Configuring Maximum Availability Architecture for Oracle Enterprise Manager with F5 BIG-IP Local Traffic Manager

Oracle Maximum Availability Architecture White Paper
February 2010

Maximum Availability Architecture

Oracle Best Practices For High Availability

ORACLE

Executive Overview

Oracle Maximum Availability Architecture (MAA) [1] is the Oracle best practices blueprint for implementing Oracle high-availability technologies. Oracle Enterprise Manager is the management platform for Oracle solutions. This white paper has been jointly written by Oracle Corporation and F5 Networks and provides the detailed steps for implementation of an Oracle MAA solution for Oracle Enterprise Manager Grid Control using BIG-IP from F5 Networks as the front end for the Grid Control mid-tiers, known as the Oracle Managements Service (OMS).

The BIG-IP hardware platform can provide load balancing, high availability, service monitoring, TCP/IP enhancements, and application persistence for the Grid Control environment as the front end for several Grid Control services, including Secure Upload, Agent Registration, Secure Console, Unsecure Console and if required, WebCache Secure, and WebCache Unsecure.

Most of the procedures in this document are performed on the BIG-IP Local Traffic Manager (LTM), targeting different areas of the infrastructure where high availability is required to provide continuous access to the Grid Control OMS application that has been deemed mission critical.

This paper is designed to provide the Grid Control Administrator with an introduction to the high availability and load balancing features available with F5 solutions. Step-by-step configuration instructions and screen shots are provided to make it easier to understand and implement BIG-IP as a critical component of the Grid Control architecture.

In general, assume that the following software versions are used in this white paper:

- BIG-IP Version 10.0.1, Build 283
- Grid Control Release 10.2

Any distinction in release numbers is noted within the relevant discussions of this paper.

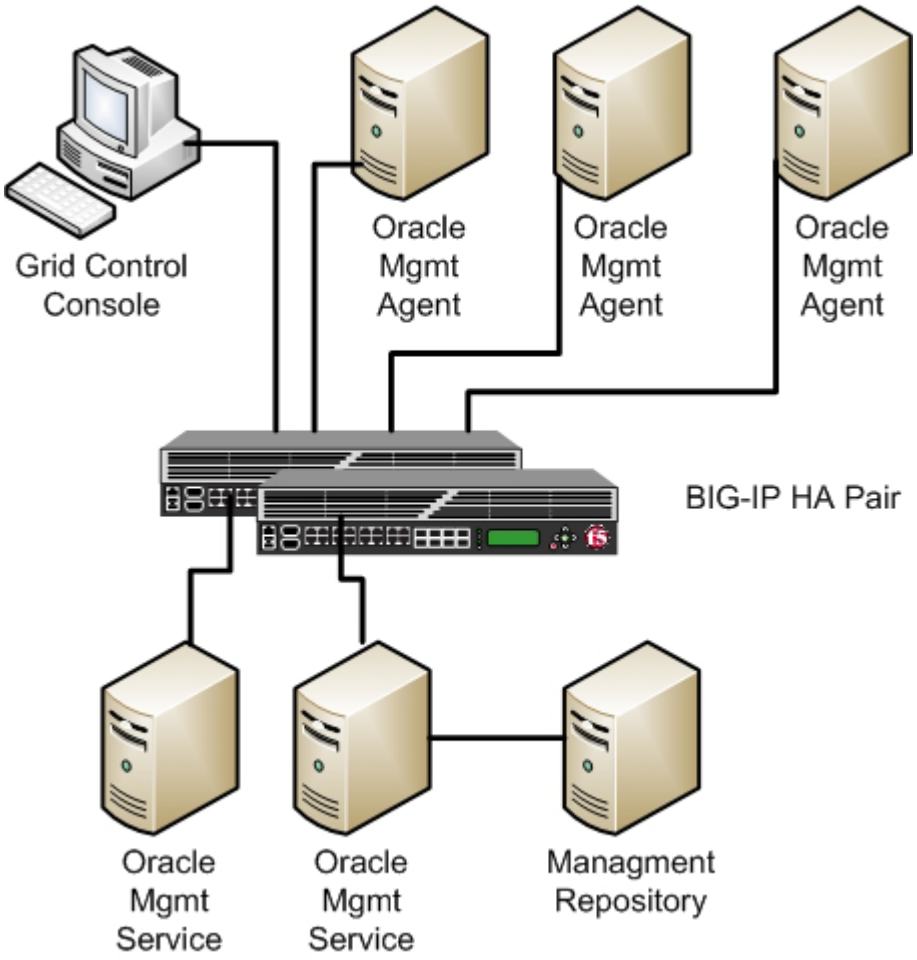
Note: This white paper assumes that you are familiar with BIG-IP from F5 Networks. See Appendix A for a quick terminology reference. For detailed information, see the BIG-

IP Solutions Guide and BIG-IP Configuration Guide, and Chapter 17 in the *Oracle Enterprise Manager Installation and Configuration Guide*.

About F5 BIG-IP and Oracle Enterprise Manager Grid Control

Figure 1 shows F5 and Oracle Enterprise Manager Elements in a Grid Control environment.

Figure 1: Configuration BIG-IP HA Pair with Grid Control



Each Grid Control service that is managed by F5 BIG-IP requires that you configure the following F5 BIG-IP Local Traffic Manager objects:

- A health monitor for the service.

The health monitor is the process by which BIG-IP determines that the service is up and running and can take connections.

- A TCP profile for the service.

  The TCP profile is used to tune the TCP/IP stack from BIG-IP for optimum performance.

- A Pool for the service.

  A Pool is a group of two or more OMS Grid Control servers that are load balanced, with each pool running an instance of the different Grid Control services.

- A Persistence profile for the service.

  The Persistence profile is used to link an OMS agent to the proper Grid Control pool member for the duration of a connection. This is required for all Grid Control services except Secure Upload (See Table 1).

- A Virtual Server for the service.

  A Virtual Server is a unique IP address and port that represents a pool of servers.

The remainder of this paper provides detailed instructions for configuring Grid Control services. Each of the configuration discussions imparts:

- Operational best practices when using the F5 BIG-IP Web configuration utility to configure Oracle Enterprise Manager Grid Control services.
- Screen shots of the BIG-IP Web interface that are based on BIG-IP Version 10.0.1 software. You can also use Version 9.*n* BIG-IP software because the configuration steps are identical.
- A Configuration Summary page naming all of the Grid Control services and matching F5 configuration elements.

For additional information about configuring BIG-IP Version 10.*n* and Version 9.*n*, see the BIG-IP documentation at http://www.f5.com.

Configuring an F5 BIG-IP LTM for Grid Control Services

Use the instructions that follow to configure Oracle Enterprise Manager to work with the F5 BIG-IP LTM. These procedures are provided for your convenience. For more detailed information and instructions, see the Oracle and F5 documentation resources that are listed in the References section at the end of this white paper.

Prerequisites and Best Practice Recommendations

Use the following general guidelines when building your configuration.

Use BIG-IP Administrative Partitions

A feature of the BIG-IP software is the ability to use *Administrative Partitions* to allow multiple administrators or operators to manage the configuration. The best practice recommendation is to create a dedicated Administrative Partition on the BIG-IP for configuration for access and use by the Grid Control administrators. All the necessary F5 configuration elements for the MAA Grid Control environment are located in the Administrative Partition. Additions, deletions, and changes to these pools created in this partition would not interfere with any other services provided by the BIG-IP. For more information about Configuring Administrative Partitions, see the BIG-IP documentation.

Use the Configuration Table and Standard Naming Conventions

To make the configuration consistent, easy to read, and easy to administer, this white paper uses a standard naming convention for the F5 configuration. Your organization may already use naming standards (which your Network Operations team can provide if necessary), or you can create naming conventions or adopt the ones used in this white paper.

The following table shows the naming conventions used by the MAA example described in this white paper.

SERVICE	PREFIX
Health monitors	mon_
TCP Profiles	tcp_
Pools	pool_
Cookie persistence profile	cookie_
Source IP Address persistence profile	sourceip_
Virtual server	vs_
Grid control services	gc_

Using the "Grid Control Secure Console" as an example, we derived the prefix "`gcsc`" and terminated each name with the TCP port number as a suffix. In the following list of names, the TCP port number 4444 is used for the servers, and 443 is used for the virtual server:

- `mon_gcsc4444`
- `tcp_gcsc4444`
- `sourceip_gcsc4444`

- `pool_gcsc4444`
- `vs_gcsc443`

Pool port numbers are referenced by the Grid Control servers. Virtual Server port numbers are referenced by the Grid Control clients.

These values are shown in Table 1, which provides a reference for all of the F5 configuration objects in this document. All of the names used in this white paper follow this convention, which is considered to be a best practice.

TABLE 1: F5 CONFIGURATION SUMMARY FOR GRID CONTROL SERVICES

GRID CONTROL SERVICE	TCP PORT	F5 MONITOR NAME	F5 TCP PROFILE NAME	F5 PERSIST PROFILE	F5 POOL NAME	F5 VIRTUAL SERVER NAME	F5 VIRTUAL SERVER PORT
Secure Upload	1159	mon_gcsu1159	tcp_gcsu1159	None	pool_gcsu1159	vs_gcsu1159	1159
Agent Registration	4889	mon_gcar4889	tcp_gcar4889	cookie_gcar4889	pool_gcar4889	vs_gcar4889	4889
Secure Console	4444	mon_gcsc4444	tcp_gcsc4444	sourceip_gcsc4444	pool_gcsc4444	vs_gcsc4444	443
Unsecure Console[1]	7777	mon_ gcuc7777	tcp_ gcuc7777	sourceip_ gcuc7777	pool_ gcuc7777	vs_ gcuc7777	7777
WebCache[2]	4443	mon_gcws4443	tcp_gcws4443	sourceip_gcws4443	pool_gcws4443	vs_gcws4443	4443
WebCache Unsecure	7779	mon_gcwu7779	tcp_gcwu7779	sourceip_gcwu7779	pool_gcwu7779	vs_gcwu7779	7779

Tip: Print Table 1 for easy reference during the configuration process.

[1] For information about configuring this pool, see the 'Create the Grid Control Unsecure Console Redirect iRule' topic in the F5 iRules at the F5 DevCentral Web site: http://devcentral.f5.com/Default.aspx?tabid=75.

[2] Configuration of the WebCache component is required only when WebCache is used. WebCache is optional unless it is specifically required by an Oracle Enterprise Manager Pack or feature.

Configure BIG-IP for Secure Upload (Port 1159)

Use the following step-by-step procedure as a template for configuring F5 BIG-IP to support the Secure Upload Service for the OMS system.

Step 1: Configure a health monitor for the Secure Upload service

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

1. On the **Monitors** screen, click **Create**.

   The New Monitor screen opens.

2. In the **Name** field, enter a unique name for the Monitor. For example: **mon_gcsu1159**
3. From the **Type** list, select **HTTPS**.

   The Monitor configuration options display.

4. From the Configuration list, select **Advanced**.
5. In the **Configuration** section, enter values in **Interval** and **Timeout** fields:

   - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   The MAA example sets Interval to 60 and Timeout to 181.

6. In the **Send String** field, add a Send String, as follows:

   ```
   GET /em/upload HTTP/1.0
   ```

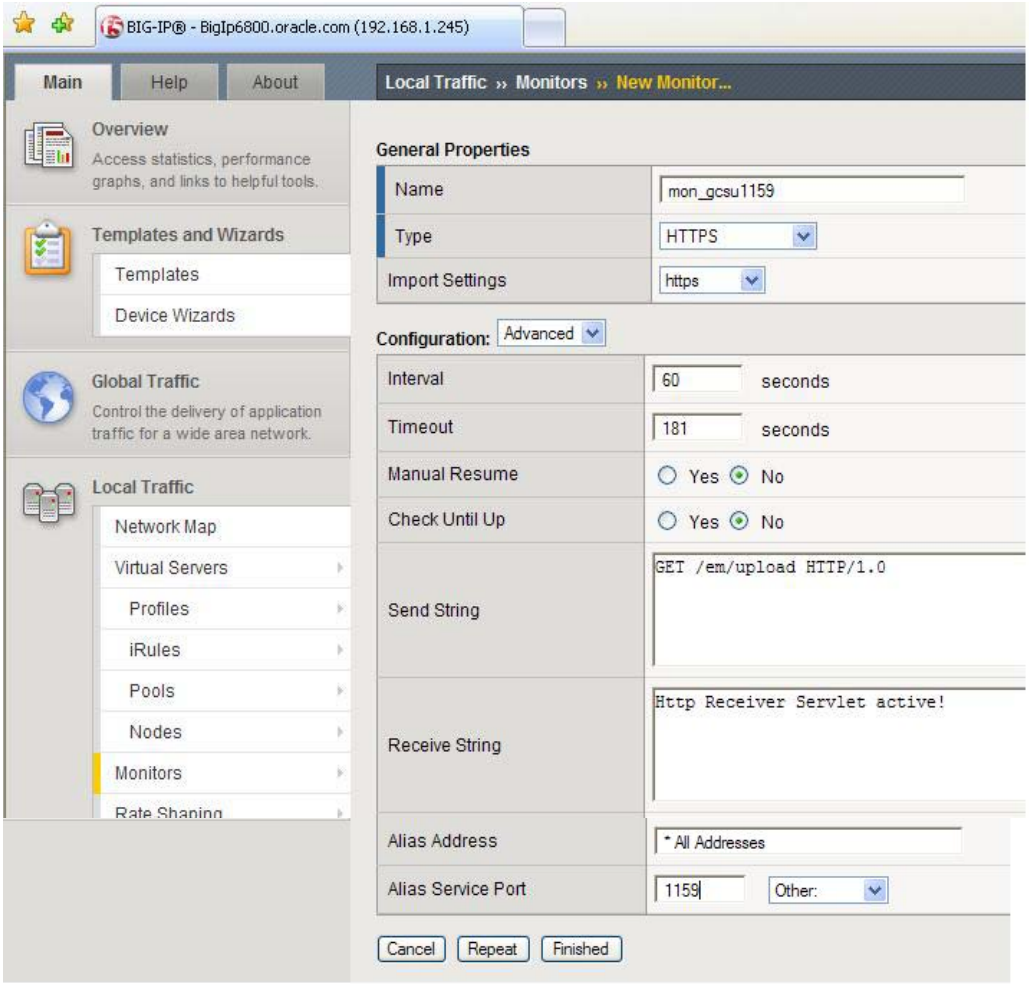
7. In the **Receive String** field, add a Receive String, as follows:

   ```
   Http Receiver Servlet active!
   ```

8. In the Alias Service Port field, enter **1159**.

   All other configuration settings are optional.

9. Click **Finished**.



Step 2: Create a new TCP profile for the Secure Upload service

In the following example, the TCP profile is based on the default TCP profile, and keeps all of the options at the default settings. You can configure these options, as appropriate, for your network.

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

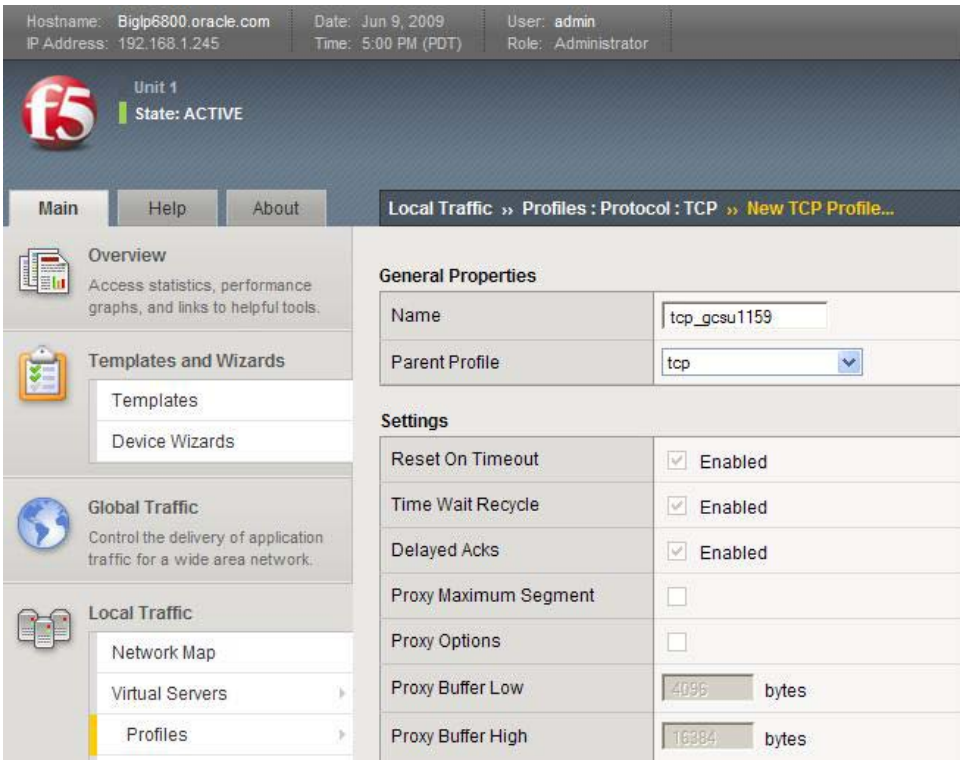
   The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

   The New TCP Profile screen opens.

5. In the **Name** field, enter a unique name for this profile. For example: **tcp_gcsu1159**.

   If needed, modify the name, as applicable, for your network. See the F5 online help for more information about the configuration options. In the MAA example the settings remain at the default levels.

6. Click **Finished**.



Step 3: Create the Secure Upload pool

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing methodology. In this configuration example, one pool is created for the Grid Control Secure Upload devices:

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

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

   The New Pool screen opens.

Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure these settings as applicable for your network.

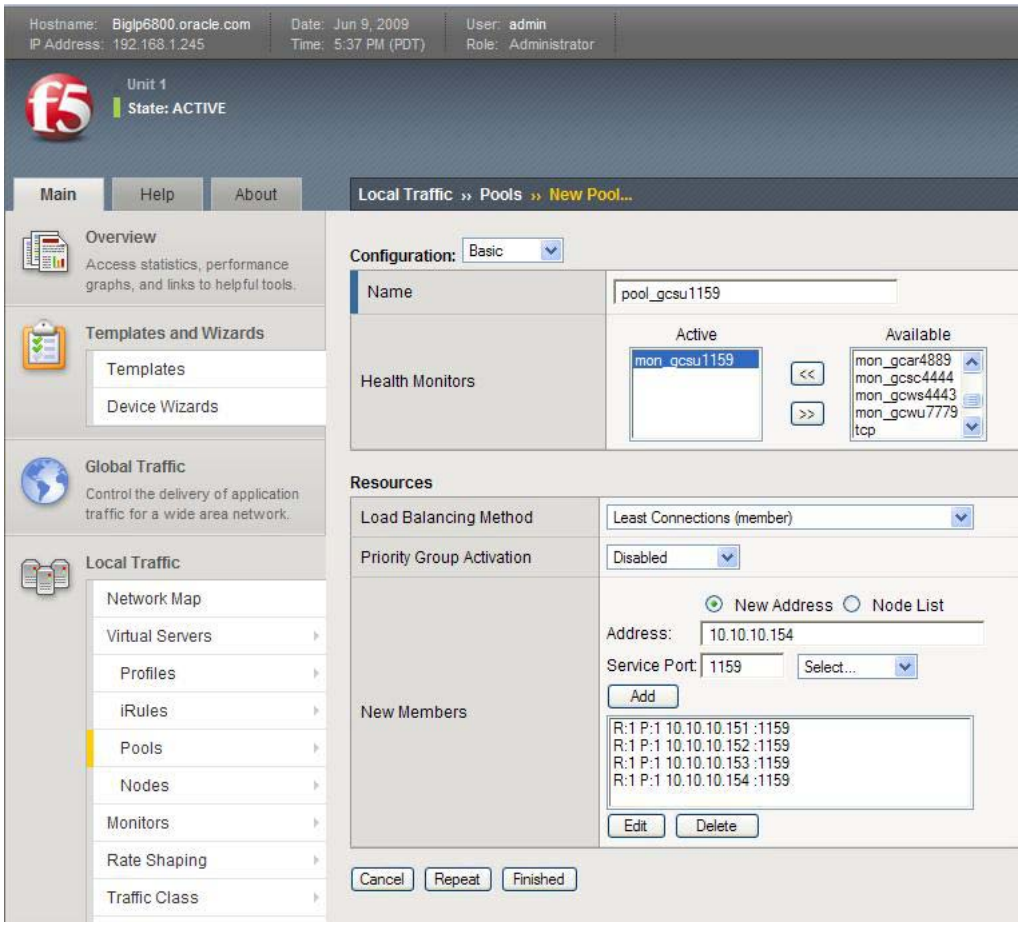
2. In the **Name** field, enter a unique name for your pool. In the MAA example, we entered **pool_gcsu1159**.
3. In the **Health Monitors** section, select the name of the monitor you created in the "Configure the Secure Upload health monitor step", and click **Add** (**<<**).

   In the MAA example, we select **mon_gcsu1159**.
4. 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 the MAA example, we select **Least Connections (member)**.
5. For this pool, keep the Priority Group Activation at **Disabled**.
6. In the New Members section, make sure the **New Address** option is selected.
7. In the **Address** field, add the first server to the pool.

   The MAA example uses **10.10.10.151.**
8. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

   The MAA example uses **1159**.
9. Click **Add** to add the member to the list.
10. Repeat steps 8 through 10 for each server that you want to add to the pool.
11. In the MAA example, we repeated these steps three times for the remaining servers: **10.10.10.152, 10.10.10.153, and 10.10.10.154**.
12. Click **Finished**.



Step 4: Create the virtual server

Perform the following steps to configure a Secure Upload virtual server that references the monitor, profiles, and pool you created in the preceding steps:

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 **Create**.

   The New Virtual Server screen opens.

3. In the **Name** field, enter a unique name for this virtual server.

   In the MAA example, we entered **vs_gcsu1159**.

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

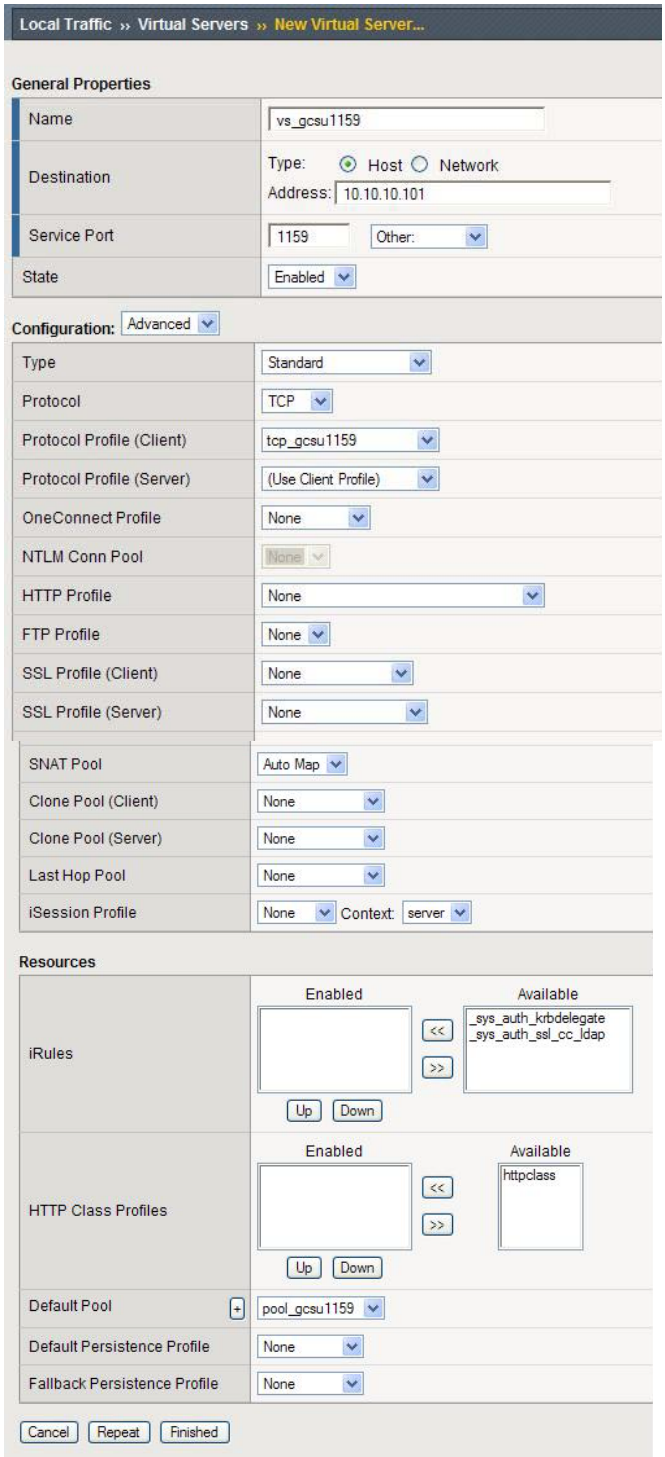
5. In the **Address** field, enter the IP address of this virtual server.

In the MAA example, we used **10.10.10.101**.

6. In the **Service Port** field, enter **1159**.
7. From the Configuration list, select **Advanced**.

   The Advanced configuration options display.
8. Keep the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the "Create a TCP profile for Secure Upload" section. In the MAA example, we selected **tcp_gcsu1159**.
10. Keep the **Protocol Profile (Server)** option at the default setting.
11. Change the **SNAT Pool** setting to **Automap**.
12. In the Resources section, from the **Default Pool** list, select the pool you created in the "Create the pool for Secure Upload" section.

    In the MAA example, we selected **pool_gcsu1159**.
13. Click **Finished**.


Local Traffic ›› Virtual Servers ›› New Virtual Server...
General Properties
Name
vs_gcsu1159
Destination
Type: Host Network
Address: 10.10.10.101
Service Port
1159
Other:
State
Enabled
Configuration: Advanced
Type
Standard
Protocol
TCP
Protocol Profile (Client)
tcp_gcsu1159
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
None
FTP Profile
None
SSL Profile (Client)
None
SSL Profile (Server)
None
SNAT Pool
Auto Map
Clone Pool (Client)
None
Clone Pool (Server)
None
Last Hop Pool
None
iSession Profile
None
Context:
server
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
<<
>>
Up
Down
HTTP Class Profiles
Enabled
Available
httpclass
<<
>>
Up
Down
Default Pool
pool_gcsu1159
Default Persistence Profile
None
Fallback Persistence Profile
None
Cancel
Repeat
Finished

Configure BIG-IP for Agent Registration (Port 4889)

Use the following procedure as a template for configuring F5 to support the Agent Registration Service for the OMS system. This procedure uses entries from the Monitor Port (Monitor Type) column in Table 1.

Step 1: Configure a health monitor for the Agent Registration service

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

   The Monitors screen opens.

2. On the Monitors screen, click **Create**.

   The New Monitor screen opens.

3. In the **Name** field, enter a unique name for this Monitor. For example: **mon_gcar4889**.

4. From the **Type** list, select the monitor type found in the **Monitor Port (Monitor Type)** column in parenthesis. Select **HTTP**. The Monitor configuration options display.

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

6. In the **Configuration** section, enter values in the **Interval** and **Timeout** fields:

   - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   The MAA example sets Interval to 60 and Timeout to 181.

7. In the Send String field, add a Send String, as follows:

   ```
   GET /em/genwallet HTTP/1.0
   ```

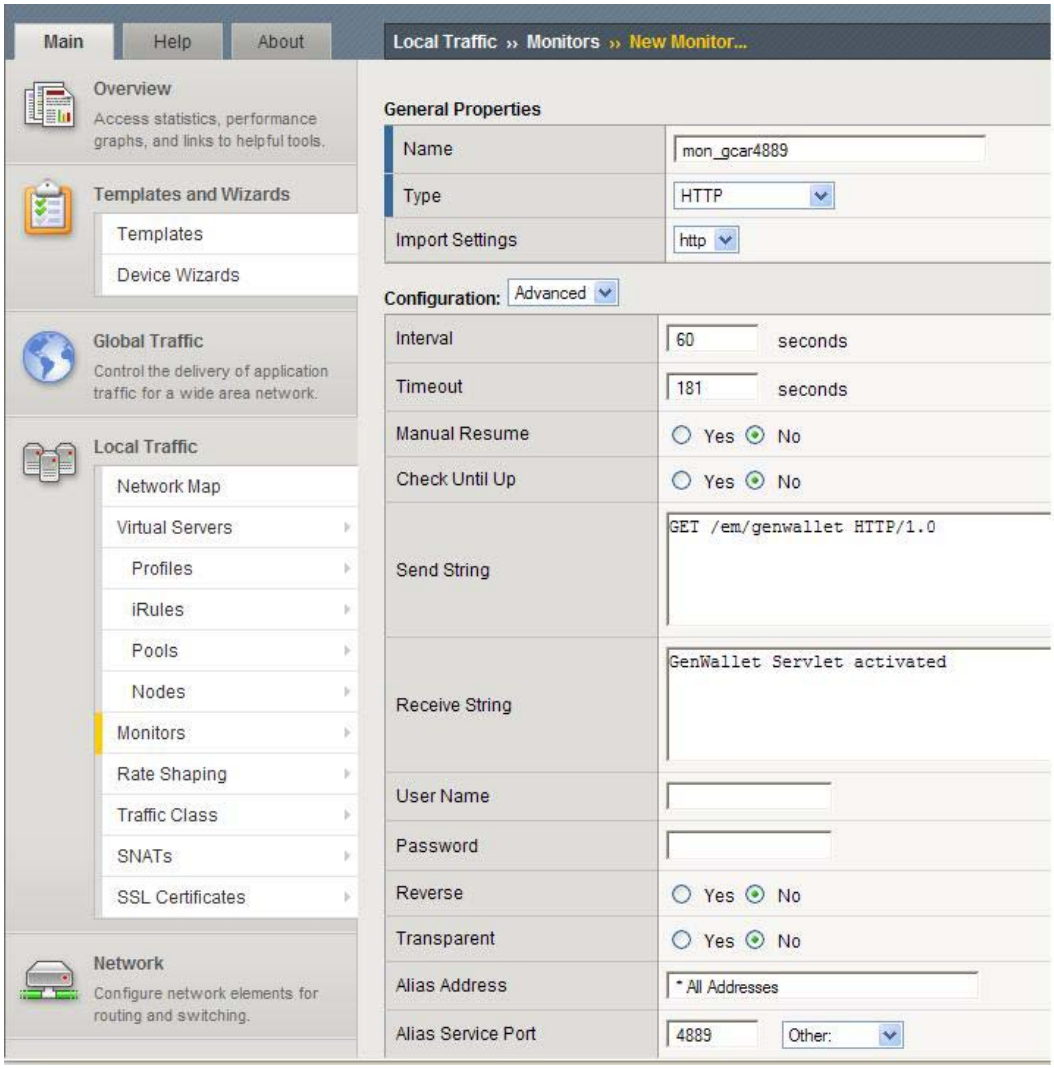
8. In the Receive String field, add a Receive String, as follows:

   ```
   GenWallet Servlet activated
   ```

9. In the **Alias Service Port** field, enter **4889**.

   All other configuration settings are optional.

10. Click **Finished**.



Step 2: Create the TCP profile for the Agent Registration service

In our MAA example, we base the TCP profile on the default TCP profile, and keep all the options at their default settings. You can configure these options, as appropriate, for your network.

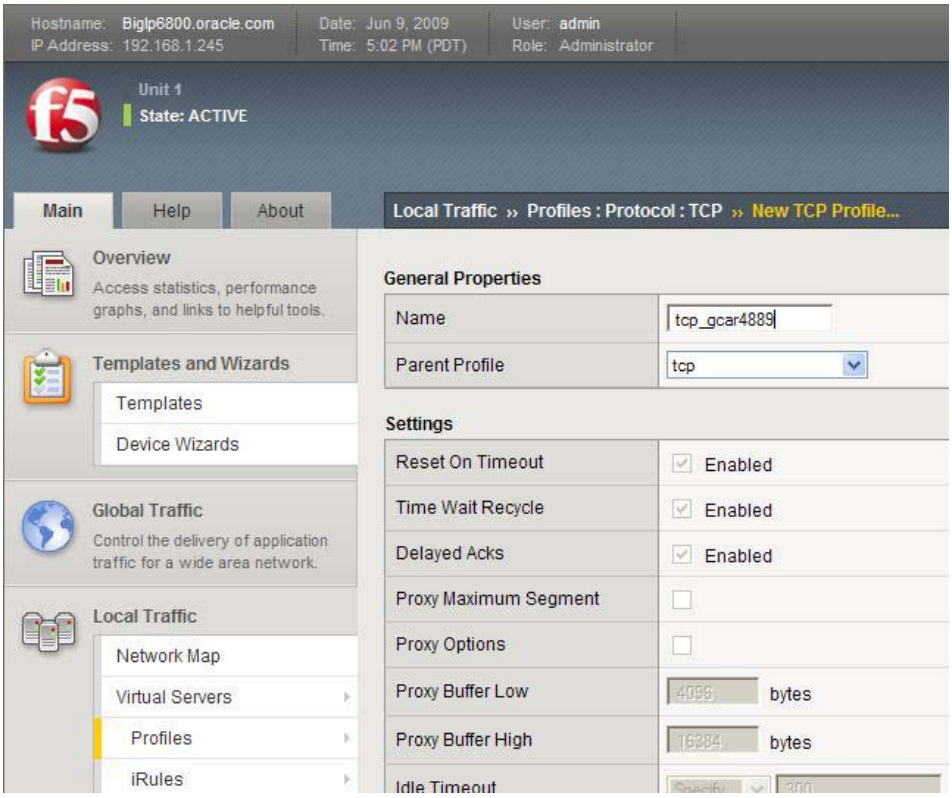
To create a new TCP profile for the Agent Registration service:

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

   The HTTP Profiles screen opens.

3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

   The New TCP Profile screen opens.
5. In the **Name** field, enter a unique name for this profile. For example: **`tcp_gcar4889`**.
6. If needed, modify as applicable for your network. See the F5 online help for more information about the configuration options. Note that the MAA example keeps the settings at their default levels.
7. Click **Finished**.



Step 3: Create a cookie persistence profile

When creating a Cookie Persistence profile, the best practice recommendation is to use the default cookie method for this profile (**HTTP cookie insert**).

To create a new cookie persistence profile based on the default 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 **Create**.

   The New Persistence Profile screen opens.

