DEPLOYMENT GUIDE
Version 1.0

Deploying the BIG-IP LTM with Oracle Enterprise Manager Grid Control Services

Introducing the F5 and Oracle Enterprise Manager Grid Control Services deployment guide

Welcome to the F5 and Oracle® Enterprise Manager Grid Control Services deployment guide. This guide contains step-by-step procedures for configuring F5 devices for Grid Control deployments in a secure, fast and highly available deployment. This document was produced as a joint effort between F5 and Oracle and describes the configuration and operational best practices for using F5 BIG-IP as the application delivery controller with an Oracle Grid Control Maximum Availability Architecture (MAA) deployment.

Oracle Enterprise Manager Grid Control is a comprehensive administrative and management suite designed to work in all areas of the Oracle Technology Stack. Whether it be Applications, Middleware, or Database, Grid Control can provide the visibility and tools necessary to keep applications available. It addresses the broad IT requirements for Application Operations Management with its comprehensive top-down approach for managing applications and technologies, ensuring customers have superior performance and end-user experiences, while delivering lower total cost of ownership.

For more information on Oracle Grid Control, see ***http://www.oracle.com/technology/products/oem/index.html***

For more information on the F5 devices included in this guide, see ***http://www.f5.com/products/***.

Prerequisites and configuration notes

The following are general prerequisites for this deployment.

- While this deployment guide includes some Oracle Enterprise Manager Grid Control configuration procedures, most of the procedures in this document are performed on the BIG-IP Local Traffic Manager (LTM) system. For information on how to deploy or configure Oracle Grid Control, consult the appropriate Oracle documentation.
- This guide is written with the assumption that you are familiar with both the F5 devices and Oracle Grid Control Services. For more information on configuring these products, consult the appropriate documentation.
- The BIG-IP LTM system should be running version 9.4.7. We strongly recommend using version 10.0.1 or later.
- The following BIG-IP LTM configuration instructions assume you are connected to the web-based configuration utility using a web browser.
- We recommend you create a dedicated Administrative Partition on the BIG-IP LTM system for configuration access and use by the Grid Control administrator. All the necessary F5 configuration elements for the MAA Grid Control environment will be located in this partition. Additions, deletions, and changes to these objects will not interfere with

any other. For more information and specific configuration instructions, see the ***Configuring Administrative Partitions*** chapter of the BIG-IP documentation, depending on your version (version 10.0 and later, **TMOS Management Guide for BIG-IP Systems**; prior to version 10.0, the **BIG-IP Network and System Management Guide**).

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	v10.0.1 (applicable to v9.4.7 and later)
Oracle Grid Control Services	v10.2.0.5

Revision history:

Document Version	Description
1.0	New deployment guide

Configuration example

The BIG-IP platform provides load balancing, high availability, service monitoring, TCP/IP enhancements, and application persistence for an OMS Grid Control environment. Several advanced features of the BIG-IP LTM are used, targeting different areas of the infrastructure where mission critical high availability is required to provide continuous access to the Grid Control OMS application.

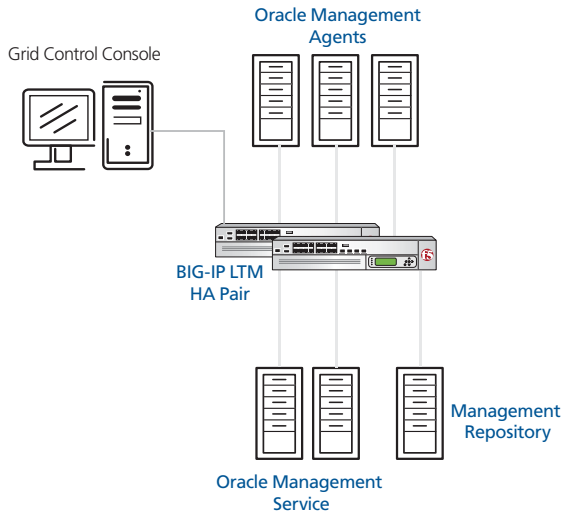

Figure 1 *Logical configuration example*

Configuring Enterprise Manager for use with BIG-IP LTM

Follow the steps in this section to configure Oracle Enterprise Manager to work with the F5 BIG-IP LTM. These procedures are provided for your convenience. For further information, see the Oracle documentation.

