Deploying F5 with Oracle Fusion Middleware Identity Management 11gR1

ORACLE
WEBLOGIC
R E A D Y

Introducing the F5 and Oracle Identity Management configuration

Welcome to the F5 and Oracle® Identity Management deployment guide. This guide provides step-by-step procedures on configuring the BIG-IP LTM with Oracle Identity Management.

Oracle Identity Management allows enterprises to manage end-to-end lifecycle of user identities across all enterprise resources both within and beyond the firewall. You can now deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and much more. Oracle Identity Management is a member of the Oracle Fusion Middleware family of products, which brings greater agility, better decision-making, and reduced cost and risk to diverse IT environments today.

For more information on Oracle Identity Management, see **http://www.oracle.com/technology/products/id_mgmt/index.html**.

For more information on F5 products, see **http://www.f5.com/products/**.

Prerequisites and configuration notes

The following are general prerequisites for this deployment; each section contains specific prerequisites:

◆ This guide was tested using Oracle Fusion Middleware Identity Management version 11.1.1.1.0

◆ This document is written with the assumption that you are familiar with both the BIG-IP LTM system and Oracle Identity Management. For more information on configuring these products, consult the appropriate documentation.

◆ The Oracle Identity Management configuration in our testing was based off of the *Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	v10.0.1 (also applicable to v9.x)
Oracle Identity Management	11.1.1.1.0

Revision history:

Version	Description
1.0	New deployment guide
1.1	Corrected an incorrect reference to a cookie persistence profile in the introduction to the OVD persistence section on page 27.

Configuration example

The BIG-IP LTM system provides intelligent traffic management, fail-over, and simple scalability for Oracle Identity Management devices. Through advanced health checking capabilities, the BIG-IP LTM recognizes when resources are unavailable or under-performing and directs traffic to another resource. An iRule on the BIG-IP prevents access to the Oracle Enterprise Manager console and Weblogic console, according to Oracle best practices.
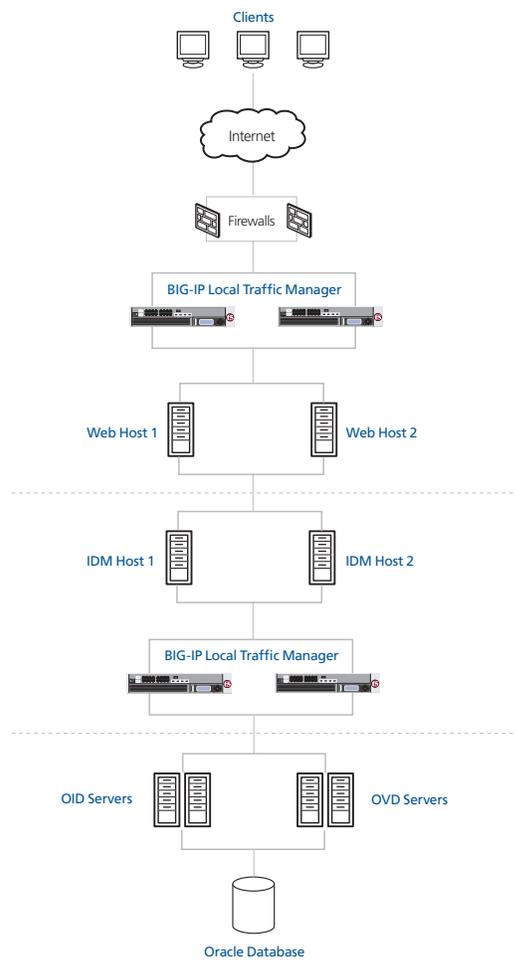

Figure 1 *F5 - Oracle Identity Management logical configuration example*

Configuring the BIG-IP LTM system for deployment with Oracle Identity Management

To configure the BIG-IP LTM system for directing traffic to the Oracle servers, you need to complete the following procedures:

- *Configuring the BIG-IP LTM for Oracle Internet Directory Single Sign On Services*, on page 4
- *Configuring the BIG-IP LTM for Oracle Identity Management Administrative console*, on page 18
- *Configuring the BIG-IP LTM for Oracle Internet Directory*, on page 20
- *Configuring the BIG-IP LTM for Oracle Virtual Directory*, on page 25

◆ **Tip**

We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. For information on backing up or restoring a BIG-IP LTM configuration, refer to the appropriate BIG-IP LTM manual, available on Ask F5.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP LTM web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
    https://<administrative IP address of the BIG-IP device>
    A Security Alert dialog box appears, click **Yes**.
    The authorization dialog box appears.