4. In the **Name** field, enter a name for this profile.

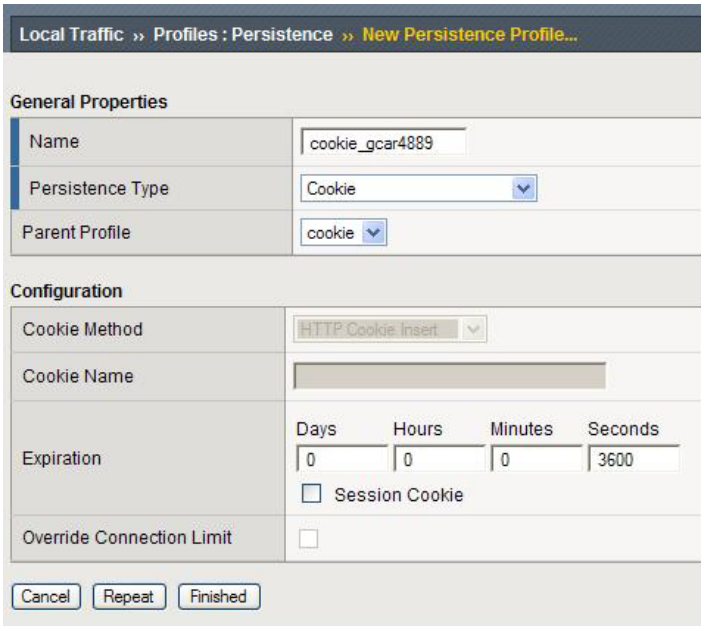
   In the MAA example, we entered **cookie_gcar4889**.

5. From the **Persistence Type** list, select **Cookie**.

   The configuration options for cookie persistence display.

6. Modify the cookie timeout value to **3600**.

7. Click **Finished**.



For more information about creating or modifying profiles or applying profiles in general, see the BIG-IP documentation listed in the References section.

Step 4: Create the pool for the Agent Registration

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In the MAA configuration, we created one pool for the Grid Control Agent Registration devices.

To create the Agent Registration 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 **Create**.

   The New Pool screen opens.

   Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings, as applicable, for your network.

3. In the **Name** field, enter a unique name for your pool.

   In the MAA example, we entered **pool_gcar4889**.

4. In the **Health Monitors** section, select the name of the monitor you created in the "Creating the Agent Registration health monitor step", and click the **Add (<<)** button.

   In the MAA example, we selected **mon_gcar4889**.

5. 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 the MAA example, we selected **Least Connections (member)**.

6. For this pool, keep the Priority Group Activation at **Disabled**.

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

8. In the **Address** field, add the first server to the pool.

   In the MAA example, we entered **10.10.10.15**.

9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

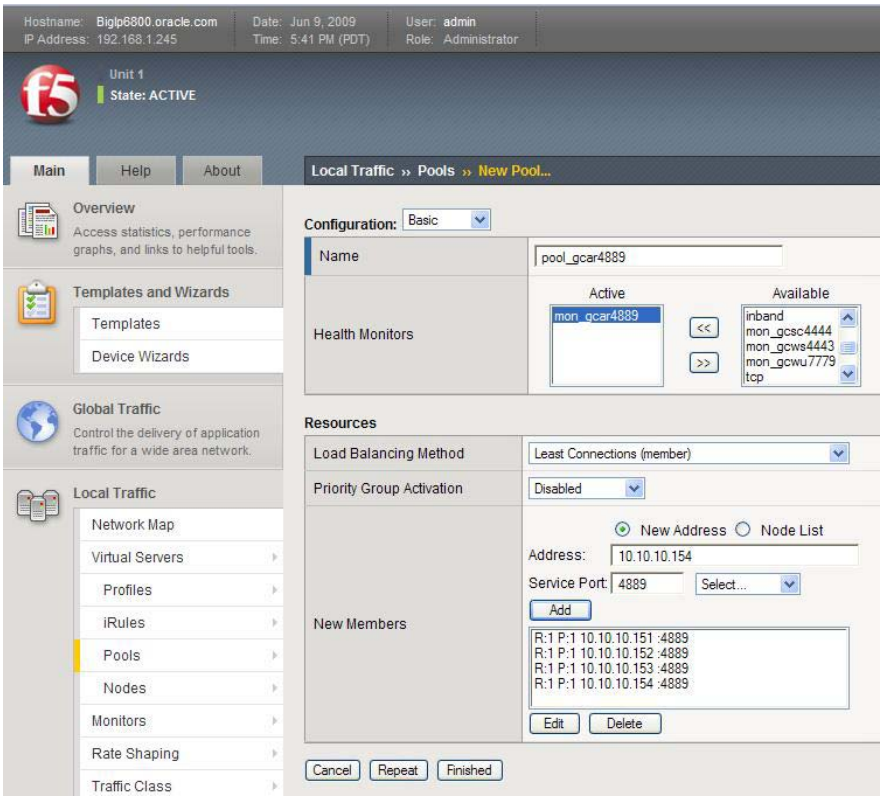
   In the MAA example, we entered **4889**.

10. Click **Add** to add the member to the list.

11. Repeat steps 8 through 10 for each server you want to add to the pool.

    In the MAA example, we repeated these steps three times for the remaining servers, 10.10.10.152, **10.10.10.153**, and **10.10.10.154**.

12. Click **Finished**.



Step 5: Create the Agent Registration virtual server

To configure an Agent Registration virtual server that references the monitor, profiles, persistence, and pool you created in the preceding procedures, perform the following steps:

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 **Create**.

   The New Virtual Server screen opens.

3. In the **Name** field, enter a unique name for this virtual server.

   In the MAA example, we entered **vs_gcar4889**.

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

5. In the **Address** field, enter the IP address of this virtual server.

   In the MAA example, we used **10.10.10.101**.

6. In the **Service Port** field, enter **4889**.

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

   The Advanced configuration options display.

8. Keep the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating a TCP profile* section.

   In the MAA example, we selected **tcp_gcar4889**.

10. Keep the **Protocol Profile (Server)** option at the default setting.

11. Change the HTTP Profile to **HTTP**.

12. Change the SNAT Pool setting to **Automap**.

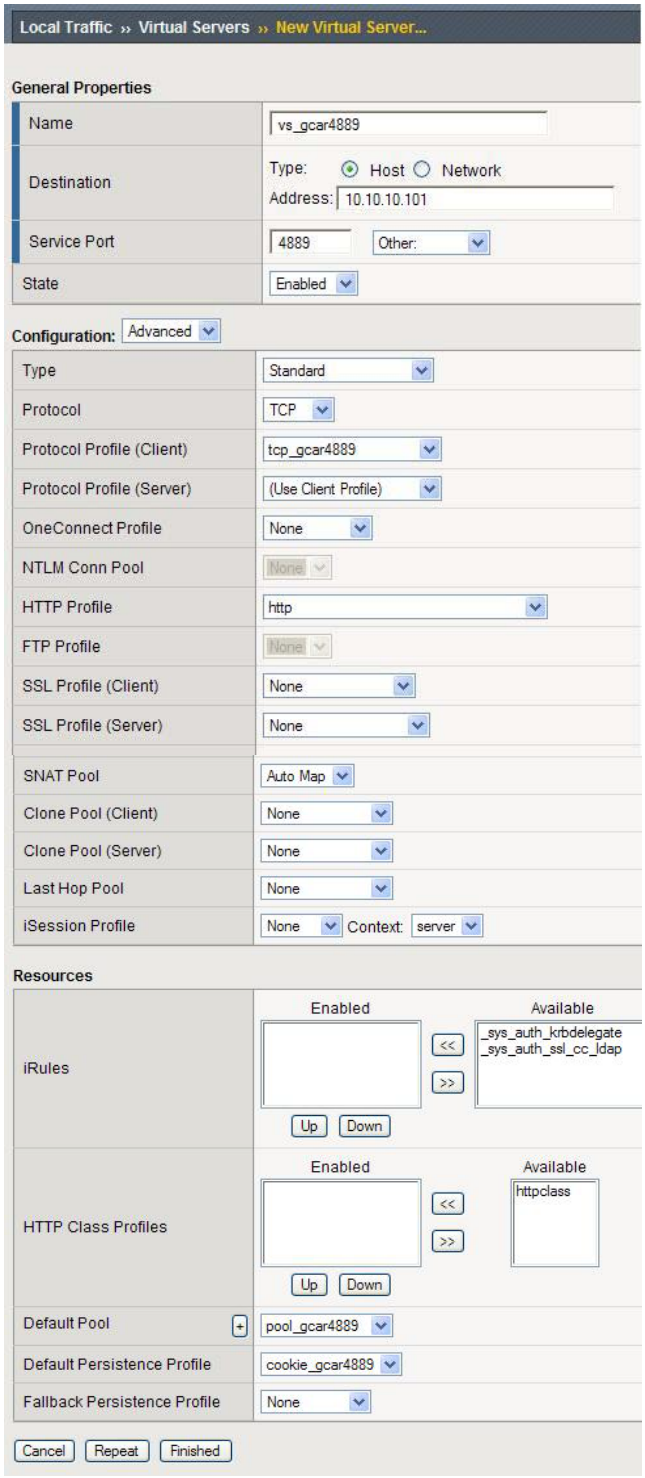
13. In the Resources section, from the **Default Pool** list, select the pool you created in the "Creating the pool for the Agent Registration" step.

    In the MAA example, we selected **pool_gcar4889**.

14. From the **Default Persistence Profile** list, select the persistence profile you created in the "Creating a cookie persistence profile for the Agent Registration" step.

    In the MAA example, we selected **cookie_gcar4889**.

15. Click **Finished**.


Local Traffic ›› Virtual Servers ›› New Virtual Server...
General Properties
Name
vs_gcar4889
Destination
Type: Host Network
Address: 10.10.10.101
Service Port
4889
Other:
State
Enabled
Configuration: Advanced
Type
Standard
Protocol
TCP
Protocol Profile (Client)
tcp_gcar4889
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
http
FTP Profile
None
SSL Profile (Client)
None
SSL Profile (Server)
None
SNAT Pool
Auto Map
Clone Pool (Client)
None
Clone Pool (Server)
None
Last Hop Pool
None
iSession Profile
None
Context:
server
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
<<
>>
Up
Down
HTTP Class Profiles
Enabled
Available
httpclass
<<
>>
Up
Down
Default Pool
pool_gcar4889
Default Persistence Profile
cookie_gcar4889
Fallback Persistence Profile
None
Cancel
Repeat
Finished

Configure BIG-IP for Secure Console (Port 4444)

Use the step-by-step procedure in this section as a template for configuring the F5 BIG-IP to support the Secure Console Service for the OMS system.

Step 1: Configure a health monitor for the Secure Console service

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

   The Monitors screen opens.

2. Click **Create**.

   The New Monitor screen opens.

3. In the **Name** field, enter a unique name for this Monitor. For example, enter **mon_gcsc4444**.

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

   The Monitor configuration options display.

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

6. In the **Configuration** section, enter values in **Interval** and **Timeout** fields:

   - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   The MAA example sets Interval to 60 and Timeout to 181.

7. In the **Send String** field, add a Send String as follows:

   ```
   GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible;
   MSIE 6.0; Windows NT 5.0)
   ```

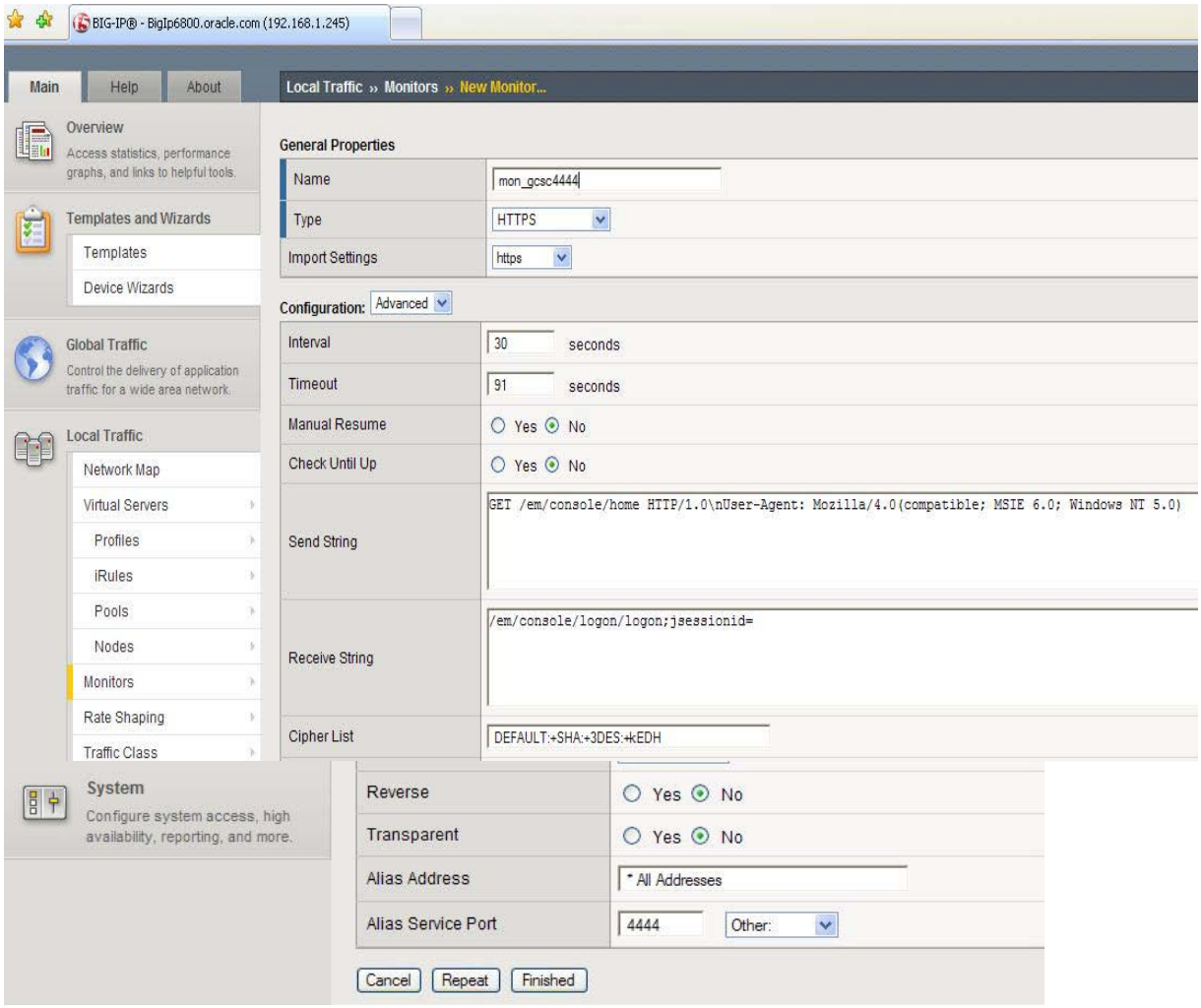
8. In the **Receive String** field, add a Receive String as follows:

   /em/console/logon/logon;jsessionid=

9. In the **Alias Service Port** field, enter **4444**.

   All other configuration settings are optional.

10. Click **Finished**.



Step 2: Create the TCP profile for the Secure Console service

In the following example, the TCP profile is based on the default TCP profile, and keeps all of the options at the default settings. You can configure these options, as appropriate, for your network.

To create a new TCP profile for the Secure Console service:

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

   The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.

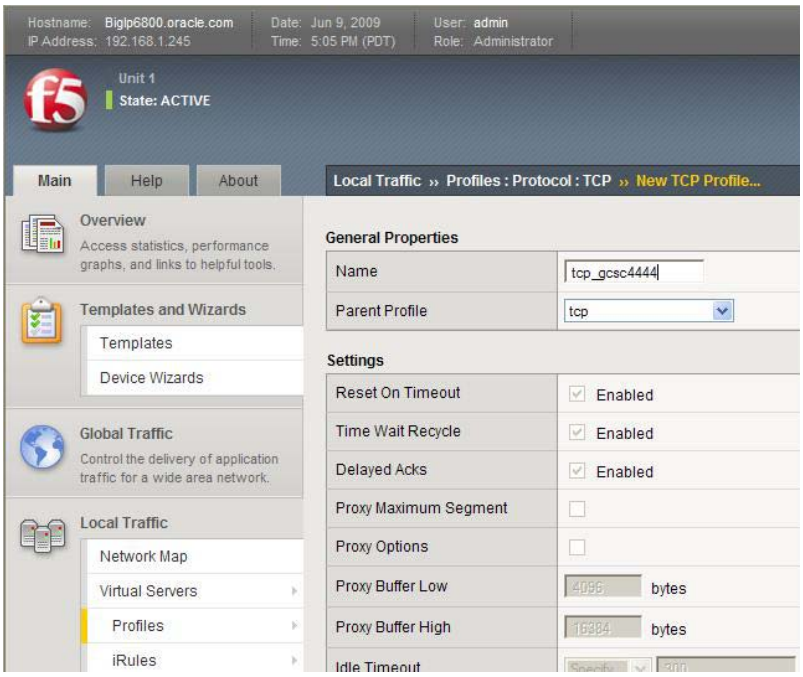
4. In the upper right portion of the screen, click **Create**.

   The New TCP Profile screen opens.

5. In the **Name** field, enter a unique name for this profile. For example: **tcp_gcsc4444**.

6. If needed, modify any of the settings as applicable for your network. See the F5 online help for more information on the configuration options. In the MAA example, we kept the settings at the default levels.

7. Click **Finished**.



Step 3: Create a ClientIP persistence profile for the Secure Console service

When creating the ClientIP Persistence profile, the best practice is to use the default SourceIP method for this profile.

To create a new ClientIP persistence profile based on the default 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**.