Oracle Enterprise Manager Middle tier framework is based on the Oracle Application Server 10g 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 servelet, 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

Refer to Chapter 17 of the Enterprise Manager Grid Control Installation and Configuration Guide for more details on configuring Multiple OMS environments.

Configuring the 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.

To configure the OMS to use a shared receive directory

1. Stop all OMS services for each OMS (cd to OMS_HOME/opmn/bin) using the following command:

   ```
   ./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 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.

Typically, the default ports used for Grid Control when using an SLB are:

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

Table 1 *Default ports used for Grid Control when using BIG-IP*

Configuring Non-SSL (HTTP) access to the user interface

For HTTP UI access, perform the following procedure on each OMS. We recommend you back up the **httpd.conf** file before editing it in Step 2.

To configure HTTP access to the UI

1. Stop the OHS using the following command:

```
~/oms10g/opmn/bin $ ./opmnctl stopproc ias-component=HTTP_Server
```

   The system responds with

   ```
   opmnctl: stopping opmn managed processes...
   ```

2. Add the VirtualHost section with SLB alias to the **httpd.conf** file using the following commands:

   a) Change directories to the **Apache/Apache/conf** directory:

   ```
   cd ~/oms10g/Apache/Apache/conf
   ```

   b) Open the httpd.conf file in a text editor:

   ```
   vi httpd.conf
   ```

   c) Add the following section to the **httpd.conf** file, and replace the section in parenthesis in the DocumentRoot line with your path:

```
<VirtualHost *:7777>
    DocumentRoot "(absolute path to your)/oms10g/Apache/Apache/htdocs"
    ServerName myslb.acme.com
    Port 7777
</VirtualHost>
```

   d) Save the **httpd.conf** file and exit

3. Start the OHS using the following command:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
```

   The system responds with

```
opmnctl: starting opmn managed processes...
```

Configuring SSL access to the user interface: v10.2.0.4 and earlier

For SSL access to the user interface, perform the following tasks on each OMS, versions **prior to** 10.2.0.5. For version 10.2.0.5, see *Configuring SSL access to the user interface: v10.2.0.5 and later*, on page 7.

We recommend you back up the **ssl.conf** file before editing it in Step 2.

To configure SSL access to the user interface, v10.2.0.4 and earlier

1. Stop the OHS using the following command:

```
~/oms10g/opmn/bin $ ./opmnctl stopproc ias-component=HTTP_Server
```

   The system responds with

```
opmnctl: stopping opmn managed processes...
```

2. Change the **Listen 4444** section of the **ssl.conf** file using the following commands:

   a) Change directories to the **Apache/Apache/conf** directory:

   ```
   cd ~/oms10g/Apache/Apache/conf
   ```

   b) Open the httpd.conf file in a text editor:

   ```
   vi ssl.conf
   ```

c) Find the following section of the **ssl.conf** file:

```
<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                       <-- current port
```

d) Change the entries in red above to look like the following:

```
<VirtualHost _default_:4444>
    #  General setup for the virtual host
    DocumentRoot "/app/oracle/Grid2/oms10g/Apache/Apache/htdocs"
    ServerName myslb.acme.com      <-- change to SLB alias
    ServerAdmin you@your.address
    ErrorLog ….
    TransferLog ….
    Port 443                       <-- change to port 443
```

e) Save the **ssl.conf** file and exit

3. Start the OHS using the following command:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
```

The system responds with

```
opmnctl: starting opmn managed processes...
```

4. Update dcm with the new configuration using the following commands:

a) Change directories to /dcm/bin, using the following command:

```
cd ~/oms10g/dcm/bin
```

b) Type the following command:

```
./dcmctl updateconfig -ct ohs
```

5. Secure each OMS using the common SLB virtual host name using the following commands:

a) Change directories to the following:

```
cd ~/oms10g/bin
```

b) Type the following command:

```
./emctl secure oms -host myslb.acme.com -secure_port 1159
```

Configuring SSL access to the user interface: v10.2.0.5 and later

If the version of OMS is 10.2.0.5 or later, you can skip editing the **ssl.conf** file and specify **secure_port**, **slb_port** and **slb_console_port** parameters when you secure the OMS.

To configure SSL access to the user interface for v10.2.0.5 and later

1. Change directories to the following:

   ```
   cd ~/oms10g/bin
   ```

2. Type the following command:

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

   This command example is based on the following assumptions for OMS and SLB parameters:

	Host name	SSL Upload Port	SSL UI Port
SLB	myslb.acme.com	1159	443
OMS	omshost.acme.com	4889	4444

Table 2 *Host name and ports for SSL access*

   The **slb_port** parameter is only required if it is different from **secure_port**.

   By specifying **slb_console_port**, you don't have to manually modify the servername and port directives in **ssl.conf**.

   If you don't specify the **slb_console_port**, then you will have to manually change the servername and port directives in **ssl.conf**.

3. Check the secure status of the OMS using the following command:

   ```
   ./emctl status oms -secure
   ```

   You will see results like the following:

```
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
```

Configuring the BIG-IP LTM for Oracle Grid Control Services

In this section we configure the BIG-IP LTM for multiple Oracle Grid Control services. Because the LTM configuration for each Grid Control service is nearly identical, rather than repeat the set of instructions for each service, we provide a detailed example for one set of BIG-IP LTM configuration objects (health monitor, load balancing pool, profile, and virtual server).

Table 3, on page 9 contains a list of Grid Control services, and the associated information (such as monitor type and ports) to use when configuring the BIG-IP LTM. Review each table, and for the services and protocols applicable to your configuration, repeat the procedures in *Configuring the BIG-IP LTM for the Grid Control services*, using the information from the table as appropriate.

How to use the following table

For each of the line items in the following tables, you must create a health monitor, pool, profile(s), and virtual server on the BIG-IP LTM. You may want to print the table for reference.

- **Grid Control Service**
  This describes the Grid Control service.
- **Monitor Type**
  This is the type of health monitor. When configuring the BIG-IP LTM monitor, you select this monitor from the **Type** list.
- **TCP Port**
  This is the TCP port used by the service. You use this port when configuring the BIG-IP LTM pool in the **Service Port** field.
- **Virtual Server Port**
  This is the Service Port you enter when configuring the BIG-IP LTM virtual server in the **Service Port** field.
- **F5 Profiles**
  This column contains the TCP profiles you must create while configuring the BIG-IP LTM system. All objects have a TCP profile. Some of the objects have additional profiles.

Note

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

Grid Control Service	Monitor	TCP Port	Profiles	Virtual Server Port
Secure Upload	HTTPS Interval: 60 Timeout: 181	1159	TCP	1159
Agent Registration	HTTP Interval: 60 Timeout: 181	4889	TCP, cookie persistence	4889
Secure Console	HTTPS Interval: 30 Timeout: 91	4444	TCP, source IP persistence	443
Unsecure Console	HTTP Interval: 30 Timeout: 91	7777	TCP, source IP persistence	7777
Web Cache Secure	HTTPS Interval: 30 Timeout: 91	4443	TCP, source IP persistence	4443
Web Cache Unsecure	HTTP Interval: 30 Timeout: 91	7779	TCP, source IP persistence	7779

Table 3 *Table of Grid Control services and associated BIG-IP configuration objects*

Configuring the BIG-IP LTM for the Grid Control services

Use the following procedures as a template for configuring the Grid Control services applicable to your configuration, as described in the table above.

Creating the health monitors

The first step is to configure the health monitor. This procedure uses entries from the **Monitor Type** and **TCP Port** columns in the tables above.