2. Type your user name and password, and click **OK**.
    The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Configuring the BIG-IP LTM for Oracle Internet Directory Single Sign On Services

The first task is to configure the BIG-IP LTM system for directing external traffic to the single sign on services. Oracle requires external clients to communicate with the web servers over HTTPS, however, the servers communicate over HTTP on a custom port of 7777. The BIG-IP LTM performs the port translation, as well as providing load distribution, high availability, increased scalability, and the Oracle recommended SSL acceleration.

In the Oracle documentation, this is the **sso.mycompany.com** virtual server with its associated objects as defined in Section 2.2.2 of the Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management 11g Release 1 (11.1.1).

In this section, we also configure an iRule on the BIG-IP LTM to comply with Oracle's requirement that access to Enterprise Manager and the WebLogic Administration Console is filtered out on this Virtual Server.

◆ **Note**

For this deployment guide, we assume you are taking advantage of the resource savings by offloading SSL processing on to the BIG-IP LTM.

Creating the health monitor

The first step is to set up a health monitor for the Oracle devices. This procedure is optional, but very strongly recommended. In our example, we create an HTTP health monitor. Although the monitor in the following example is quite simple, you can configure more complex Send and Receive Strings to make the monitor much more specific.

To configure a HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.

2. Click the **Create** button. The New Monitor screen opens.

3. In the **Name** box, type a name for the Monitor. In our example, we type **oracle-sso-http**.

4. From the **Type** list, select **HTTP**.

5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval** of **5** and a **Timeout** of **16.**

6. In the **Send String** box, type the following string:
   `GET /\n\n`

7. The rest of the settings are optional, configure as appropriate for your implemenation.

8. Click the **Finished** button.

Figure 2 Creating the HTTP monitor

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the Oracle devices. A BIG-IP LTM pool is a set of devices grouped together to receive traffic according to a load balancing method. A BIG-IP LTM pool makes future scaling of your Oracle Identity Management deployment extremely easy; simply add a new device to the network, then add it to the pool. The BIG-IP LTM immediately begins monitoring and directing traffic to the device.

To create the pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.

3. From the Configuration list, select **Advanced**.

4. In the **Name** box, enter a name for your pool. In our example, we use **oracle-sso-web**.

5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the health monitor* section, and click the Add (<<) button. In our example, we select **oracle-sso-http**.

6. In the **Slow Ramp Time** box, type **300**.
   Because we are using the Least Connections load balancing method, we set the Slow Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the BIG-IP LTM does not send all new connections to that member (a newly available member will always have the least number of connections).

7. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Least Connections (member)**.

8. For this pool, we leave the Priority Group Activation **Disabled**.

9. In the New Members section, make sure the **New Address** option button is selected.

10. In the **Address** box, add the first server to the pool. In our example, we type **10.133.15.60**.

11. In the **Service Port** box, type the appropriate port for your device. In our example, we type **7777**.

12. Click the **Add** button to add the member to the list.

13. Repeat steps 8-10 for each server you want to add to the pool.

14. Click the **Finished** button.

Figure 3 *Creating the BIG-IP LTM pool*

Importing SSL certificates and keys

In this deployment guide, we are configuring the BIG-IP LTM system to act as an SSL proxy, so you must install a SSL certificate on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP

LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive.

To import a key or certificate

1. On the Main tab, expand **Local Traffic**.

2. Click **SSL Certificates**. The list of existing certificates displays.

3. In the upper right corner of the screen, click **Import**.

4. From the **Import Type** list, select the type of import (Certificate or Key).

5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.

6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.

7. Click **Import**.

8. If you imported the certificate, repeat this procedure for the key.

Creating the profiles

The next task is to create the profiles. A *profile* is an object that contains user-configurable settings 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.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.

3. In the **Name** box, type a name for this profile. In our example, we type **oracle-sso-http**.

4. From the **Parent Profile** list, select **http**. The profile settings appear.

5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.

6. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Oracle users are accessing the deployment via a Local Area Network, we recommend using the **tcp-lan-optimized** parent profile (for server-side TCP connections). If the majority of the users are accessing the system from remote or home offices, we recommend using an additional TCP profile, called **tcp-wan-optimized** (for client-side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you do not want to use this optimized profile, you can choose the default TCP parent profile.

To create a new LAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

2. On the Menu bar, from the **Protocol** menu, click **tcp**.

3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle-idm-sso-lan**.

5. From the **Parent Profile** list, select **tcp-lan-optimized**.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most of the users are accessing the system over the LAN or other low latency links, you do not need to create this profile.