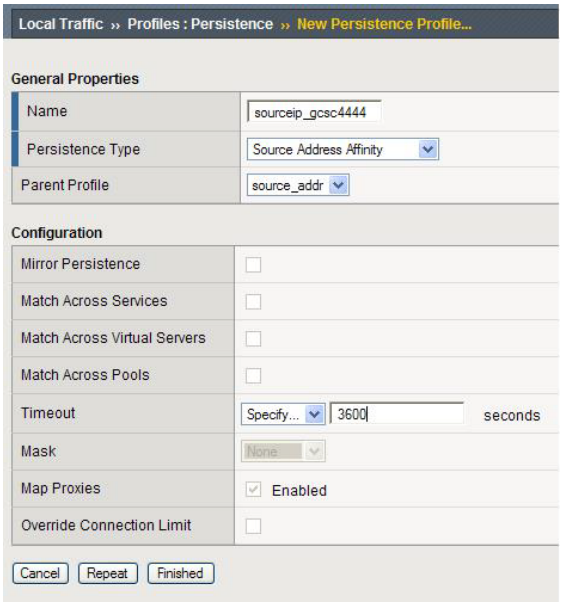
   The Persistence Profiles screen opens.

3. In the upper right portion of the screen, click **Create**.

4. The New Persistence Profile screen opens.

5. In the Name field, enter a unique name for this profile. For example, enter **sourceip_gcsc4444**.
6. From the Persistence Type list, select **Source Address Affinity**.

   The configuration options for SourceIP persistence display.
7. Modify the persistence timeout value to **3600**.
8. Click **Finished**.



For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation, which is listed in the References section.

Step 4: Create the pool for the Secure Console service

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control Secure Console devices.

To create the Secure Console 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 **Create**.

   The New Pool screen opens.

   Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings, as applicable, for your network.

3. In the **Name** field, enter a unique name for your pool.

   In the MAA example, we entered **pool_gcsc4444**.

4. In the **Health Monitors** section, select the name of the monitor you created in the "Creating the Secure Console health monitor" step, and click **Add (<<)**.

   In the MAA example, we selected **mon_gcsc4444**.

5. 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 the MAA example, we selected **Least Connections (member)**.

6. For this pool, we kept the Priority Group Activation **Disabled**.

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

8. In the **Address** field, add the first server to the pool.

   In the MAA example, we entered **10.10.10.151**

9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

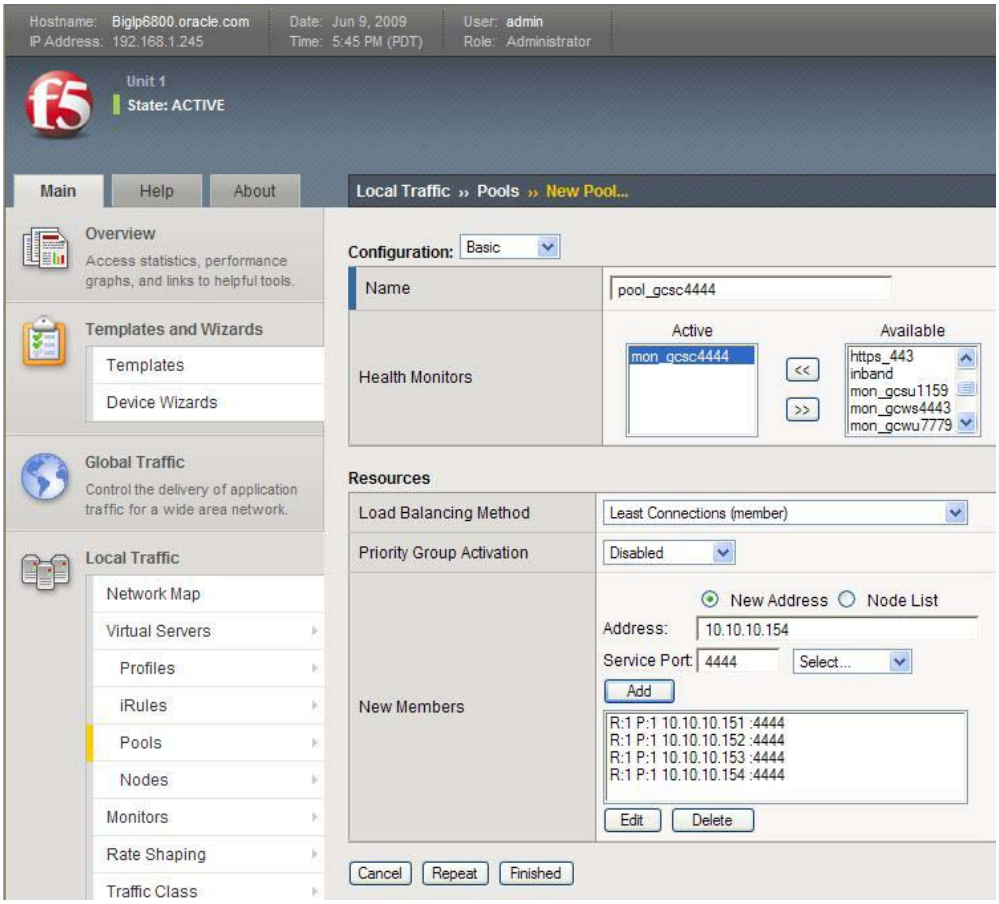
   In the MAA example, we entered **4444**.

10. Click **Add** to add the member to the list.

11. Repeat steps 8 through 10 for each server that you want to add to the pool.

    In the MAA example, we repeated these steps three times for the remaining servers, **10.10.10.152, 10.10.10.153, and 10.10.10.154**.

12. Click **Finished**.



Step 5: Create the Secure Console virtual server

This step configures a Secure Console virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures.

To create the 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** field, enter a unique name for this virtual server.

   In the MAA example, we entered **vs_gcsc4444**.

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

5. In the **Address** field, enter the IP address of this virtual server.

   In the MAA example, we used **10.10.10.101**.

6. In the **Service Port** field, enter **443**.

   Note: The virtual server is listening on port 443, but the Secure Console service is running on port 4444 on the OMS servers. You may need to change this virtual server port number, depending on the installation.

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

   The Advanced configuration options display.

8. Keep the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list select the name of the profile you created in the "Creating a TCP profile" step.

   In the MAA example, we selected **tcp_gcsc4444**.

10. Keep the **Protocol Profile (Server)** option at the default setting.

11. Change the SNAT Pool setting to **Automap**.

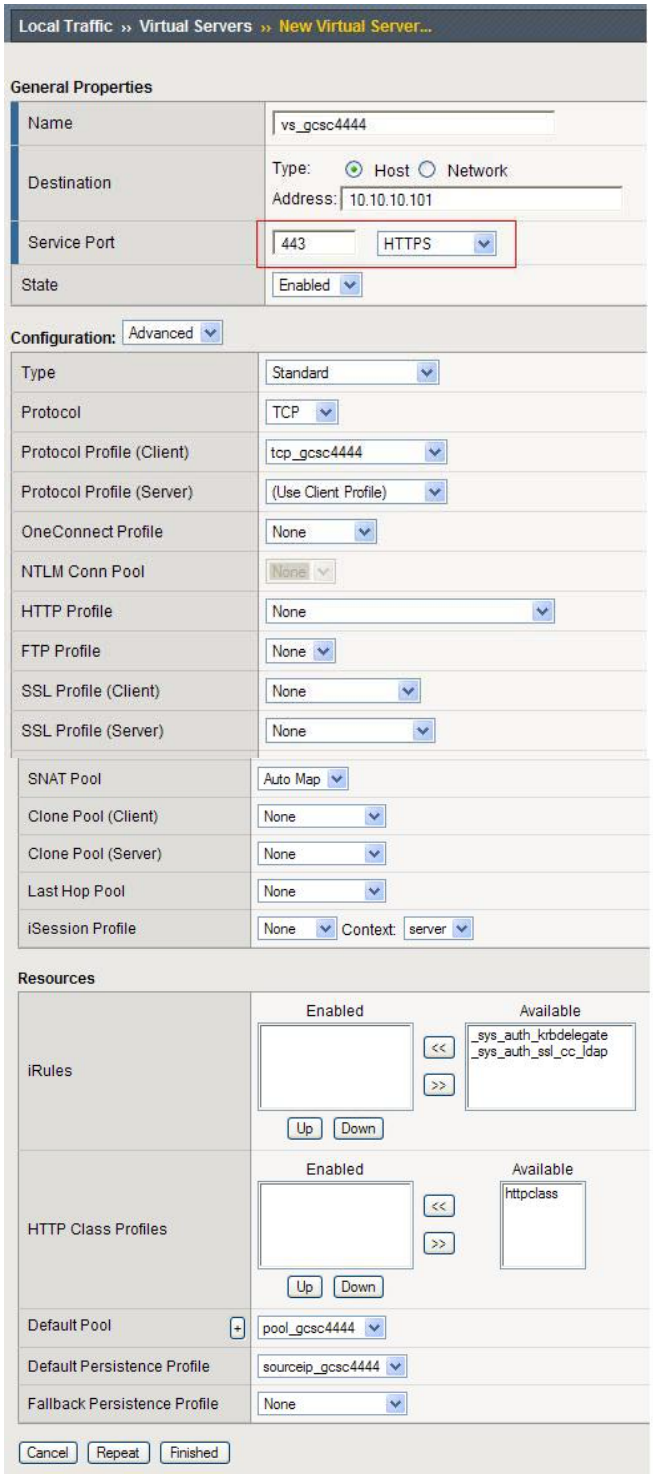
12. In the Resources section, from the **Default Pool** list, select the pool you created in the "Creating the pool" step.

    In the MAA example, we selected **pool_gcsc4444**.

13. From the **Default Persistence Profile** list, select the persistence profile you created in the "Creating a ClientIP persistence profile" step.

    In the MAA example, we selected **sourceip_gcsc4444**.

14. Click **Finished**.


Local Traffic ›› Virtual Servers ›› New Virtual Server...
General Properties
Name
vs_gcsc4444
Destination
Type: Host Network
Address: 10.10.10.101
Service Port
443
HTTPS
State
Enabled
Configuration: Advanced
Type
Standard
Protocol
TCP
Protocol Profile (Client)
tcp_gcsc4444
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
None
FTP Profile
None
SSL Profile (Client)
None
SSL Profile (Server)
None
SNAT Pool
Auto Map
Clone Pool (Client)
None
Clone Pool (Server)
None
Last Hop Pool
None
iSession Profile
None
Context:
server
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
<<
>>
Up
Down
HTTP Class Profiles
Enabled
Available
httpclass
<<
>>
Up
Down
Default Pool
pool_gcsc4444
Default Persistence Profile
sourceip_gcsc4444
Fallback Persistence Profile
None
Cancel
Repeat
Finished

Configure BIG-IP for Unsecure Console (Port 7777)

Use the step-by-step procedure in this section as a template for configuring the F5 BIG-IP to support the Unsecure Console Service for the OMS system.

> **Note:** The procedure to configure the Unsecure Console pool is for informational purposes only. The best practice is to route all traffic to and from Oracle Enterprise Manager in a secure fashion. Instead of configuring the Unsecure Console, Oracle recommends configuring the iRule (as described in the "Create Grid Control Unsecure Console Redirect iRule" step) to redirect all traffic to the secure port that was inadvertently sent to the unsecure pool.

Step 1: Create the Unsecure Console health monitor

The following procedure uses entries from the **Monitor Port (Monitor Type)** column shown in Table 1.

To configure a health monitor for the Unsecure Console service:

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

   The Monitors screen opens.

2. Click **Create**.

   The New Monitor screen opens.

3. In the **Name** field, enter a unique name for this Monitor. For example: **mon_gcuc7777**.

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

   The Monitor configuration options display.

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

6. In the **Configuration** section, enter values in the **Interval** and **Timeout** fields:

   - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   The MAA example sets Interval to 30 and Timeout to 91.

7. In the **Send String** field, add a Send String, as follows:

```
GET /em/console/home HTTP/1.0\nUser-Agent:
Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0)
```

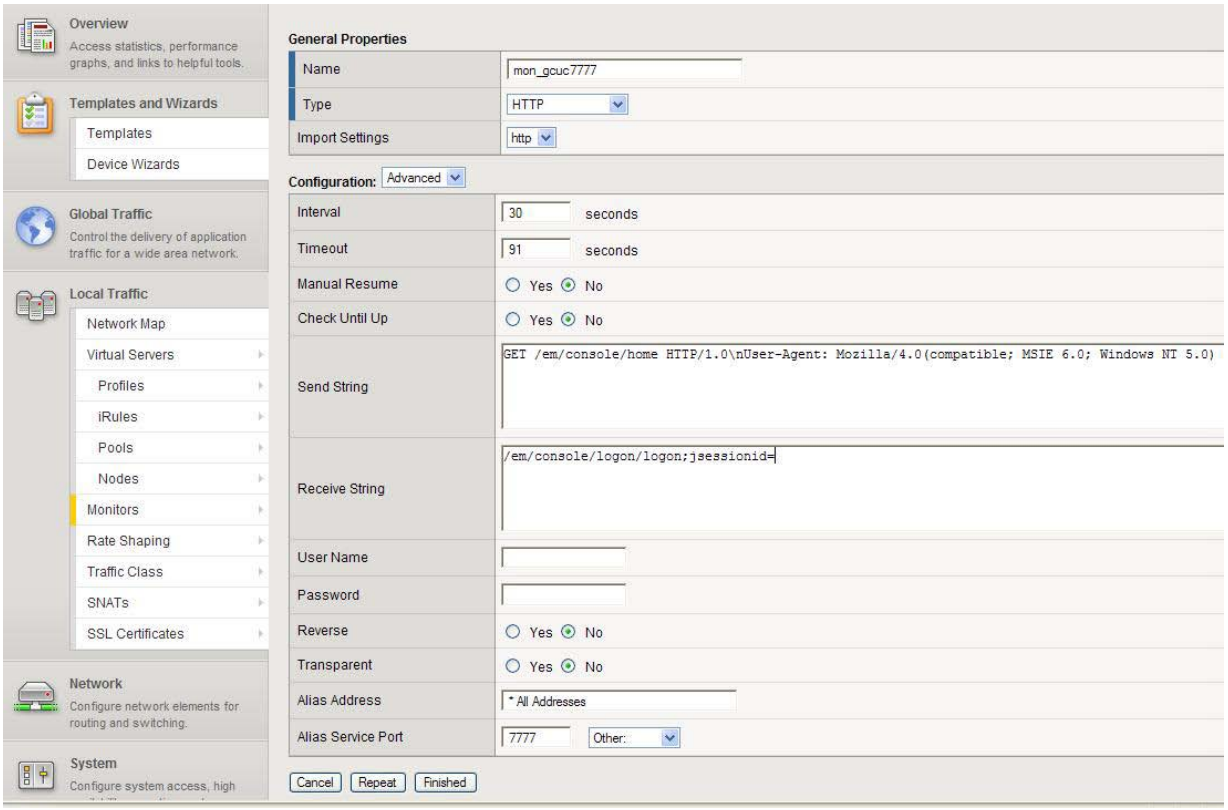
8. In the **Receive String** field, add a Receive String, as follows:

   ```
   /em/console/logon/logon;jsessionid=
   ```

9. In the **Alias Service Port** field, enter **7777**.

   All other configuration settings are optional.

10. Click **Finished**.



Step 2: Create a new TCP profile for the Unsecure Console service

In the MAA example, the TCP profile is based on the default TCP profile, and keeps all of the options set to their default values. You can configure these options, as appropriate, for your network.

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

   The HTTP Profiles screen opens.

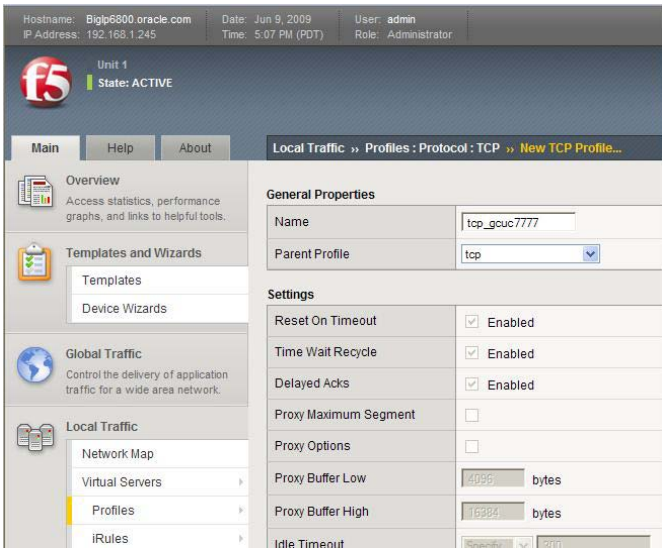
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

5. In the **Name** field, enter a unique name for this profile. For example: **tcp_gcuc7777**.

   If needed, modify the name appropriately for your network. See the F5 BIG-IP online help for more information about the configuration options. In the MAA example, we kept the settings at their default levels.

6. Click **Finished**.



Step 3: Create a ClientIP persistence profile for the Unsecure Console

When creating a ClientIP Persistence profile, the best practice is to use the default SourceIP method for this profile.

To create a new ClientIP persistence profile based on the default 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 **Create**.

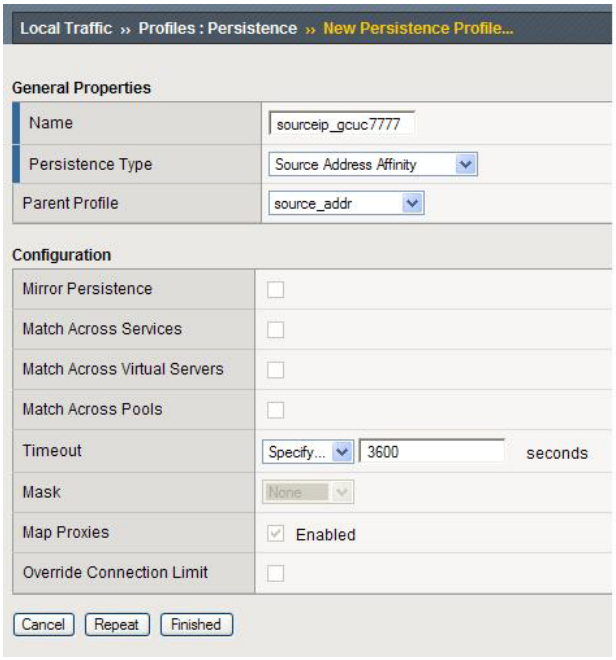
   The New Persistence Profile screen opens.