The following monitors use Send and Receive Strings in order to retrieve specific information from the services to not only ensure the device is up, but also serving the expected content. You will notice in the following procedure the Secure Upload and Agent Registration services use unique strings, the other four services use the same strings.

To configure a 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 unique name for this monitor.
   We recommend prefacing the monitor name with *mon_* and then including the Grid Control Service and TCP port number from Table 3. For example, we use **mon_gcsu1159** for the Grid Control Secure Upload service.
4. From the **Type** list, select the monitor type found in the **Monitor** column in Table 3. For example, if the column contains **HTTPS**, select **HTTPS** from the list.
   The Monitor configuration options appear.
5. From the **Configuration** list, select **Advanced**.
6. In the Configuration section, in the **Interval** and **Timeout** boxes, type the Interval and Timeout that corresponds to this Grid Control service in the **Monitor** column of Table 3. We recommend at least a 1:3 +1 ratio between the interval and the timeout. For example, the **mon_gcsu1159** monitor uses **90** and **181**.
7. For the **Secure Upload** service monitor only:
   a) In the **Send String** box, type the following:
   ```
   GET /em/upload HTTP/1.0
   ```
   b) In the **Receive String** box, type the following:
   ```
   Http Receiver Servlet active!
   ```
8. For the **Agent Registration** service monitor only:
   a) In the **Send String** box, type the following:
   ```
   GET /em/genwallet HTTP/1.0
   ```
   b) In the **Receive String** box, type the following:
   ```
   GenWallet Servlet activated
   ```
9. For the remaining services (**Secure Console, Unsecure Console, Web Cache Secure and Web Cache Unsecure**):
   a) In the **Send String** box, type the following:

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

   b) In the **Receive String** box, type the following:
   ```
   /em/console/logon/logon;jsessionid=
   ```
10. In the **Alias Service Port** box, type the appropriate port found in the **TCP Port** column. For example, if the column contains **1159**, type **1159** in the **Alias Service Port** box (see Figure 2 this example).
11. All other configuration settings are optional, configure as applicable for your deployment.
12. Click the **Finished** button.

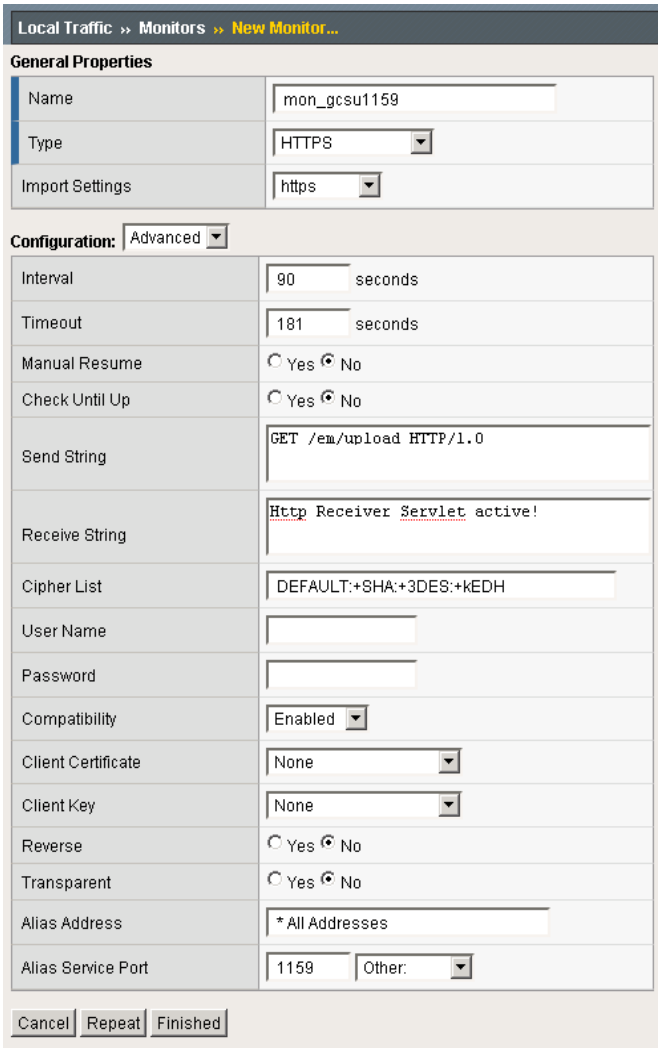

Figure 2 *Creating the health monitor*

Creating the Grid Control pools

The next step is to create the pools on the BIG-IP LTM system. This procedure uses entries from the **TCP Port** column in the table above.

To create the pools

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. Click the **Create** button. The New Pool screen opens.

3. In the **Name** box, type a unique name for this Pool.