To create a new WAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

2. On the Menu bar, from the **Protocol** menu, click **tcp**.

3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle-sso-tcp-wan**.

5. From the **Parent Profile** list, select **tcp-wan-optimized**.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating the persistence profiles

Next, we create the persistence profiles. We recommend using cookie persistence (HTTP cookie insert) as the default profile, and configuring Source Address persistence as a fallback mode.

Creating the cookie persistence profile

Use this procedure to configure the cookie persistence profile.

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

2. On the Menu bar, click **Persistence**. The Persistence Profiles screen opens.

3. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle-sso-cookie**.

5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating the source address persistence profile

Use this procedure to configure the source address persistence profile.

To create a new source address persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.

2. On the Menu bar, click **Persistence**.

3. Click the **Create** button.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle-sso-source**.

5. From the **Persistence Type** list, select **Source Address Affinity**.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating a OneConnect profile

The final profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. This can provide significant performance improvements for Oracle implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

2. On the Menu bar, from the **Other** menu, click **OneConnect**.

3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle-sso-oneconnect**.

5. From the **Parent Profile** list, ensure that **oneconnect** is selected.

6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating a Client SSL profile

The next step in this configuration is to create a Client SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, and the click **Profiles**.

2. On the Menu bar, from the SSL menu, select **Client**.

3. In the upper right portion of the screen, click the **Create** button. The New Client SSL Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oam-sso-clientssl**.

5. In the Configuration section, check the **Certificate** and **Key Custom** boxes.

6. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.

7. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.

8. Click the **Finished** button.

Creating the iRules

In the following procedures, we create two iRules on the BIG-IP LTM system. While these iRules are optional, we recommend using them as they can greatly improve end user experience.

Creating the Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and redirects them to the correct HTTPS (secure) virtual server, without user interaction.

To create the Redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.

3. In the **Name** box, enter a name for your iRule. In our example, we use **oracle-sso-httptohttps**.

4. In the Definition section, copy and paste the following iRule:

```
when HTTP_REQUEST {

    if { [string length [HTTP::host]] } {
```

```
                    HTTP::redirect https://[getfield [HTTP::host] ":" 1][HTTP::uri]
            }
            else {
                HTTP::redirect https://[IP::local_addr][HTTP::uri]
            }
    }
```

5. Click the **Finished** button.

Creating the filtering iRule

We create the filtering iRule to disallow access to the Oracle Enterprise Manager console and Weblogic console, according to Oracle best practices.

To create the filtering iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.

3. In the **Name** box, enter a name for your iRule. In our example, we use **oracle-sso-filter**.

4. In the Definition section, copy and paste the following iRule:

```
when HTTP_REQUEST {
    if { [HTTP::uri] starts_with "/console" } {
        #log local0.warn "Rejecting request to browse to console."
        #reject
        HTTP::respond 403 content "<html><body><b>HTTP Error 403 - Forbidden</b></body></html>"
    }
    if { [HTTP::uri] starts_with "/em" } {
        #log local0.warn "Rejecting request to browse to EM."
        #reject
        HTTP::respond 403 content "<html><body><b>HTTP Error 403 - Forbidden</b></body></html>"
    }
}
```

5. Click the **Finished** button.

Creating the Oracle Identity managment virtual servers

The final task in this section is to create the BIG-IP LTM virtual servers. The first virtual server is solely to intercept incoming HTTP traffic and redirect it to HTTPS using the iRule you created; this virtual is optional. The second virtual server terminates the SSL (HTTPS) connections and sends traffic via HTTP to the pool of Oracle devices.

Creating the HTTP virtual server

The first virtual server we create is the HTTP virtual server. This server simply redirects users to the HTTPS virtual server you create in the next procedure.

To create the HTTP virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.

3. In the **Name** box, type a name for this virtual server. In our example, we type **oracle-sso-http**.

4. In the **Destination** section, select the **Host** option button.

5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.100.171**.

6. In the **Service Port** box, type **80**, or select **HTTP** from the list.

7. In the Configuration section, select **Advanced** from the list. The Advanced configuration options appear.

8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **oracle-idm-wan**. This is optional, an only necessary if you created a WAN optimized profile.

9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **oracle-idm-lan**.

10. From the **HTTP Profile** list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **oracle-sso-http**.

11. From the **SNAT Pool** list, select **Automap**.

12. In the Resources section, from the **iRules** Available list, select the iRule you created for redirection in the *Creating the Redirect iRule* section. In our example, we select **oracle-idm_httptohttps**.