4. In the **Name** field, enter a unique name for this profile. In the MAA example, we entered **sourceip_gcuc7777**.

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

   The configuration options for persistence display.

6. Click **custom** (not shown) to activate the timeout column; Modify the persistence timeout value to **3600**.
7. Click **Finished**.



For more information about creating or modifying profiles, or applying profiles in general, see the F5 BIG-IP documentation listed in the References section.

Step 4: Create the Grid Control Unsecure Console Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and redirects them to the correct HTTPS (secure) virtual server, without user interaction. This Redirect iRule will be used on the Grid Control Unsecure Console virtual server, to redirect clients to the matching SSL Secured Console Service.

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 **Create**.

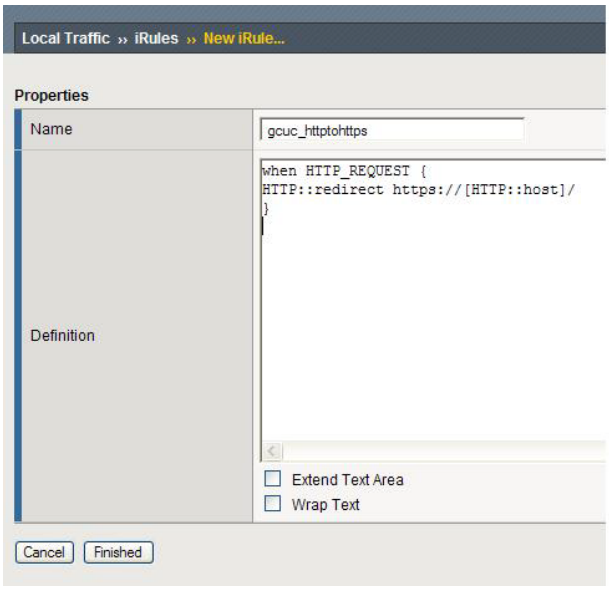
   The New iRule screen opens.
3. In the **Name** field, enter a name for your iRule.

In the MAA example, we used **gcuc_httptohttps**.

