statistics specific to the Application Service if you have provisioned AVR. Otherwise, you can always get object-level statistics.

AVR statistics
If you have provisioned AVR, you can get application-level statistics for your Oracle AS 10g application service.

To view AVR statistics

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the Application Service List, click the Oracle AS 10g service you just created.
3. On the Menu bar, click **Analytics**.
4. Use the tabs and the Menu bar to view different statistics for your Oracle AS 10g iApp.

Object-level statistics
If you haven't provisioned AVR, or want to view object-level statistics, use the following procedure.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Appendix: Manual configuration tables

We strongly recommend using the iApp template to configure the BIG-IP LTM for Oracle AS 10g. Advanced users extremely familiar with the BIG-IP system can use the following tables to manually configure the BIG-IP system.

These tables contain a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the tables can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

Oracle Application Server 10g Portal

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the 10g Portal nodes	
	Service Port	**7778** (click **Add** to repeat Address and Port for all nodes)	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Rewrite Redirect[2]	**Matching**[2]
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Persistence (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Cookie**
	OneConnect (*Profiles-->Other*)	Name	Type a unique name
		Parent Profile	**oneconnect**
	Client SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Web Acceleration (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**optimized-caching**
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
		Content List -->Include List *(Add each entry to the Content Type box and then click Include)*	application/vnd.ms-publisher
			application/(xls|excel|msexcel|ms-excel|x-excel|x-xls|xmsexcel|x-ms-excel|vnd.excel|vnd.msexcel|vnd.ms-excel)
			application/(word|doc|msword|winword|ms-word|x-word|x-msword|vnd.word|vnd.msword|vnd.ms-word)
			application/(xml|x-javascript|javascript|x-ecmascript|ecmascript)
			application/(powerpoint|mspowerpoint|ms-powerpoint|x-powerpoint|x-mspowerpoint|vnd.powerpoint|vnd.mspowerpoint |vnd.ms-powerpoint|vnd.ms-pps)
			application/(mpp|msproject|x-msproject|x-ms-project|vnd.ms-project)
			application/(visio|x-visio|vnd.visio|vsd|x-vsd|x-vsd)
			application/(pdf|x-pdf|acrobat|vnd.pdf)

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *Only required if offloading SSL on the BIG-IP LTM*

Oracle AS 10g Portal configuration table, continued

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**HTTP**	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	Protocol Profile (client)[1,2]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1,2]	Select the LAN optimized TCP profile you created above
	HTTP Profile[2]	Select the HTTP profile you created above
	Web Acceleration profile[2]	Select the Web Acceleration profile you created above
	HTTP Compression profile[2]	Select the HTTP Compression profile you created above
	OneConnect[2]	Select the OneConnect profile you created above
	SNAT Pool[3]	**Automap** (optional; see footnote [3])
	Default Pool[2]	Select the pool you created above
	Persistence Profile[2]	Select the Persistence profile you created
	iRule[4]	If offloading SSL only: Enable the built-in **_sys_https_redirect irule**
	HTTPS[5]	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	Web Acceleration profile	Select the Web Acceleration profile you created above
	HTTP Compression profile	Select the HTTP Compression profile you created above
	OneConnect	Select the OneConnect profile you created above
	SSL Profile (client)	Select the Client SSL profile you created above
	SNAT Pool[2]	**Automap** (optional; see footnote [3])
	Default Pool	Select the pool you created above
	Persistence Profile	Select the Persistence profile you created

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server, and only requires a name, IP address, Port, and the redirect iRule.*

[3] *If want to use SNAT, and you have a large Oracle deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

[4] *Only enable this iRule if offloading SSL*

[5] *Only create this virtual server if offloading SSL*

Oracle AS 10g Single Sign On configuration table

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the 10g SSO nodes	
	Service Port	**7778** (click **Add** to repeat Address and Port for all nodes)	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Rewrite Redirect[2]	**Matching**[2]
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Persistence (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Cookie**
	OneConnect (*Profiles-->Other*)	Name	Type a unique name
		Parent Profile	**oneconnect**
	Client SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Web Acceleration (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**optimized-caching**
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
		Content List -->Include List *(Add each entry to the Content Type box and then click Include)*	application/vnd.ms-publisher
			application/(xls|excel|msexcel|ms-excel|x-excel|x-xls|xmsexcel|x-ms-excel|vnd.excel|vnd.msexcel|vnd.ms-excel)
			application/(word|doc|msword|winword|ms-word|x-word|x-msword|vnd.word|vnd.msword|vnd.ms-word)
			application/(xml|x-javascript|javascript|x-ecmascript|ecmascript)
			application/(powerpoint|mspowerpoint|ms-powerpoint|x-powerpoint|x-mspowerpoint|vnd.powerpoint|vnd.mspowerpoint |vnd.ms-powerpoint|vnd.ms-pps)
			application/(mpp|msproject|x-msproject|x-ms-project|vnd.ms-project)
			application/(visio|x-visio|vnd.visio|vsd|x-vsd|x-vsd)
			application/(pdf|x-pdf|acrobat|vnd.pdf)

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *Only required if offloading SSL on the BIG-IP LTM*

Oracle AS 10g SSO configuration table, continued

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**HTTP**	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	Protocol Profile (client)[1,2]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1,2]	Select the LAN optimized TCP profile you created above
	HTTP Profile[2]	Select the HTTP profile you created above
	Web Acceleration profile[2]	Select the Web Acceleration profile you created above
	HTTP Compression profile[2]	Select the HTTP Compression profile you created above
	OneConnect[2]	Select the OneConnect profile you created above
	SNAT Pool[3]	**Automap** (optional; see footnote [3])
	Default Pool[2]	Select the pool you created above
	Persistence Profile[2]	Select the Persistence profile you created
	iRule[4]	If offloading SSL only: Enable the built-in **_sys_https_redirect irule**
	HTTPS[5]	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	Web Acceleration profile	Select the Web Acceleration profile you created above
	HTTP Compression profile	Select the HTTP Compression profile you created above
	OneConnect	Select the OneConnect profile you created above
	SSL Profile (client)	Select the Client SSL profile you created above
	SNAT Pool[2]	**Automap** (optional; see footnote [3])
	Default Pool	Select the pool you created above
	Persistence Profile	Select the Persistence profile you created

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] *Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server, and only requires a name, IP address, Port, and the redirect iRule.*
[3] *If want to use SNAT, and you have a large Oracle deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*
[4] *Only enable this iRule if offloading SSL*
[5] *Only create this virtual server if offloading SSL*

Document Revision History

Version	Description
1.0	New Version

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com