    Do not select a pool for the virtual server.

13. Click the **Finished** button.

Creating the HTTPS virtual server

Next, we create the HTTPS virtual server.

To create the HTTPS virtual server

1. On the Main tab, expand **Local Traffic**, click **Virtual Servers**, and then click the **Create** button.

2. In the **Name** box, type a name for this virtual server. In our example, we type **oracle-sso-https**.

3. In the **Destination** section, select the **Host** option button.

4. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.100.171**.

5. In the **Service Port** box, type **443**, or select HTTPS from the list.

Figure 4 *Configuring the general properties of the virtual server*

6. From the Configuration list, select **Advanced**. The Advanced configuration options appear.

7. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **oracle-sso-wan**. This is optional, an only necessary if you created a WAN optimized profile.

8. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **oracle-sso-lan**.

9. From the **OneConnect Profile** list, select the name of the profile you created in the *Creating a OneConnect profile* section. In our example, we select **oracle-sso-oneconnect**.

10. From the **HTTP Profile** list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **oracle-sso-http**.

11. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **oracle-sso-clientssl**.

12. From the **SNAT Pool** list, select **Automap** (see Figure 5).

Figure 5 *Configuration section of the virtual server (condensed)*

13. In the Resources section, from the **iRules** Available list, select the iRule you created in the *Creating the filtering iRule* section. In our example, we select **oracle-sso-filter**.

14. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **oracle-sso-web**.

15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating the cookie persistence profile* section. In our example, we select **oracle-sso-cookie**.

16. From the **Fallback Persistence Profile** list, select the persistence profile you created in the *Creating the source address persistence profile* section. In our example, we select **oracle-sso-source**.
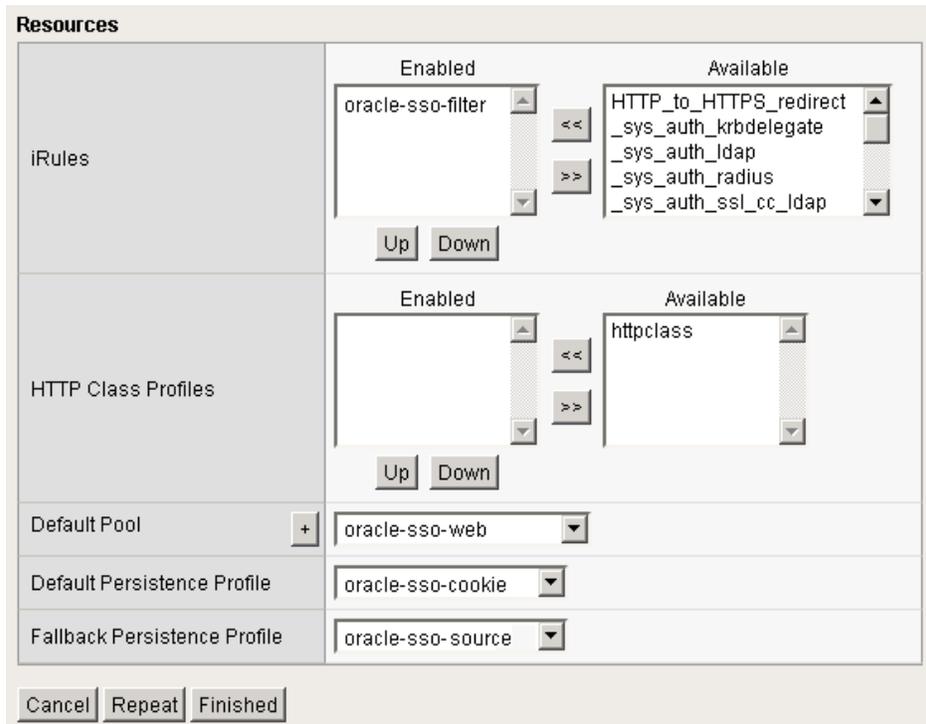
17. Click the **Finished** button (see Figure 6).

Figure 6 *Resource section of the virtual server*

Configuring the BIG-IP LTM for Oracle Identity Management Administrative console

The next set of BIG-IP LTM configuration objects we create are for internal access to the Weblogic console, Oracle Enterprise Manager console, and Oracle Directory Services Manager for Identify Management. This is known as the **admin.mycompany.com** virtual server with its associated objects as defined in Section 2.2.2 of the Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management 11g Release 1 (11.1.1).

Oracle Identity Management provides an Administration Console, not only for users, but for processes that need access to administrative objects. The BIG-IP LTM provides load distribution and high availability in addition to satisfying the security requirement that the Administration Console be accessible only from your internal network.