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

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host]/
}
```

5. Click **Finished**.



Step 5: Create the Unsecure Console pool

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control Unsecure Console devices.

To create the Unsecure Console 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.

   Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure the advanced settings appropriately for your network.

3. In the **Name** field, enter a unique name for your pool.

   In the MAA example, we entered **pool_gcuc7777**.

4. In the Health Monitors section, select the name of the monitor you created in the "Creating the Unsecure Console health monitor" step, and click **Add (<<)**.

   In the MAA example, we selected **mon_gcuc7777**.

5. 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 the MAA example, we selected **Least Connections (member)**.

6. For this pool, we kept the Priority Group Activation at **Disabled**.

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

8. In the **Address** field, add the first server to the pool.

   In the MAA example, we entered **10.10.10.151**.

9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

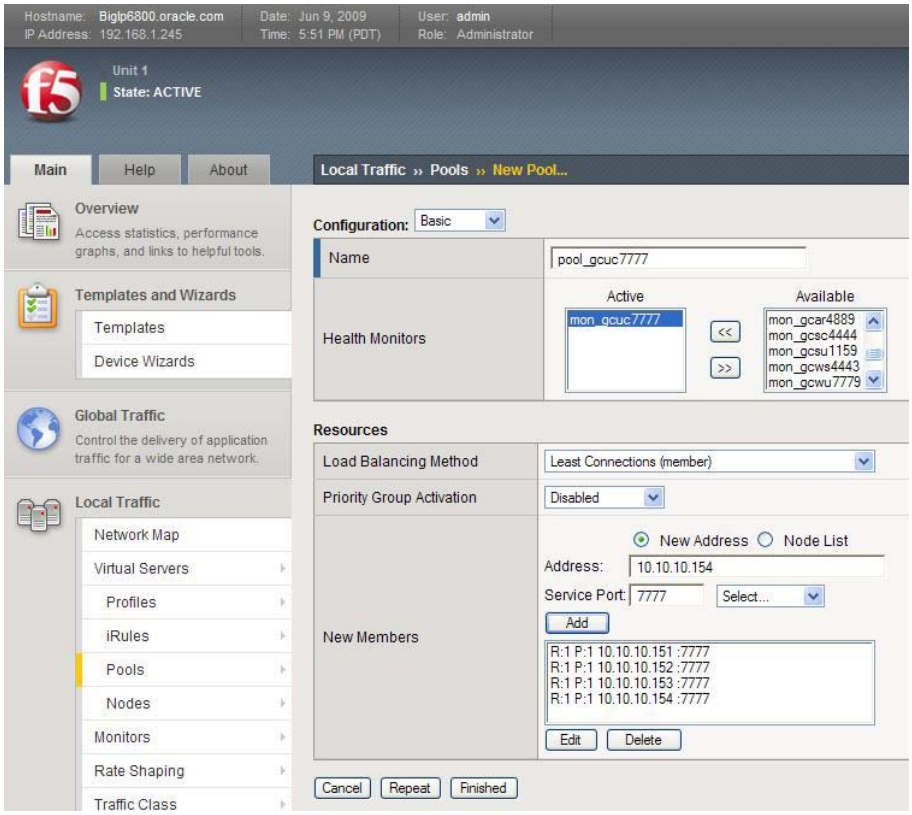
   In the MAA example, we entered **7777**.

10. Click **Add** to add the member to the list.

11. Repeat steps 8 through 10 for each server you want to add to the pool.

    In the MAA example, we repeated these steps three times for the remaining servers, **10.10.10.152**, **10.10.10.153**, and **10.10.10.154**.

12. Click **Finished**.



Step 6: Create the Unsecure Console virtual server

To configure an Unsecure Console virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures.

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 **Create**.

   The New Virtual Server screen opens.

3. In the **Name** field, enter a unique name for this virtual server.

   In the MAA example, we entered **vs_gcuc7777**.

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

5. In the **Address** field, enter the IP address of this virtual server.

   In the MAA example, we used **10.10.10.101**.

6. In the **Service Port** field, enter **7777**.

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

   The Advanced configuration options display.

8. Keep the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the "Creating a TCP profile" step. In the MAA example, we selected **tcp_gcuc7777**.

10. Keep the **Protocol Profile (Server)** option at the default setting.

11. Change the HTTP Profile to **http**.

12. Change the SNAT Pool setting to **Automap**.

13. In the Resources section, in the iRules **Available** list, select the iRule you created in the "Creating the iRule" step, and click **<<** to move it to the **Enabled** list.

    In the MAA example, we selected **gcuc_httptohttps**.

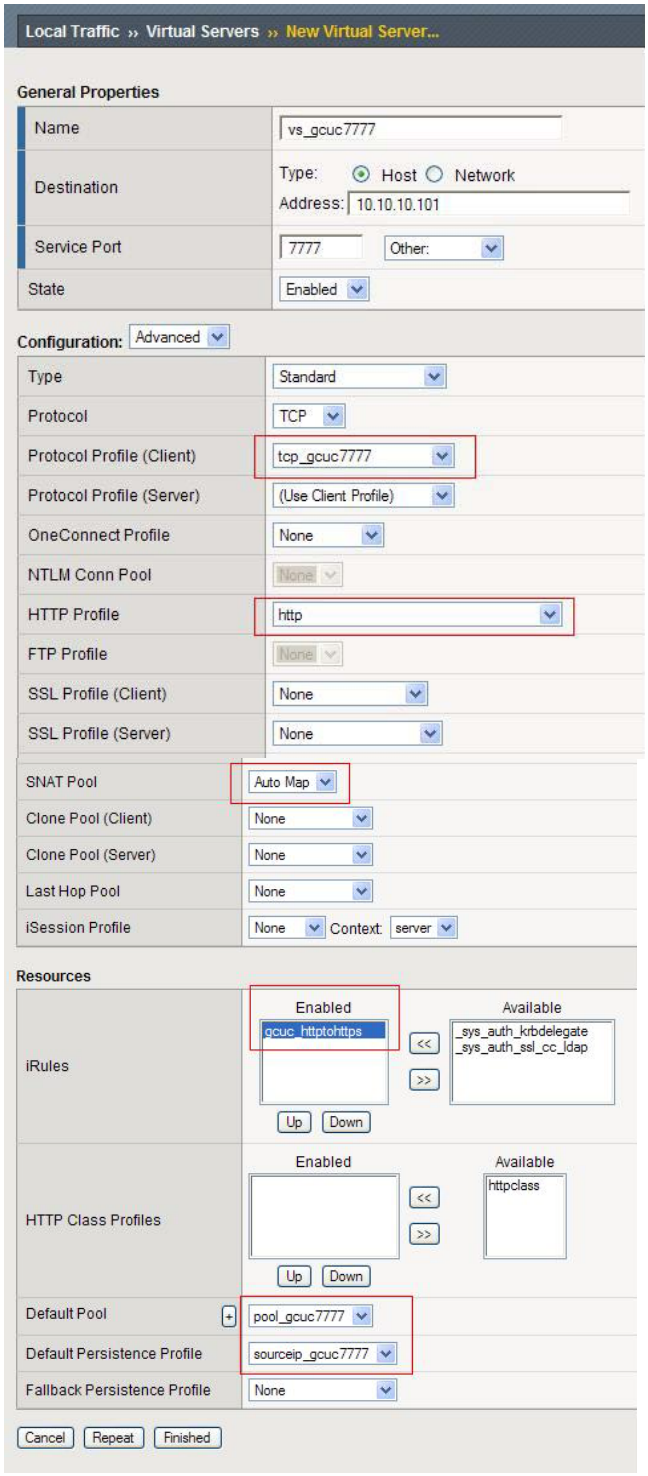
14. In the Resources section, from the **Default Pool** list, select the pool you created in the "Creating the pool" step.

    In the MAA example, we selected **pool_gcuc7777**.

15. From the **Default Persistence Profile** list, select the persistence profile you created in the "Creating a ClientIP persistence profile" step.

    In the MAA example, we selected **sourceip_gcuc7777**.

16. Click **Finished**.


Local Traffic ›› Virtual Servers ›› New Virtual Server...
General Properties
Name
vs_gcuc7777
Destination
Type: Host Network
Address: 10.10.10.101
Service Port
7777
Other:
State
Enabled
Configuration: Advanced
Type
Standard
Protocol
TCP
Protocol Profile (Client)
tcp_gcuc7777
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
http
FTP Profile
None
SSL Profile (Client)
None
SSL Profile (Server)
None
SNAT Pool
Auto Map
Clone Pool (Client)
None
Clone Pool (Server)
None
Last Hop Pool
None
iSession Profile
None
Context:
server
Resources
iRules
Enabled
gcuc_httptohttps
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
<<
>>
Up
Down
HTTP Class Profiles
Enabled
Available
httpclass
<<
>>
Up
Down
Default Pool
pool_gcuc7777
Default Persistence Profile
sourceip_gcuc7777
Fallback Persistence Profile
None
Cancel
Repeat
Finished

Configure BIG-IP for WebCache Secure (Port 4443)

Use the following step-by-step procedure as a template for configuring the F5 BIG-IP to support the WebCache Secure Service for the OMS system.

Step 1: Create the WebCache Secure health monitor

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

   The Monitors screen opens.

2. Click **Create**.

   The New Monitor screen opens.

3. In the **Name** field, enter a unique name for this Monitor. For example: **mon_gcws4443**.

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

   The Monitor configuration options display.

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

6. In the **Configuration** section, enter values in **Interval** and **Timeout** fields:

   - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   The MAA example sets Interval to 30 and Timeout to 91.

7. In the **Send String** field, add a Send String, as follows:

   ```
   GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible;
   MSIE 6.0; Windows NT 5.0)
   ```

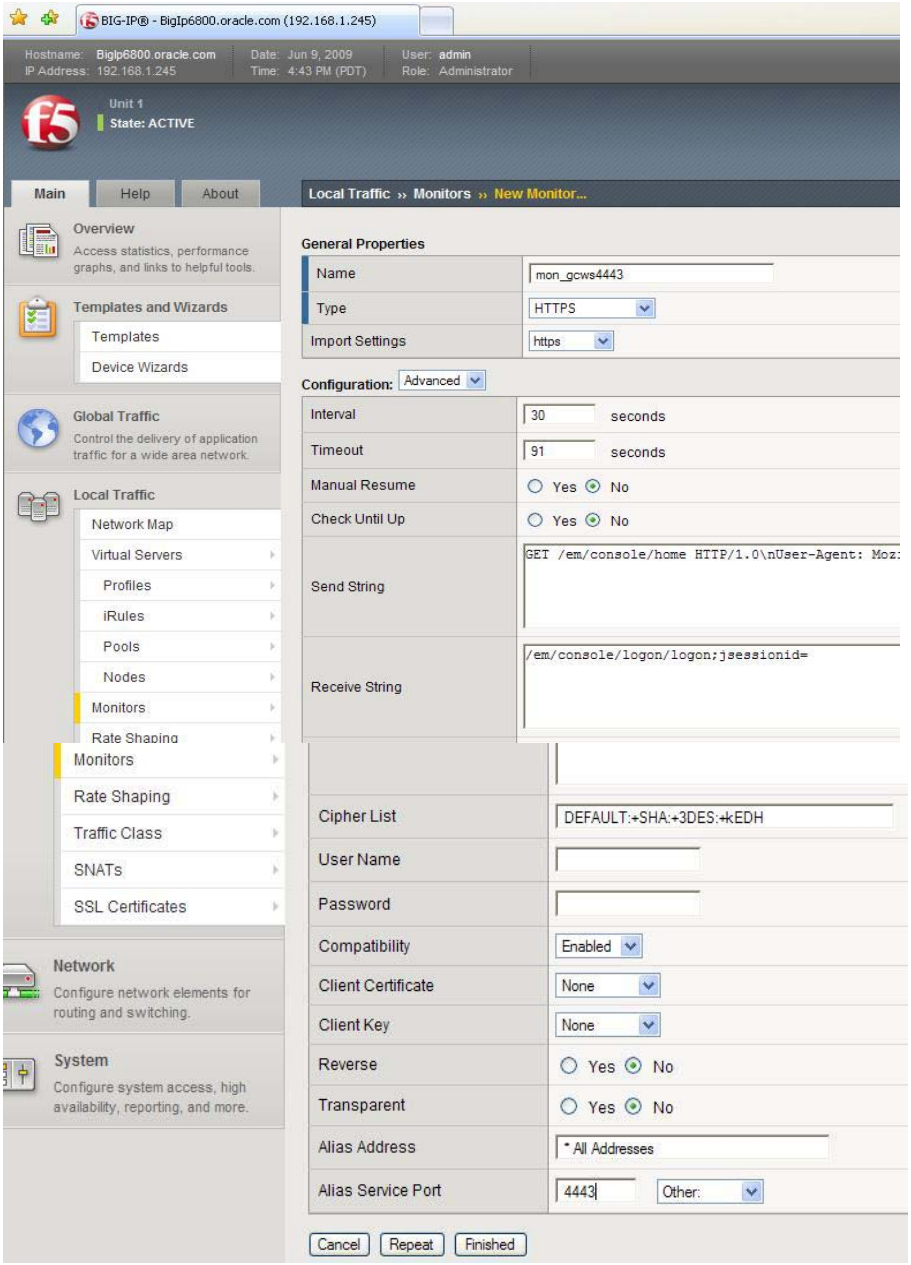
8. In the **Receive String** field, add a Receive String, as follows:

   ```
   /em/console/logon/logon;jsessionid=
   ```

9. In the **Alias Service Port** field, enter in **4443**.

   All other configuration settings are optional.

10. Click **Finished**.



Step 2: Create the TCP profile for WebCache Secure service

The following procedure bases the TCP profile on the default TCP profile, and keeps all of the options at their default settings. You can configure these options as appropriate for your network.

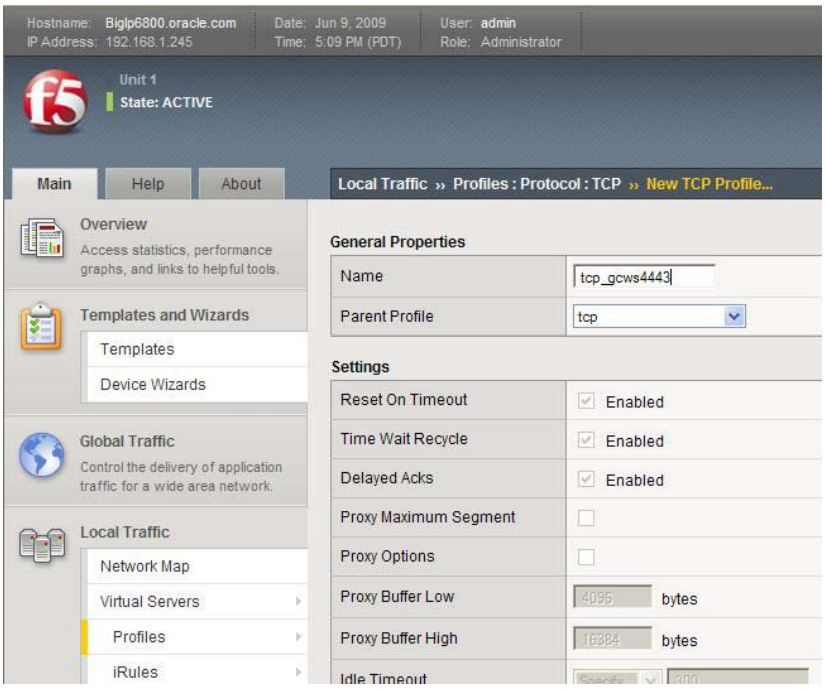
To create a new TCP profile for the WebCache Secure service:

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

   The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

   The New TCP Profile screen opens.
5. In the **Name** field, enter a unique name for this profile. For example: **tcp_gcws4443**.

   If needed, modify the name as applicable for your network. See the F5 BIG-IP online help for more information about the configuration options. In the MAA example, we kept the settings at the default levels.
6. Click **Finished**.



Step 3: Create a ClientIP persistence profile for the WebCache Secure service

When creating a ClientIP Persistence profile, the recommendation is to use the default SourceIP method for this profile, as follows:

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 **Create**.

   The New Persistence Profile screen opens.

4. In the **Name** field, enter a unique name for this profile.

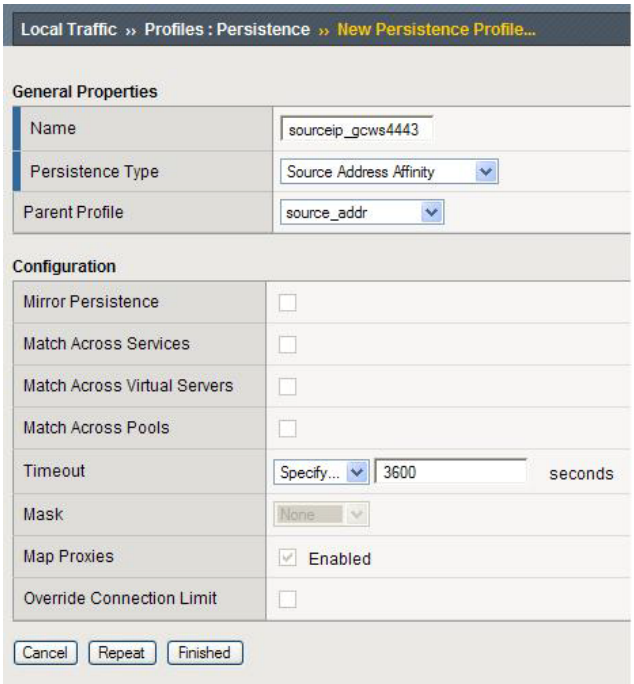
   In the MAA example, we entered **sourceip_gcws4443**.

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

   The configuration options for SourceIP persistence display.

6. Modify the persistence timeout value to **3600**.

7. Click **Finished**.



For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation resources listed in the References section.

Step 4: Create the pool for the WebCache Secure service

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control WebCache Secure devices.

To create the WebCache Secure 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 **Create**.

   The New Pool screen opens.

   Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings appropriately for your network.

3. In the **Name** field, enter a unique name for your pool.

   In the MAA example, we entered **pool_gcws4443**.

4. In the **Health Monitors** section, select the name of the monitor you created in the "Create the WebCache Secure health monitor" step, and click **Add (<<)**.

   In the MAA example, we selected **mon_gcws4443**.

5. 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 the MAA example, we selected **Least Connections (member)**.

6. For this pool, we keep the Priority Group Activation at **Disabled**.

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

8. In the **Address** field, add the first server to the pool.

   In the MAA example, we entered **10.10.10.151**.

9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

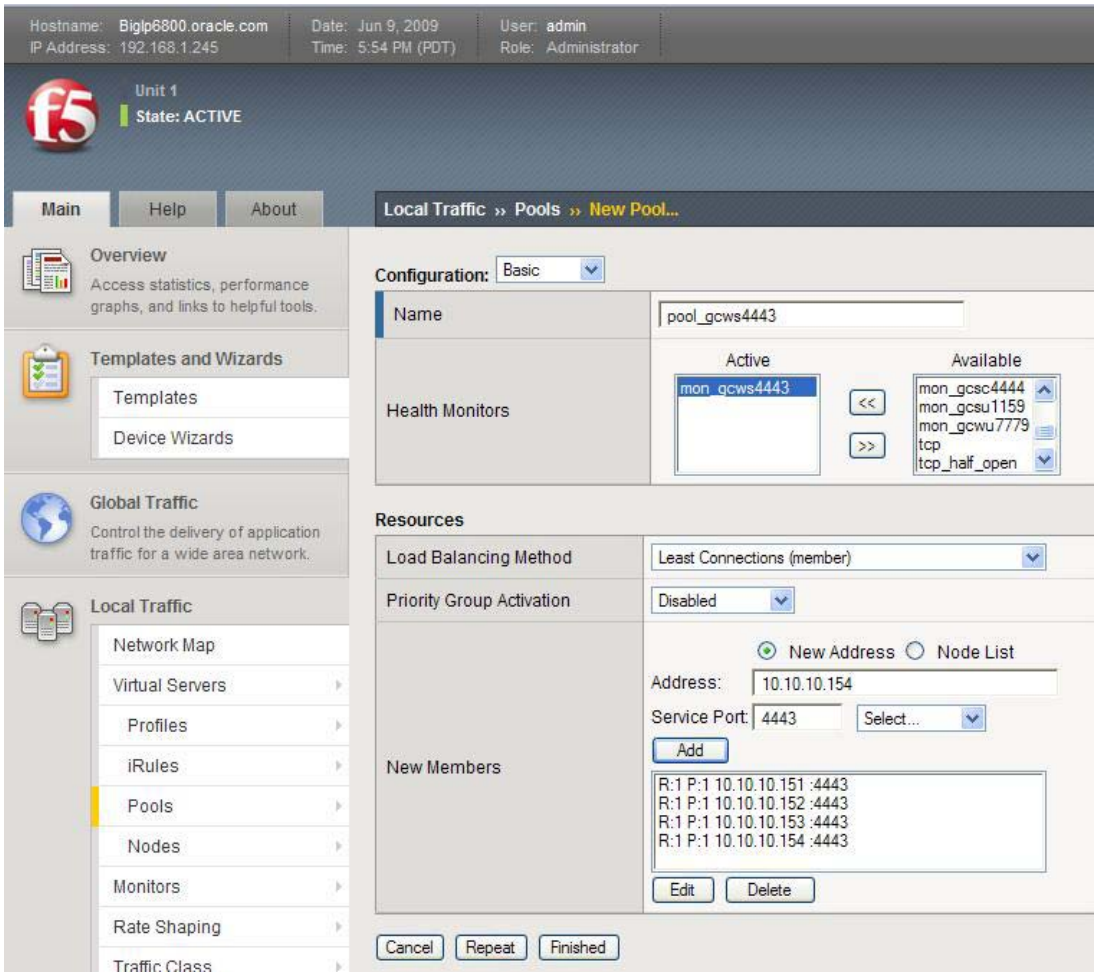
   In the MAA example, we entered **4443**.

10. Click **Add** to add the member to the list.

11. Repeat steps 8 through 10 for each server you want to add to the pool.

    In the MAA example, we repeated these steps three times for the remaining servers: **10.10.10.152, 10.10.10.153, and 10.10.10.154**.

12. Click **Finished**.



Step 5: Create the WebCache Secure virtual server

This step configures a WebCache Secure virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures.

To create the 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 **Create**.

   The New Virtual Server screen opens.

3. In the **Name** field, enter a unique name for this virtual server.

   In the MAA example, we entered **vs_gcws4443**.

4. In the **Destination** section, select the **Host** option.
5. In the **Address** field, enter the IP address of this virtual server.

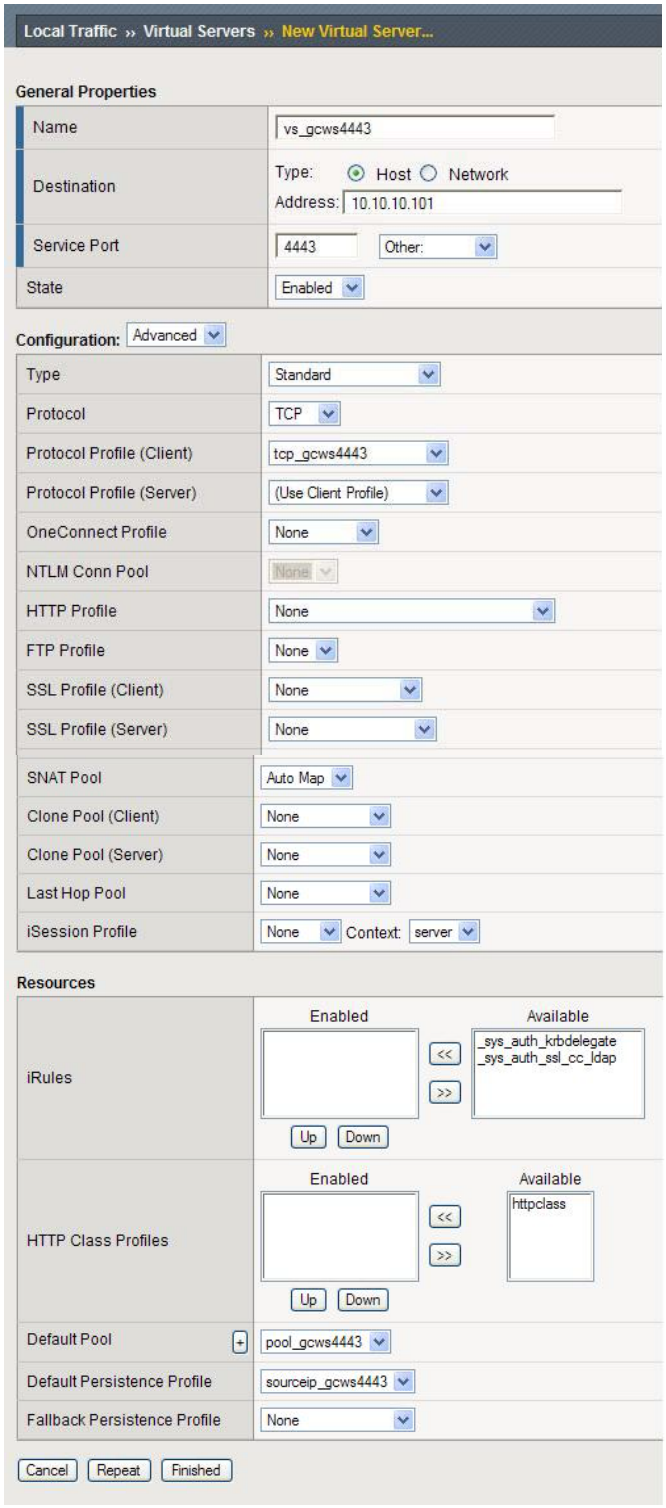
   In the MAA example, we used **10.10.10.101**.
6. In the **Service Port** field, enter **4443**.
7. From the Configuration list, select **Advanced**.

   The Advanced configuration options display.
8. Keep the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the "Create a TCP profile" step.

   In the MAA example, we selected **tcp_gcws4443**.
10. Keep the **Protocol Profile (Server)** option at the default setting.
11. Change the SNAT Pool setting to **Automap**.
12. In the Resources section, from the **Default Pool** list, select the pool you created in the "Creating the pool" step.

    In the MAA example, we selected **pool_gcws4443**.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the "Creating a ClientIP persistence profile" step.

    In the MAA example, we selected **sourceip_gcws4443**.
14. Click **Finished**.


Local Traffic ›› Virtual Servers ›› New Virtual Server...
General Properties
Name
vs_gcws4443
Destination
Type: Host Network
Address: 10.10.10.101
Service Port
4443
Other:
State
Enabled
Configuration: Advanced
Type
Standard
Protocol
TCP
Protocol Profile (Client)
tcp_gcws4443
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
None
FTP Profile
None
SSL Profile (Client)
None
SSL Profile (Server)
None
SNAT Pool
Auto Map
Clone Pool (Client)
None
Clone Pool (Server)
None
Last Hop Pool
None
iSession Profile
None
Context:
server
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
<<
>>
Up
Down
HTTP Class Profiles
Enabled
Available
httpclass
<<
>>
Up
Down
Default Pool
pool_gcws4443
Default Persistence Profile
sourceip_gcws4443
Fallback Persistence Profile