   We recommend prefacing the pool name with *pool_* and then including the Grid Control Service and TCP port number from Table 3. For example, **pool_gcsu1159**.
4. In the Health Monitors section, from the **Available** list, select the name of the monitor you created in *Creating the health monitors*, on page 9, and click the Add (**<<**) button. Be sure to use the monitor that is associated with the same service or protocol as this pool. For example, if you are configuring the pool **pool_gcsu1159**, you would select **mon_gcsu1159**.
5. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). We recommend selecting **Least Connections (member)** for all pools in this configuration.
6. In the New Members section, you add the Grid Control servers to the pool.
   a) In the **Address** box, type the IP address of the Grid Control Server.
   b) In the **Service Port** box, type the service number from the **TCP Port** column in the table above. For example, if you are configuring the Secure Upload pool, use port **1159**.
   c) Click the **Add** button to add the member to the list.
   d) Repeat steps a-c for each server you want to add to the pool.
7. Click the **Finished** button (see Figure 3).

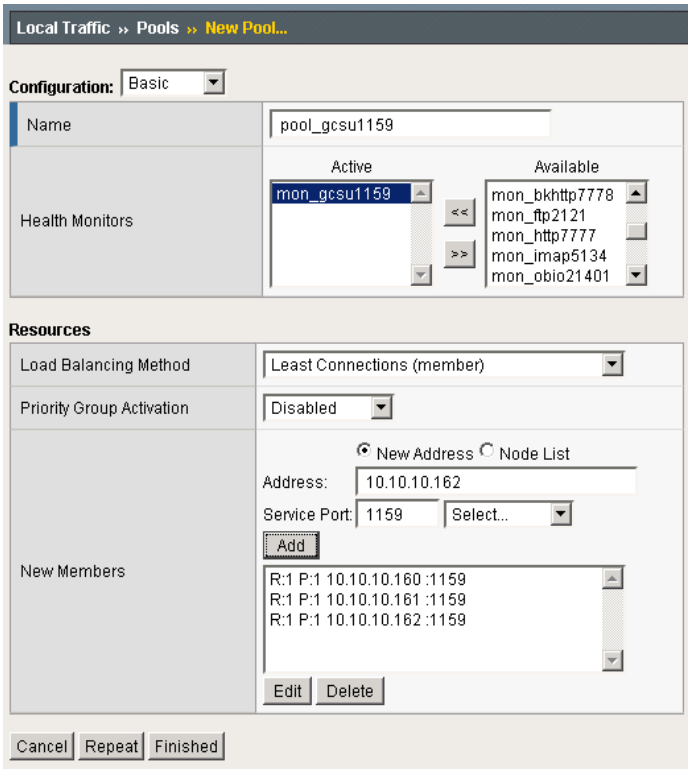

Figure 3 *Configuring the BIG-IP pool*

Creating the TCP profiles

The next step is to create a TCP 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. 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 client or applications.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Protocol** menu, select **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 unique name for this profile. We recommend prefacing the profile name with *tcp_* and then including the Grid Control service and TCP port number from Table 3. For example, **tcp_gcsu1159**.
5. Modify the rest of the settings as applicable for your network. The default settings should suffice for most networks.

6. Click the **Finished** button.

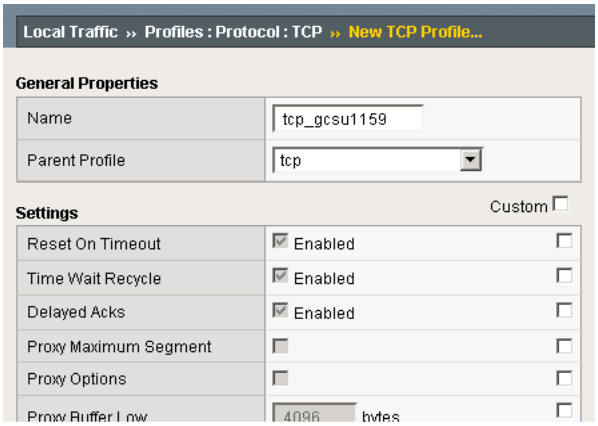

Figure 4 *Configuring the TCP profile (truncated)*

Tip

If majority of your clients are connecting over a wide area network (WAN), consider selecting ***tcp-wan-optimized*** *from the* ***Parent Profile*** *list.*

Creating the persistence profiles

The next task is to create the persistence profiles. All Grid Control Services with the exception of Secure Upload use a persistence profile. The Agent Registration service uses a cookie persistence profile, the rest of the Grid Control Services use Source IP persistence (see the Profile column of Table 3, on page 9 if you are unsure of which persistence type to use).

Important

You do not need to create a persistence profile for the Secure Upload Service.

Creating the cookie persistence profile for the Agent Registration service

This cookie persistence profile is only for the Agent Registration service.