◆ **Note**

This guide is written with the assumption that you are using VLANs to segment your traffic, and you have internal and external VLANs already configured on the BIG-IP LTM. This virtual server is locked down to the internal VLANs. For more information on creating VLANs, see the BIG-IP LTM documentation. If you are using a dedicated BIG-IP system on the internal network, there is no need to lock this virtual server down to the internal VLAN.

There is no need to create a health monitor or pool, as this virtual server uses the same pool you created earlier in this guide.

Creating the profiles

While you can use the profiles you created in the previous section, we recommend you create new profiles for the console access.

Creating the HTTP profile

To create the HTTP profile, follow the procedure found in *Creating an HTTP profile*, on page 8. Use a unique name, all other settings are optional.

Creating the LAN optimized TCP profile

To create the TCP profile, follow the procedure *Creating the LAN optimized TCP profile*, on page 9. Use a unique name, all other settings are optional. In this case, we only use a LAN optimized profile because access to the console is internal.

Creating the OneConnect profile

To create the OneConnect profile, follow the procedure found in *Creating a OneConnect profile*, on page 11. Use a unique name, all other settings are optional.

Creating the administrative console virtual server

The final step is to create a virtual server for the Administrative Console.

To create the console virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.

2. Click the **Create** button.

3. In the **Name** box, type a name for this virtual server. In our example, we type **oracle-idm-admin**.

4. In the **Destination** section, select the **Host** option button.

5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.15.104**

6. In the **Service Port** box, type **80**, or select **HTTP** from the list.

7. From the Configuration list, select **Advanced**.

8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **oracle-admin-lan**.

9. From the **OneConnect Profile** list, select the name of the profile you created in the *Creating a OneConnect profile* section. In our example, we select **oracle-admin-oneconnect**.

10. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **oracle-admin-http**.

11. In the **VLAN List** section, from the **Available** list, select the name of an internal VLAN and click the Add (**<<**) button. Repeat this procedure for all internal VLANs.

12. From the **SNAT Pool** list, select **Automap**.

13. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **oracle-sso-web**.

14. Click the **Finished** button.

Configuring the BIG-IP LTM for Oracle Internet Directory

The next group of objects we configure on the BIG-IP LTM system is for the Oracle Internet Directory (OID) component.

In the Oracle documentation, this is the **oid.mycompany.com** virtual server with its associated objects as defined in Section 2.2.2 of the Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management 11g Release 1 (11.1.1).

Oracle Identity Management provides LDAP access via the Oracle Internet Directory service. Using the BIG-IP LTM to direct traffic to a pool of OID servers provides load distribution, high availability, and increased scalability.

The BIG-IP LTM configuration for OID is also very similar to the IDM configuration, so in some the following sections, we reference the procedures from the IDM section.

This section is broken up into two parts:

*   *Configuring the BIG-IP LTM for OID using LDAP*, following
*   *Configuring the BIG-IP LTM for OID using LDAPS*, on page 23

◆ **Note**

A reminder that this guide is written with the assumption that you are using VLANs to segment your traffic, and you have internal and external VLANs already configured on the BIG-IP LTM. This OID virtual server is also locked down to the internal VLANs. For more information on creating VLANs, see the BIG-IP LTM documentation. If you are using a dedicated BIG-IP system on the internal network, there is no need to lock this virtual server down to the internal VLAN.

Configuring the BIG-IP LTM for OID using LDAP

First, we configure the BIG-IP LTM for OID using LDAP.

Creating a LDAP health monitor

The first task is to create a LDAP health monitor for OID. For this monitor, you need a user name and password from your LDAP directory. You may want to create a new user in LDAP to be used solely for this purpose.

To create the LDAP monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors**, and then click the **Create** button. The New Monitor screen opens.

2. In the **Name** box, type a name for the Monitor.
    In our example, we type **oracle-oid-ldap**.

3. From the **Type** list, select **LDAP**.

4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout In our example, we use a **Interval** of **5** and a **Timeout** of **16**.

5. In the **User Name** box, type a valid user name in the LDAP directory. In our example, we type **cn=bigipuser**.

6. In the **Password** box, type the password associated with the user.

7. The rest of the settings are optional, configure as appropriate for your implemenation.

8. Click the **Finished** button.

Creating the pool

The next task is to create a pool for the OID devices. Follow the procedure *Creating the pool*, on page 5. Type a unique name for the pool, configure the pool to use the LDAP health monitor you just created, and add the appropriate IP address and port (default port is **389**). All other settings are optional, configure as applicable for your configuration.