None
Cancel
Repeat
Finished

Configure BIG-IP for WebCache Unsecure (Port 7779)

Use the following procedures as a template for configuring the F5 BIG-IP to support the WebCache Unsecure Service for the OMS system.

Step 1: Create the WebCache Unsecure health monitor

This procedure uses entries from the **Monitor Port (Monitor Type)** column in the Table 1.

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

   The Monitors screen opens.

2. Click **Create**.

   The New Monitor screen opens.

3. In the **Name** field, enter a unique name for this Monitor. For example: **mon_gcwu7779**.

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

   The Monitor configuration options display.

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

6. In the **Configuration** section, enter values in **Interval** and **Timeout** fields:

   - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   The MAA example sets Interval to 30 and Timeout to 91.

7. In the **Send String** field, add a Send String, as follows:

   ```
   GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible;
   MSIE 6.0; Windows NT 5.0)
   ```

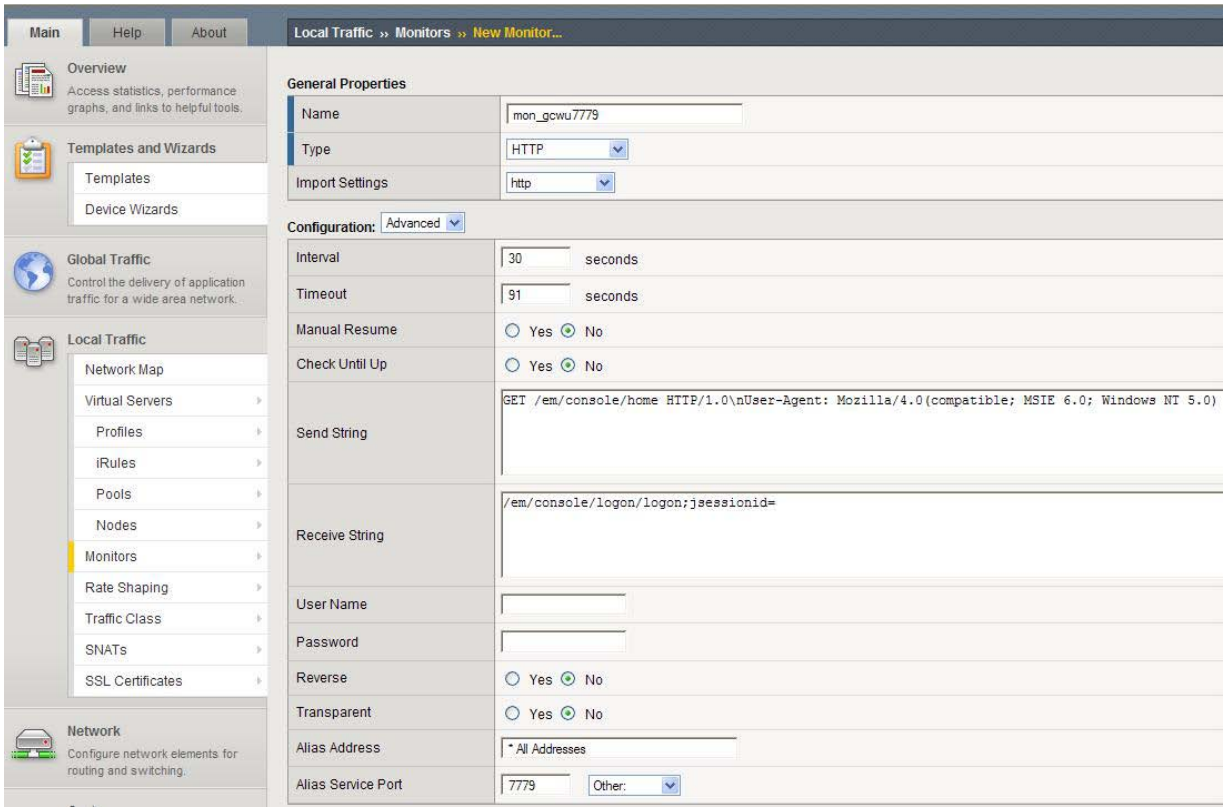
8. In the **Receive String** field, add a Receive String, as follows:

   ```
   /em/console/logon/logon;jsessionid=
   ```

9. In the **Alias Service Port** field, enter **7779**.

   All other configuration settings are optional.

10. Click **Finished**.



Step 2: Create the TCP profile for the WebCache Unsecure service

The following procedure bases the TCP profile on the default TCP profile, and keeps all of the options at their default settings. You can configure these options as appropriate for your network.

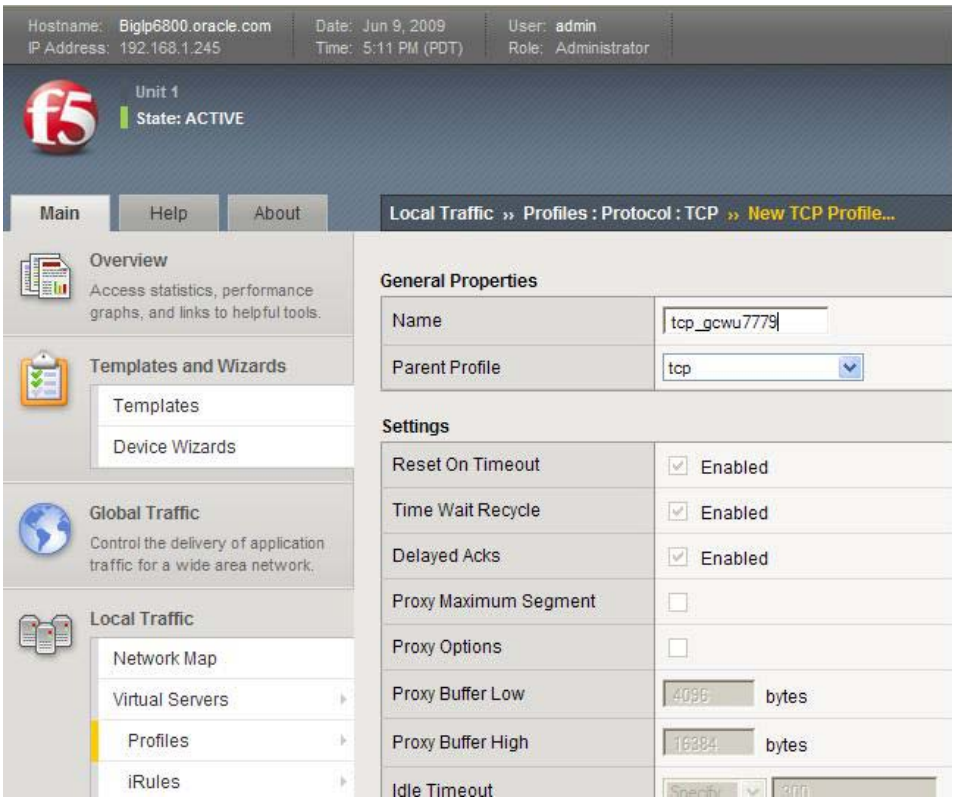
1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

   The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

   The New TCP Profile screen opens.
5. In the **Name** field, enter a unique name for this profile, For example: **tcp_gcwu7779**.

   If needed, modify the name, as applicable for your network. See the F5 BIG-IP online help for more information about the configuration options. In the MAA example, we kept the settings at their default levels.

6. Click **Finished**.



Step 3: Creating a ClientIP persistence profile for the WebCache Unsecure service

When creating a ClientIP Persistence profile, the recommendation is to use the default SourceIP method for this profile.

To create a new ClientIP persistence profile based on the default 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 **Create**.

   The New Persistence Profile screen opens.

4. In the **Name** field, enter a unique name for this profile.

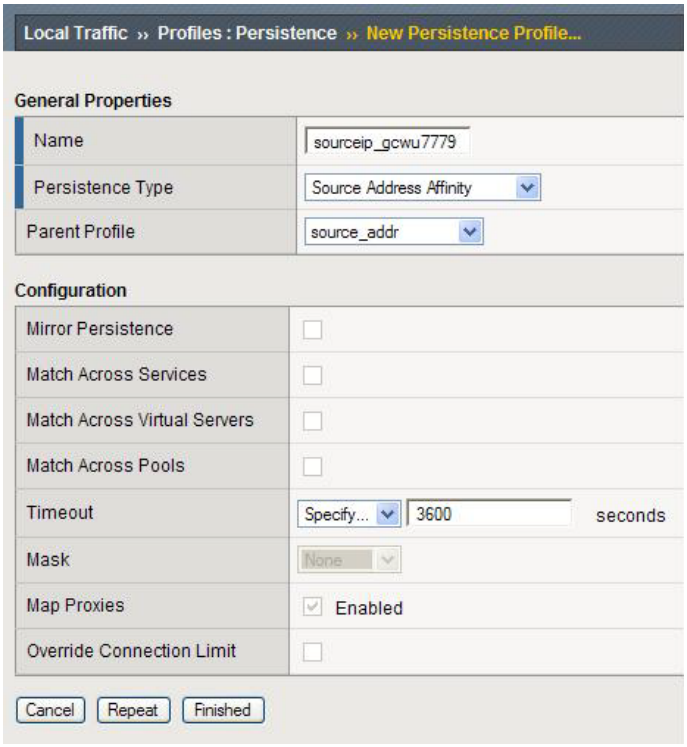
   In the MAA example, we used **sourceip_gcwu7779**.

5. From the **Persistence Type** list, select **SourceIP**.

   The configuration options for SourceIP persistence display.

6. Modify the persistence timeout value to **3600**.

7. Click **Finished**.



For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation that you can access by means of the References section.

Step 4: Creating the pool for the WebCache Unsecure service

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control WebCache Unsecure devices.

To create the WebCache Unsecure 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 **Create**.

   The New Pool screen opens.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.

3. In the **Name** field, enter a unique name for your pool.

   In the MAA example, we entered **pool_gcwu7779**.

4. In the **Health Monitors** section, select the name of the monitor you created in the "Creating the WebCache Unsecure health monitor" step, and click **Add (<<)**.

   In the MAA example, we selected **mon_gcwu7779**.

5. 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 the MAA example, we selected **Least Connections (member)**.

6. For this pool, we kept the Priority Group Activation as **Disabled**.

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

8. In the **Address** field, add the first server to the pool.

   In the MAA example, we used **10.10.10.151**.

9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

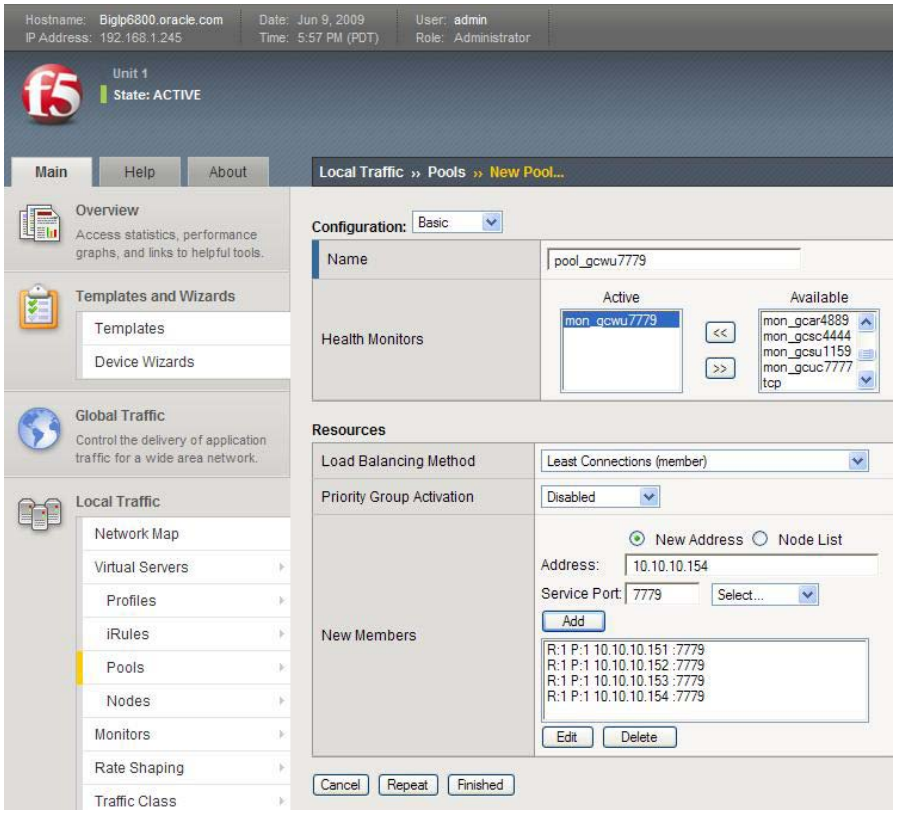
   In the MAA example, we entered **7779**.

10. Click **Add** to add the member to the list.

11. Repeat steps 8 through 10 for each server you want to add to the pool.

    In the MAA example, we repeated these steps three times for the remaining servers: **10.10.10.152, 10.10.10.153, and 10.10.10.154**.

12. Click **Finished**.



Step 5: Create the WebCache Unsecure virtual server

This step configures a WebCache Unsecure virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures

To create the 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** field, enter a unique name for this virtual server.

   In the MAA example, we entered **vs_gcwu7779**.

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

5. In the **Address** field, enter the IP address of this virtual server.

   In the MAA example, we used **10.10.10.101**.

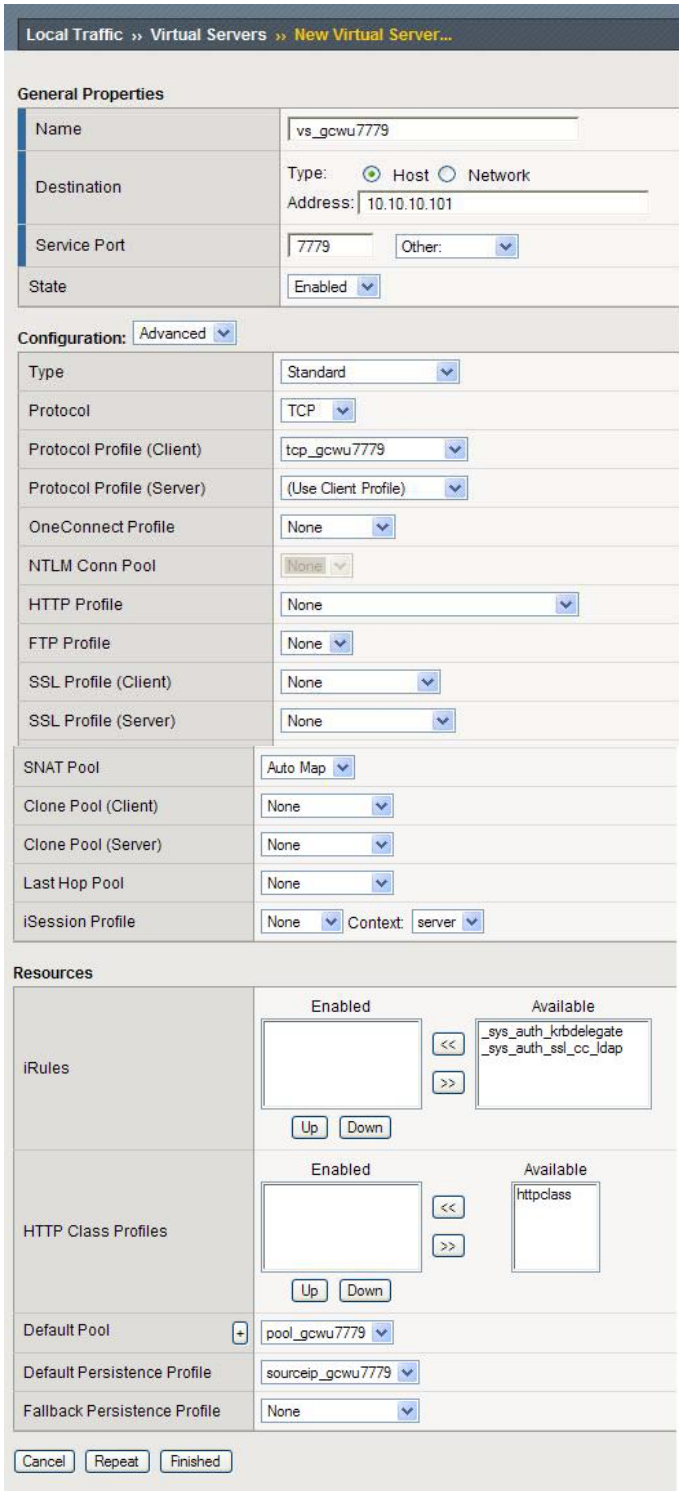
6. In the **Service Port** field, enter **7779**.
7. From the Configuration list, select **Advanced**.

   The Advanced configuration options display.
8. Keep the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list select the name of the profile you created in the "Creating a TCP profile" step.

   In the MAA example, we selected **tcp_gcwu7779**.
10. Keep the **Protocol Profile (Server)** option at the default setting.
11. Change the SNAT Pool setting to **Automap**.
12. In the **Resources** section, from the **Default Pool** list, select the pool you created in the "Creating the pool" step.

    In the MAA example, we selected **pool_gcwu7779**.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the "Create a ClientIP persistence profile" step.

    In the MAA example, we selected **sourceip_gcwu7779**.
14. Click **Finished**.


Local Traffic ›› Virtual Servers ›› New Virtual Server...
General Properties
Name
vs_gcwu7779
Destination
Type: Host Network
Address: 10.10.10.101
Service Port
7779
Other:
State
Enabled
Configuration: Advanced
Type
Standard
Protocol
TCP
Protocol Profile (Client)
tcp_gcwu7779
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
None
FTP Profile
None
SSL Profile (Client)
None
SSL Profile (Server)
None
SNAT Pool
Auto Map
Clone Pool (Client)
None
Clone Pool (Server)
None
Last Hop Pool
None
iSession Profile
None
Context:
server
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
<<
>>
Up
Down
HTTP Class Profiles
Enabled
Available
httpclass
<<
>>
Up
Down
Default Pool
pool_gcwu7779
Default Persistence Profile
sourceip_gcwu7779
Fallback Persistence Profile
None
Cancel
Repeat
Finished

Configuring Enterprise Manager for Use with F5 BIG-IP LTM

Oracle Enterprise Manager Architecture Overview

Oracle Enterprise Manager Middle tier framework is based on the Oracle Application Server 10*g* architecture and is comprised of the following components:

- Oracle HTTP Server (OHS)
- OC4J_EM
- OC4J_EMPROV
- WebCache
- dcm-daemon

The Oracle Management Service (OMS) application is contained in an OC4J container OC4J_EM, which handles a number of operations including console UI access servlet, agent upload receivelet, repository loader servlet, job dispatchers. The OMS application provides various services, each using its own protocol. To access the client and agent services, an OHS Web interface is integrated with each OMS.

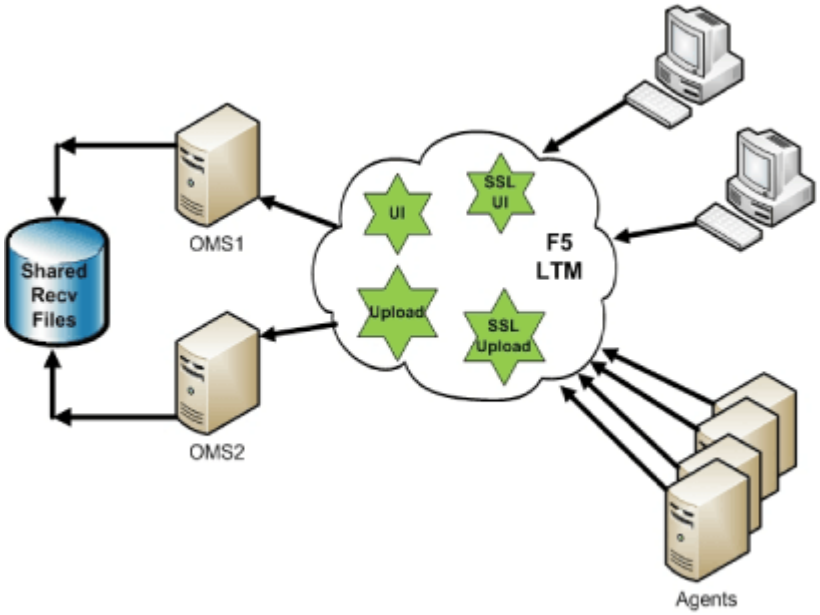
For the OMS to maintain service availability for its "clients" (the console UI and Management Agents), the following services minimally must be available:

- UI Access Services
  - SSL
  - Non-SSL
- Agent Upload Services
  - SSL
  - Non-SSL

In configurations with more than one OMS installed, a common OMS name must be established for Enterprise Manager Agents and Console UI. The F5 BIG-IP LTM will act as a single point of contact for these components, distributing the load to any available OMS. For more details about configuring Multiple OMS environments, see Chapter 17 in the *Oracle Enterprise Manager Grid Control Installation and Configuration Guide* at http://download.oracle.com/docs/cd/B16240_01/doc/install.102/e10953/toc.htm

In Figure 2 multiple OMS servers and an F5 Load Balancer are configured to manage traffic from Management Agents and Console UIs.

Figure 2 : Multiple OMS Servers and F5 Load Balancer Configuration



Note: The Virtual IP address used by the F5 BIG-IP must be in the same subnet as the one of the Self-IPs of the load balancer. The Self-IP is configured using the network configuration tab on the BIG-IP management interface. The OMS machines that will be used in this configuration should also be in the same subnet.

Configuring Shared Loader Directory

The first step to configure multiple OMS servers behind an SLB requires that you setup a shared disk for access by all OMS servers. Then, configure each OMS to use the same directory on this shared disk for receiving and staging uploaded files from monitored agents. This way, each OMS can share the load of processing and loading these files into the repository database. This *shared receive* directory also ensure continuous data processing in the event of a single OMS failure by the surviving OMSs.

Use the following steps to configure the OMS to use a shared receive directory.

1. Stop all OMS services for each OMS (cd to `OMS_HOME/opmn/bin`):

   ```
   ./opmnctl stopall
   ```

2. Run the following command from the `OMS_HOME/bin` directory:
   ```
   ./emctl config oms loader –shared yes –dir
   /vol3/OMS/shared_recv
   ```
3. Repeat these commands for all other OMS servers.
4. Start the OMS from `OMS_HOME/bin` directory using the following command:
   ```
   ./emctl start oms
   ```

Configuring OHS

At this point, you are ready to configure each OMS to enable the use of the common OMS name on the SLB for client UI traffic.

The following table shows the default ports that are typically used for Grid Control when using an SLB:

TABLE 2: DEFAULT PORTS USED FOR GRID CONTROL WITH SLB

PORT	DESCRIPTION
4889	Agent unsecure Upload HTTP service and Agent Registration port
1159	Agent secure HTTPS service port
7777	Console UI unsecure service port
4444	Console UI secure HTTPS service port

Configure Non-SSL UI

For HTTP UI access, perform the following tasks on each OMS:

1. Stop the OHS:
   ```
   ~/oms10g/opmn/bin $ ./opmnctl stopproc ias-component=HTTP_Server
   opmnctl: stopping opmn managed processes...
   ~/oms10g/opmn/bin $
   ```

   Note: Backup the `httpd.conf` file before editing it in step 2
2. Add VirtualHost section with SLB alias in `httpd.conf`.

   Note: This should match the F5 Virtual server port. In this case, both are set to 7777.