To create the cookie persistence profile for the Agent Registration service

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, click **Persistence**.
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 **cookie-gcar4889**.

5. From the **Persistence Type** list, select **Cookie**.
   The configuration options for cookie persistence appear.
6. Click the **Custom** box for **Expiration**, and then clear the **Session Cookie** box. The expiration options appear.
7. In the **Seconds** box, type **3600**.
8. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
9. Click the **Finished** button.

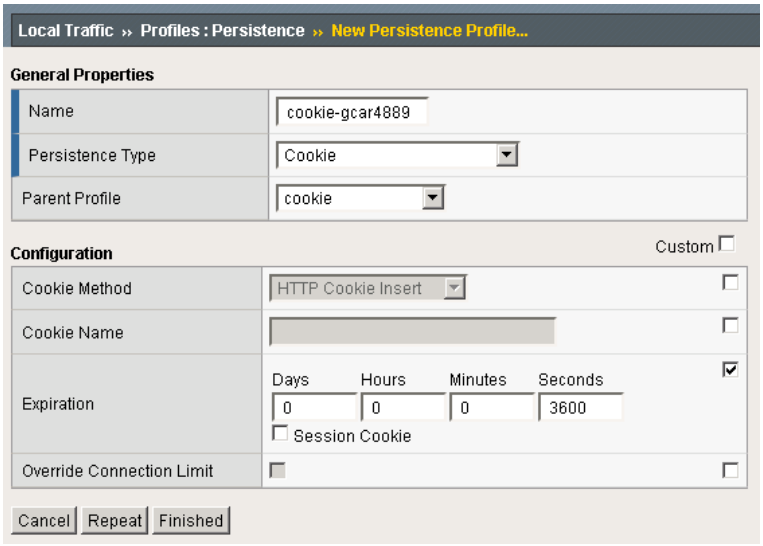

Figure 5 *Configuring the Beekeeper cookie persistence profile*

Creating the Source IP persistence profile

The following persistence profile is for the **Secure Console**, **Unsecure Console**, **Web Cache Secure** and **Web Cache Unsecure** services.

To create the Source IP persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, click **Persistence**.
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 unique name for this profile.
   We recommend prefacing the profile name with *sourceip_* and then including the Grid Control service and TCP port number from Table 3. For example, **sourceip_gcsc4444**.
5. From the **Persistence Type** list, select **Source Address Affinity**.
   The configuration options for Source IP persistence appear.

6. Click the **Custom** box for **Timeout**, and then clear the **Session Cookie** box. The expiration options appear.
7. In the **Seconds** box, type **3600**.
8. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
9. Click the **Finished** button.

Creating the Redirect iRule for the Unsecure Console service

The next task is to create an iRule for the Unsecure Console service. The Redirect iRule takes incoming HTTP requests (non-secure) and redirects the requests to the correct HTTPS (secure) virtual server, without user interaction. This Redirect iRule is 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 click **iRules**.
2. In the upper right portion of the iRule screen, click **Create**.
3. In the Name field on the New iRule screen, enter a name for your iRule. In our example, we use **gcuc_httptohttps**.
4. 4. In the **Definition** section, copy and paste the following iRule:

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

5. Click **Finished**.

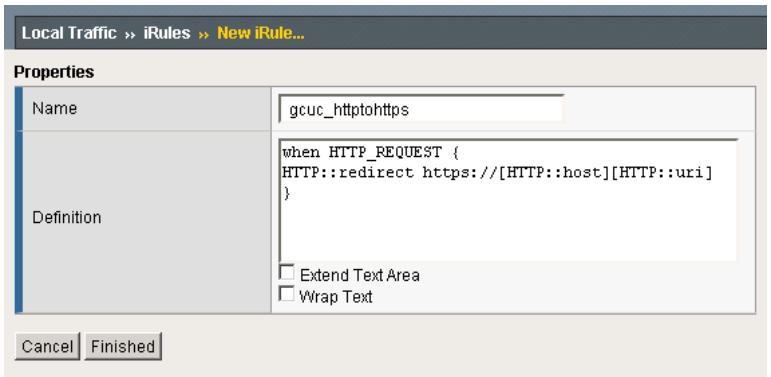

Figure 6 *Creating the iRule*

Creating the virtual servers

The final step is to define virtual servers that references the profile and pool you created. A virtual server with its virtual address and port number, is the client addressable host name or IP address through which members of a load balancing pool are made available to a client. This procedure uses entries from the **VIP TCP Port** column in the tables above.

To create the virtual servers