Creating the profiles

For OID, we create three profiles, a TCP profile and two persistence profiles.

Creating the TCP profile

To create the TCP profile, follow the procedure *Creating the LAN optimized TCP profile*, on page 9. Use a unique name, all other settings are optional. In this case, we only use a LAN optimized profile because this is an internal virtual server.

Creating the persistence profiles

For this virtual server, we create two persistence profiles. The default persistence profile will be source address affinity, and the fallback profile is destination address affinity.

◆ To create the Source Address persistence profile, follow the procedure *Creating the source address persistence profile*, on page 11. Use a unique name, all other settings are optional.

◆ Use the procedure to configure the destination address persistence profile.

To create a new destination address persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.

2. On the Menu bar, click **Persistence**.

3. Click the **Create** button.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle-oid-destination**.

5. From the **Persistence Type** list, select **Destination Address Affinity**.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating the OID virtual server

The final step is to create a virtual server for the OID devices. Follow the procedure *Creating the administrative console virtual server*, on page 19. Give this virtual server a unique name, and use the appropriate address and port (the default port is **389**), and configure the virtual server to use the pool and profiles you created in the preceding procedures. Be sure to lock down the virtual server to the internal VLANs in step 11.

Configuring the BIG-IP LTM for OID using LDAPS

Now we configure the BIG-IP LTM for LDAPS. The LDAPS configuration is similar to the configuration for LDAP, however the health monitor and ports are different.

Creating a LDAPS health monitor

For this monitor, you need a user name and password from your LDAP directory. You may want to create a new user in LDAP to be used solely for this purpose.

To create the LDAP monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors**, and then click the **Create** button. The New Monitor screen opens.

2. In the **Name** box, type a name for the Monitor.
   In our example, we type **oracle-oid-ldaps**.

3. From the **Type** list, select **LDAP**.

4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. In our example, we use a **Interval** of **5** and a **Timeout** of **16**.

5. In the **User Name** box, type a valid user name in the LDAP directory. In our example, we type **cn=bigipuser**.

6. In the **Password** box, type the password associated with the user.

7. From the **Security** list, select **TLS** or **SSL** as appropriate for your configuration. In our example, we select **TLS**.

8. The rest of the settings are optional, configure as appropriate for your implemenation.

9. Click the **Finished** button.

◆ Note

If your LDAP monitor for LDAPS is not working properly, you can use the **TCP Half Open** *monitor. In Section 10.6.1 of the Oracle IDM Enterprise Deployment Guide, Oracle states it is sufficient to succesfully monitor the LDAP side with the BIG-IP LDAP monitor, and, on the LDAPS side, monitor the port with the TCP Half Open monitor.*

Creating the LDAPS pool

The next task is to create a pool for the OID devices. Follow the procedure *Creating the pool*, on page 5. Type a unique name for the pool, configure the pool to use the LDAPS health monitor you just created, and add the appropriate IP address and port (default port is **636**). Any additional settings are optional, configure as applicable for your configuration.

Creating the profiles

For OID using LDAPS, we create three profiles, a TCP profile and two persistence profiles.

Creating the TCP profile

To create the TCP profile, follow the procedure *Creating the LAN optimized TCP profile*, on page 9. Use a unique name, any additional settings are optional. In this case, we only use a LAN optimized profile because this is an internal virtual server.

Creating the persistence profiles

For this virtual server, we create two persistence profiles. The default persistence profile will be source address affinity, and the fallback profile is destination address affinity.

◆ To create the Source Address persistence profile, follow the procedure *Creating the source address persistence profile*, on page 11. Use a unique name, all other settings are optional.

◆ To create the Destination Address persistence profile, follow the procedure *To create a new destination address persistence profile*, on page 22. Use a unique name, all other settings are optional.

Creating the OID using LDAPS virtual server

The final step is to create a virtual server for the OID devices. Follow the procedure *Creating the administrative console virtual server*, on page 19. Give this virtual server a unique name, and use the appropriate address and port (the default port is **636**), and configure the virtual server to use the pool and profiles you created in the preceding procedures. Be sure to lock down the virtual server to the internal VLANs in step 11.

Configuring the BIG-IP LTM for Oracle Virtual Directory

The next group of objects we configure on the BIG-IP LTM system is for the Oracle Virtual Directory (OVD) component. Oracle Identity Management also provides virtualized LDAP and database access via the Oracle Virtual Directory Service. Oracle Virtual Directory, however, communicates over a custom port (6501/7501). Using the BIG-IP LTM to direct traffic to a pool of OVD servers provides port translation, load distribution, high availability, and increased scalability.