```
cd ~/oms10g/Apache/Apache/conf
vi httpd.conf
<VirtualHost *:7777>
    DocumentRoot "absolute path to
your/oms10g/Apache/Apache/htdocs"
    ServerName myslb.acme.com
    Port 7777
</VirtualHost>
```

3. Save the `httpd.conf` file and exit.
4. Start the OHS:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
opmnctl: starting opmn managed processes...
~/oms10g/opmn/bin $
```

Configure SSL UI (10.2.0.4 and earlier versions)

For SSL UI access, perform the following tasks on each OMS (versions < 10.2.0.5):

1. Stop the OHS:

```
~/oms10g/opmn/bin $ ./opmnctl stopproc ias-component=HTTP_Server
opmnctl: stopping opmn managed processes...
~/oms10g/opmn/bin $
```

   Note: Backup the `ssl.conf` file before editing it in step 2.

2. Change the following section in `~/oms10g/Apache/Apache/conf/ssl.conf` files, as shown in the following table:

ORIGINAL SECTION	NEW SECTION
Listen 4444 <VirtualHost _default_:4444> # General setup for the virtual host DocumentRoot "/app/oracle/Grid2/oms10g/Apache/Apache/htdocs" ServerName omshost.acme.com <<< current OMS hostname ServerAdmin you@your.address ErrorLog …. TransferLog …. Port 8250	Listen 4444 <VirtualHost _default_:4444> # General setup for the virtual host DocumentRoot "/app/oracle/Grid2/oms10g/Apache/Apache/htdocs" ServerName myslb.acme.com <<< change to your SLB alias ServerAdmin you@your.address ErrorLog …. TransferLog …. Port 443

3. Save the `ssl.conf` file and exit.
4. Start the OHS:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
opmnctl: starting opmn managed processes...
~/oms10g/opmn/bin $
```

5. Update `dcm` with the new configuration:

```
cd ~/oms10g/dcm/bin
./dcmctl updateconfig -ct ohs
```

6. Start OHS:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
opmnctl: starting opmn managed processes...
~/oms10g/opmn/bin $
```

7. Secure each OMS using the common SLB virtual hostname:

```
cd ~/oms10g/bin
./emctl secure oms -host myslb.acme.com -secure_port 1159

Oracle Enterprise Manager 10g Release 4 Grid Control
Copyright (c) 1996, 2007 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root Password :
Enter Agent Registration password :
OPMN processes successfully stopped...   Done.
Securing central oms...   Started.
Checking Repository...   Done.
```

```
Checking Em Key...   Done.
Checking Repository for an existing Enterprise Manager Root Key...
Done.
Fetching Root Certificate from the Repository...   Done.
Generating Registration Password Verifier in the Repository...
Done.
Generating Oracle Wallet Password for Enterprise Manager OMS...
Done.
Generating Oracle Wallet for Enterprise Manager OMS...   Done.
Generating Oracle Wallet for iAS HTTP Server...   Done.
Updating HTTPS port in emoms.properties file...   Done.
Generating HTTPS Virtual Host for Enterprise Manager OMS...
Done.
Securing central oms...   Ended.
OPMN processes successfully restarted...   Done.
```

Configure SSL UI (10.2.0.5 and later versions)

If the OMS is running release 10.2.0.5 or higher, you can skip editing the `ssl.conf` file and specify the `SECURE_PORT`, `SLB_PORT` and `SLB_CONSOLE_PORT` parameters when you secure the OMS:

```
cd ~/oms10g/bin
./emctl secure oms -host myslb.acme.com -secure_port 4888 -slb_port 1159
-slb_console_port 443
```

The preceding example is based on assumptions for the OMS and SLB parameters that are shown in the following table:

	HOSTNAME	SSL UPLOAD PORT	SSL UI PORT
SLB	myslb.acme.com	1159	443
OMS	omshost.acme.com	4889	4444

Note the following:

- The `SLB_PORT` parameter is required only if it is different from the `SECURE_PORT` parameter.
- By specifying the `SLB_CONSOLE_PORT` parameter, you do not need to manually modify the `servername` and `port` directives in the `ssl.conf` file.
- If you do not specify the `SLB_CONSOLE_PORT` parameter, then you will have to manually change the `servername` and `port` directives in the `ssl.conf` file.

Finally, check the secure status of the OMS by issuing the following command:

```
./emctl status oms -secure

Oracle Enterprise Manager 10g Release 4 Grid Control
Copyright (c) 1996, 2007 Oracle Corporation.  All rights reserved.
Checking the security status of the OMS at location set in
/app/oracle/Grid2/oms10g/sysman/config/emoms.properties...  Done.
OMS is secure on HTTPS Port 1159
```

Appendix A: F5 BIG-IP Local Traffic Manager Terms

This document assumes that you are familiar with F5 Networks BIG-IP. This section discusses the basic terminology. For a detailed discussion of these terms, see the BIG-IP Solutions Guide and the BIG-IP Configuration Guide.

The version of BIG-IP software used in this white paper is BIG-IP Version 10.0.1, Build 283. Terminology is identical between Version 9 and 10 of the BIG-IP software, but specific commands may have slightly different syntax.

Monitor

Monitors are used to verify the operational state of pool members. Monitors verify connections and services on nodes that are members of load-balancing pools. A monitor is designed to check the status of a service on an ongoing basis, at a set interval. If the service being checked does not respond within a specified timeout period, or the status of the service indicates that the performance has degraded, the BIG-IP system automatically takes it out of the pool and will choose the other members of the pool. When the node or service becomes available again, the monitor detects this and the member is automatically accessible to the pool and able to handle traffic. Monitors can be as simple as an ICMP ping to a server's IP address, to a TCP 3-way handshake to a service port, or as sophisticated as an HTTP Get Request with parameters, or SSL session negotiation. F5 monitors can also be custom programmed for specific needs.

Pool

A *pool* is a set of servers grouped together to receive traffic on a specific TCP port using a load balancing method. Each pool can have its own unique characteristic for a persistence definition and the load-balancing algorithm used. The preferred setting of the load balance algorithm for all Grid Control pools is Least Connections (Member).

Pools are associated with specific virtual servers directly or by rules (see later). As a result, the traffic coming to a virtual server is directed to one of the associated pools, and ultimately to one of the pool members.

Member

A *member* of the pool is defined as a node, as a destination for traffic, with an IP address and a port definition, expressed as `a.b.c.d:nn`, or `192.168.1.200:80` for a Web server with IP address 192.168.1.200 and listening on port 80. There must be at least two members in every pool to provide high availability. If one of the pool members is unavailable or offline, traffic is sent to the remaining member or members.

Virtual Server

A *virtual server* with its virtual IP Address and port number is the client addressable hostname or IP address through which members of a load balancing pool are made available to a client. After a virtual server receives a request, it directs the request to a member of the pool based on a chosen load balancing method. After a virtual server receives traffic, either directly or through a rule, the virtual server can optionally perform a number of different operations, such as inserting or modifying a header into an HTTP request, setting a persistence record, or redirecting the request to another site or fallback destination.

Before creating a virtual server, you must configure a load balancing pool of the actual physical devices (members) you wish to forward the traffic to. You can then create the virtual server, specifying that pool as the destination for any traffic coming from this virtual server. Also, if you want some of the traffic from that virtual server to go to multiple pools based on a pre-determined criterion, then you can create a rule specifying the criteria, and BIG-IP would forward the traffic to a pool matching the rule's criteria. A virtual server is configured to a specific port or to accept "ANY" ports.

A given F5 BIG-IP device may contain one or more virtual servers.

Profile

A `profile` is an F5 object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as TCP or HTTP connections. BIG-IP version 9.0 and later uses profiles.

Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient. It also allows for different characteristics to be matched to specific clients or applications. For example, one HTTP profile could be configured for Internet Explorer browsers, a different profile for Mozilla browsers, and yet another profile for hand held mobile browsers. You would have complete control over all the HTTP options in each profile, to match the characteristics of these different Web browser types.

Although it is possible to use the default profiles, the best practice recommendation is to 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 that you do not accidentally overwrite the default profile.

Persistence

Certain types of applications may require the same client returning to the same pool member, this is called persistence, or "stickiness". It can be configured using a persistence profile, and applied to the virtual server. For ORACLE Grid Control services, persistence needs to be configured for every service, except for the Secure Upload service.

Rule

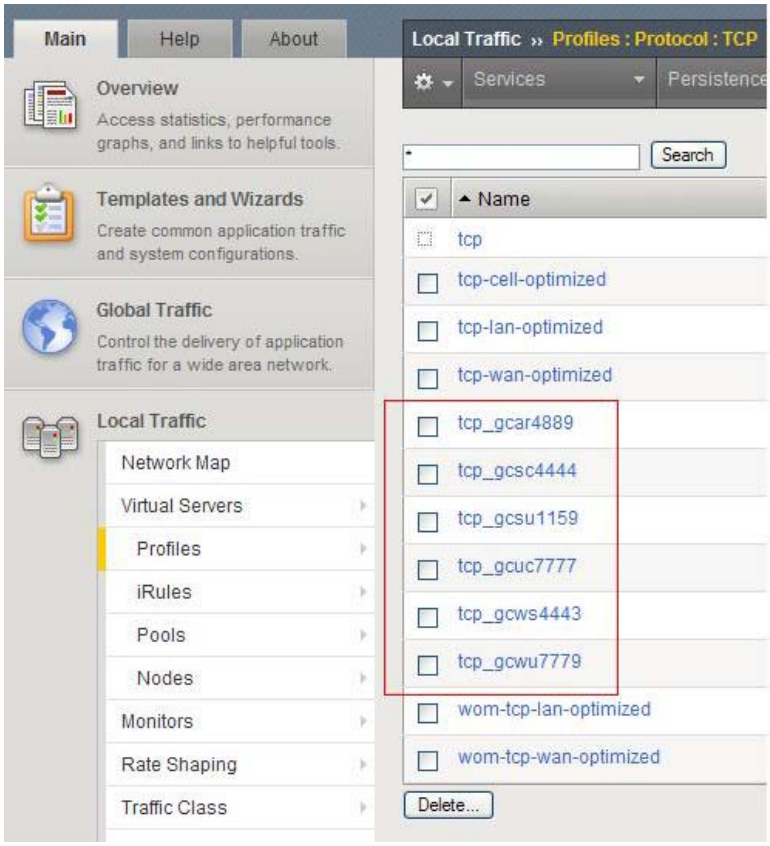
A rule is a user-written script that uses criteria to choose among one or more pools. In the BIG-IP software, it is called an iRule and provides a powerful and more granular level of control over traffic management. For an incoming request to a virtual server, the iRule is evaluated and selects the pool to which a request will be sent. For more information about F5 iRules, see the F5 DevCentral Web site at http://devcentral.f5.com/Default.aspx?tabid=75

Appendix B: Summary and Examples

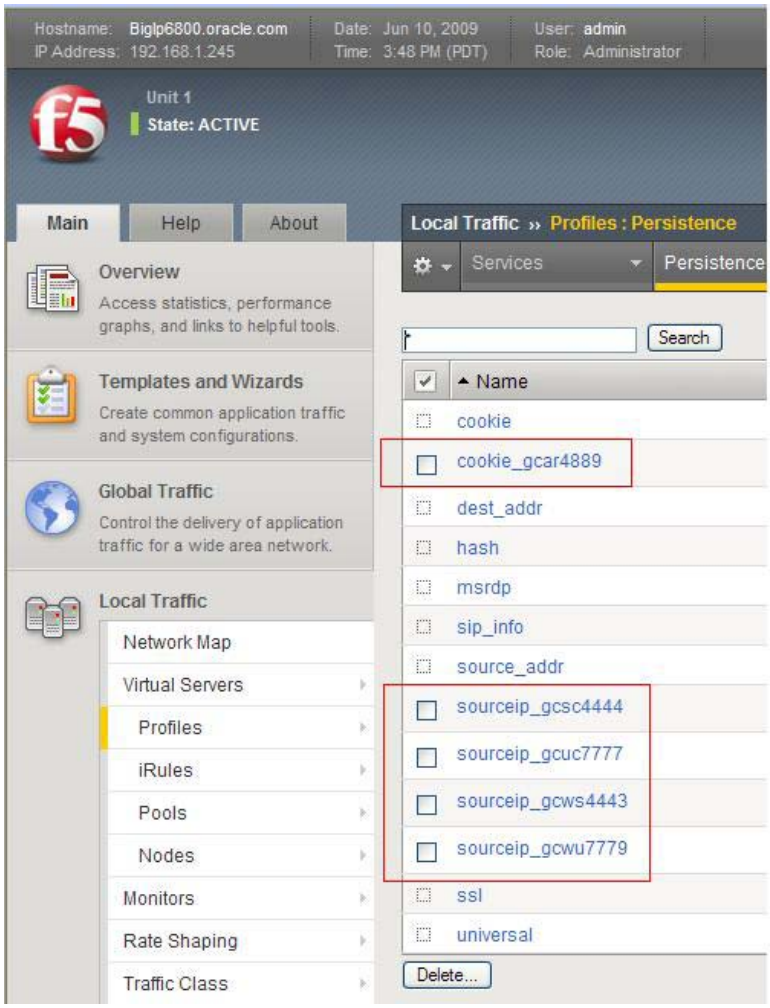
F5 Configuration Summary

Based on the configuration example used throughout this document, you should finish the F5 configuration and have a working environment. The finished configuration should look similar to the screen shots shown here of a BIG-IP LTM configured for all six of the Grid Control Services.

These are the Health Monitors for the Grid Control services.

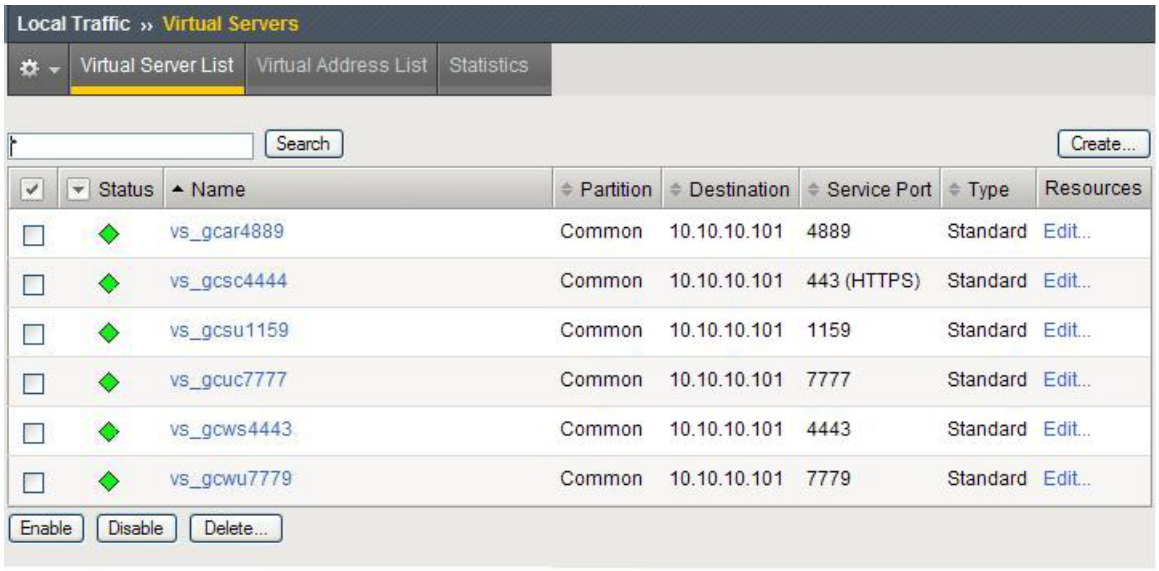


These are the TCP profiles created for the Grid Control services.



Persistence Profiles for the Grid Control services.

Pools for the Grid Control services.



Virtual Servers for the Grid Control services.

References

Oracle

1. Oracle Maximum Availability Architecture Web site
   http://www.otn.oracle.com/goto/maa
2. Oracle Database High Availability Overview (Part #B14210)
   http://otn.oracle.com/pls/db111/db111.to_toc?partno=b28281
3. Oracle Database High Availability Best Practices (Part B25159)
   http://otn.oracle.com/pls/db111/db111.to_toc?partno=b28282

F5

1. F5 Networks Home Page
   http://www.f5.com
2. F5 and Oracle Solutions Home Page
   http://www.f5.com/solutions/applications/oracle/
3. F5 Oracle Grid Control Configuration Guide
   http://www.f5.com/pdf/deployment-guides/oracle-grid-control-big-ip-dg.pdf
4. F5 BIG-IP Product Documentation
   http://www.f5.com/products/big-ip/
5. F5 Version 10 Software Configuration Guide
   https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm_configuration_guide_10_0_0.html
6. F5 Technical Support Knowledge Base
   https://support.f5.com/kb/en-us.html
7. F5 and Oracle Cooperative Support Agreement
   http://www.f5.com/news-press-events/press/archive/20050725b.html
8. F5 Training and Support
   http://www.f5.com/training-support/
9. F5 DevCentral Web site
   http://devcentral.f5.com/Default.aspx?tabid=75

Configuring Maximum Availability Architecture for Oracle Enterprise Manager with F5 BIG-IP Local Traffic Manager
February 2010
Authors:
Farouk Abushaban, Oracle Corporation
Chris Akker, F5 Networks
James Viscusi, Oracle Corporation

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109