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a unique name for this virtual server. We recommend prefacing the profile name with *vs_* and then including the Grid Control Service and TCP port number from Table 3. For example, **vs_gcsu1159**.
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 **10.10.10.101**.
6. In the **Service Port** box, type the service number from the **VIP TCP Port** column in Table 3. For example, if you are configuring the Secure Upload virtual server, use port **1159**.
   Note: This port does not always match the port used for the pool.
7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the profile you created for this service in *Creating the TCP profiles*, on page 13.

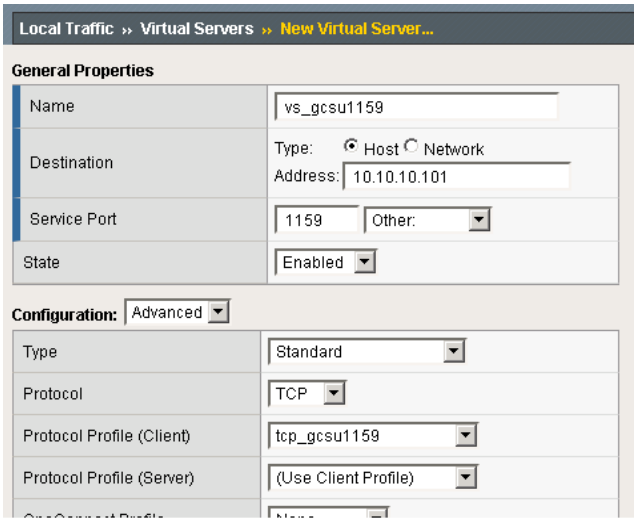

Figure 7 *Configuring the virtual server (truncated)*

9. For **Agent Registration** and **Unsecure Console** services only: From the **HTTP Profile** list, select **http**.
10. From the **SNAT Pool** list, select **Auto Map**.
11. For the **Unsecure Console** service only, in the iRules row, from the Available list, select the iRule you created in *Creating the Redirect iRule for the Unsecure Console service*, on page 16, and click the Add (<<) button. In our example, we select **gcuc_httptohttps**.
12. In the Resources section, from the **Default Pool** list, select the pool you made for this service in *Creating the Grid Control pools*, on page 11.
13. From the **Default Persistence Profile** list:
    a) For the **Secure Upload** service, leave the list at None.
    b) For the **Agent Registration** virtual server, select the profile you created in *Creating the cookie persistence profile for the Agent Registration service*, on page 14. In our example, we select **cookie-gcar4889**.
    c) For the **Secure Console**, **Unsecure Console**, **Web Cache Secure** and **Web Cache Unsecure** virtual server, select the profile you created in *Creating the Source IP persistence profile*, on page 15. For example, **sourceip_gcsc4444**.
14. Configure any other settings as appropriate for your configuration.
15. Click the **Finished** button (see Figure 8).

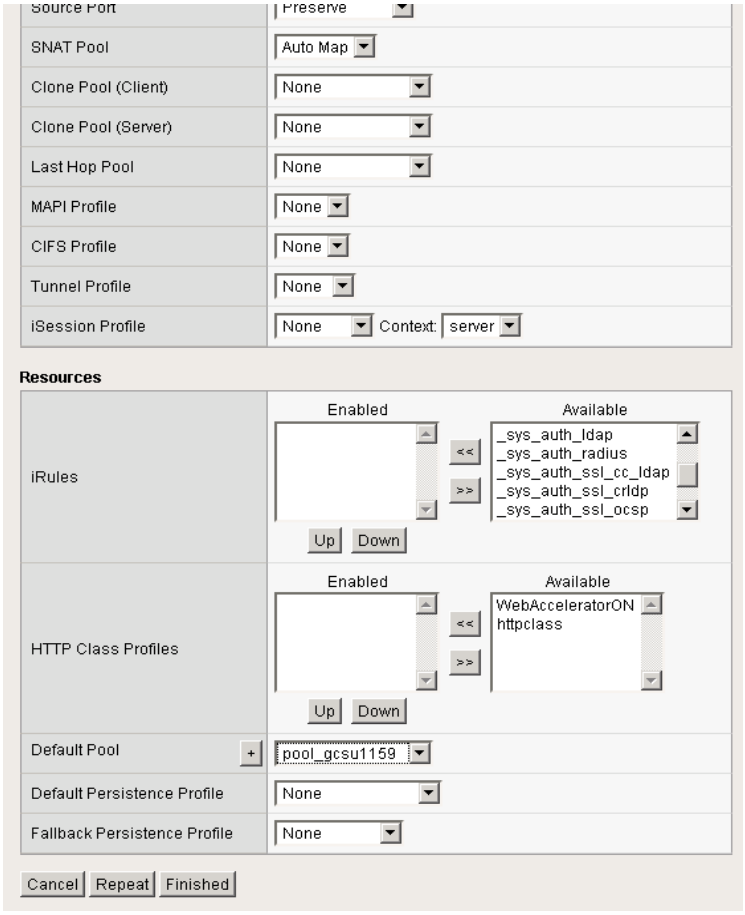

Figure 8 *Configuring the virtual server SNAT pool and default pool*

Repeating the procedures

Return to *Creating the health monitors*, on page 9 and using Table 3, on page 9, repeat all of the procedures for each of the Grid Control services applicable to your configuration.

Synchronizing the BIG-IP configuration if using a redundant system

When you have completed the configuration of your virtual servers and related objects, and if you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

The method of synchronizing the BIG-IP configuration depends on your version, see the appropriate BIG-IP LTM manual, available on Ask F5 (*https://support.f5.com/kb/en-us/products/big-ip_ltm.html*).