In the Oracle documentation, this is the **ovd.mycompany.com** virtual server with its associated objects as defined in Section 2.2.2 of the Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management 11g Release 1 (11.1.1).

The BIG-IP LTM configuration for OVD is nearly indentical to the configuration for OID with the exception of port numbers, so in the following sections, we reference the procedures from the OID section.

This section is broken up into two parts:

- *Configuring the BIG-IP LTM for OVD using LDAP*, following
- *Configuring the BIG-IP LTM for OVD using LDAPS*, on page 26

◆ **Note**

A reminder that this guide is written with the assumption that you are using VLANs to segment your traffic, and you have internal and external VLANs already configured on the BIG-IP LTM. This OVD virtual server is also locked down to the internal VLANs. For more information on creating VLANs, see the BIG-IP LTM documentation. If you are using a dedicated BIG-IP system on the internal network, there is no need to lock this virtual server down to the internal VLAN.

Configuring the BIG-IP LTM for OVD using LDAP

First, we configure the BIG-IP LTM for OVD using LDAP.

Creating a LDAP health monitor

To configure the LDAP health monitor, follow the procedure *Creating a LDAP health monitor*, on page 25. Use a unique name, any additional settings are optional.

Creating the pool

The next task is to create a pool for the OVD devices. Follow the procedure *Creating the pool*, on page 5. Type a unique name for the pool, configure the pool to use the LDAP health monitor you just created, and add the appropriate IP address and port (default port is **6501**). Any additional settings are optional, configure as applicable for your configuration.

Creating the profiles

For OVD, we create three profiles, a TCP profile and two persistence profiles.

Creating the TCP profile

To create the TCP profile, follow the procedure *Creating the LAN optimized TCP profile*, on page 9. Use a unique name, any additional settings are optional. In this case, we only use a LAN optimized profile because this is an internal virtual server.

Creating the persistence profiles

For this virtual server, we create two persistence profiles, a default cookie persistence profile, and a fallback Source Address persistence profile.

◆ To create the Source Address persistence profile, follow the procedure *Creating the source address persistence profile*, on page 11. Use a unique name, all other settings are optional.

◆ To create the Destination Address persistence profile, follow the procedure *To create a new destination address persistence profile*, on page 22. Use a unique name, all other settings are optional.

Creating the OVD virtual server

The final step is to create a virtual server for the OID devices. Follow the procedure *Creating the administrative console virtual server*, on page 19. Give this virtual server a unique name, and use the appropriate address and port (the default port is **6501**), and configure the virtual server to use the pool and profiles you created in the preceding procedures. Be sure to lock down the virtual server to the internal VLANs in step 11.

Configuring the BIG-IP LTM for OVD using LDAPS

Now we configure the BIG-IP LTM for OVD using LDAPS. The LDAPS configuration is similar to the configuration for LDAP, however the health monitor and ports are different.

Creating a LDAPS health monitor

To configure the LDAP health monitor, follow the procedure *Creating a LDAPS health monitor*, on page 27. Use a unique name, any additional settings are optional.

◆ Note

*If your LDAP monitor for LDAPS is not working properly, you can use the **TCP Half Open** monitor. In Section 10.6.1 of the Oracle IDM Enterprise Deployment Guide, Oracle states it is sufficient to succesfully monitor the LDAP side with the BIG-IP LDAP monitor, and, on the LDAPS side, monitor the port with the TCP Half Open monitor.*

Creating the LDAPS pool

The next task is to create a pool for the OVD devices. Follow the procedure *Creating the pool*, on page 5. Type a unique name for the pool, configure the pool to use the LDAPS health monitor you just created, and add the appropriate IP address and port (default port is **7501**). All other settings are optional, configure as applicable for your configuration.

Creating the profiles

For OVD using LDAPS, we create three profiles, a TCP profile and two persistence profiles.

Creating the TCP profile

To create the TCP profile, follow the procedure *Creating the LAN optimized TCP profile*, on page 9. Use a unique name, all other settings are optional. In this case, we only use a LAN optimized profile because this is an internal virtual server.

Creating the persistence profiles

For this virtual server, we create two persistence profiles: a source address persistence profile, and a destination address persistence profile.

◆ To create the Source Address persistence profile, follow the procedure *Creating the source address persistence profile*, on page 11. Use a unique name, all other settings are optional.

◆ To create the Destination Address persistence profile, follow the procedure *To create a new destination address persistence profile*, on page 22. Use a unique name, all other settings are optional.

Creating the OVD using LDAPS virtual server

The final step is to create a virtual server for the OID devices. Follow the procedure *Creating the administrative console virtual server*, on page 19. Give this virtual server a unique name, and use the appropriate address and

port (the default port is **7501**), and configure the virtual server to use the pool and profiles you created in the preceding procedures. Be sure to lock down the virtual server to the internal VLANs in step 11.

Appendix A: Oracle configuration

The following table contains configuration settings that need to be changed on the Oracle devices. This information is provided for your convenience, for more information, consult the Oracle documentation.

The following links are located in the Oracle document: **Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management 11g Release 1 (11.1.1)** -- Part Number E12035-02 .

Virtual Server	Task	Location in Oracle documentation
Ext. SSO HTTPS virtual server (oracle-sso-https in our example)	Define the HTTPS virtual server as a Virtual Host on your Web Tier machines.	Section 6.5: http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/webtier_im.htm#IMEDG304
Admin virtual server (oracle-idm-admin in our example)	Define the admin HTTP virtual server as a Virtual Host on your Web Tier machines.	Section 6.5: http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/webtier_im.htm#IMEDG304
	Define the admin HTTP virtual server as the Preferred HTTP Host.	Section 7.4.3.1 (step 4): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG404
	Define the admin HTTP virtual server as the Preferred HTTP Host.	Section 8.2.3 (step 8): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/confg_sso_admconsoles_im.htm#IMEDG437
	Define the admin HTTP virtual server as the Preferred HTTP Host.	Section 8.2.4 (step 7): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/confg_sso_admconsoles_im.htm#IMEDG438
OID Virtual Server (oracle-oid-ldap(s) in our example)	Use the LDAP and LDAPS virtual servers when validating the Directory Tier Components with the ldapbind command.	Section 4.7: http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/directorytier_im.htm#BABDFBGH
	Use the LDAP virtual server for the hostname when Specifying OID Details	Section 5.1 (step 12): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/domain_im.htm#CACEADGE
	Use the OID LDAP virtual server for the host when creating a connection to OID in the ODSM console	Section 5.3.1 (step 2b): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/domain_im.htm#CACIDFEB
	Use the OID LDAP virtual server for the Host machine or IP in which your directory server resides.	Section 7.3.1.1 (step 16): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG386
	Use the OID LDAP virtual server for the Host machine or IP in which your directory server resides.	Section 7.3.4.1 (step 5): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG395
	Use the OID LDAP virtual server for the Host machine or IP in which your directory server resides.	Section 7.4.1.1 (step 6): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG399
	Use the OID LDAP virtual server for the Host of your Oracle configuration data directory server.	Section 7.4.2.2 (step 8): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG402
	Use the OID LDAP virtual server for the hostname when creating a WebGate profile via the OAM Configuration Tool	Section 8.2.2: http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/confg_sso_admconsoles_im.htm#IMEDG312

Virtual Server	Task	Location in Oracle documentation
OID Virtual Server - cont. (oracle-oid-ldap(s) in our example)	Use the OID LDAP virtual server for the Host when specifying your LDAP server details.	Section 8.4.1 (step 3n): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/confg_sso_admconsoles_im.htm#IMEDG319
	Use the OID LDAP virtual server for the host name when provisioning Admin Users and Groups in an LDAP Directory with the ldapadd command.	Section 8.6.1 (steps 2 and 4): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/confg_sso_admconsoles_im.htm#IMEDG430
	Use the OID LDAP virtual server for the hostname when adding entries to Oracle Internet Directory with the ldapadd command.	Section 8.7.1 (step 2): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/confg_sso_admconsoles_im.htm#IMEDG324
OVD Virtual Server (oracle-ovd-ldap(s) in our example)	Use the OVD LDAP and LDAPS virtual servers when validating the Directory Tier Components with the ldapbind command.	Section 4.7: http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/directorytier_im.htm#BABDFBGH
	Use the OVD LDAP virtual server for the Host machine or IP in which your directory server resides.	Section 7.3.1.1 (step 16): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG386
	Use the OVD LDAP virtual server for the Host machine or IP in which your directory server resides.	Section 7.3.4.1 (step 5): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG395
	Use the OVD LDAP virtual server for the Host machine or IP in which your directory server resides.	Section 7.4.1.1 (step 6): http://download.oracle.com/docs/cd/E12839_01/core.1111/e12035/oam_im.htm#IMEDG399