DEPLOYMENT GUIDE

DEPLOYING THE BIG-IP LTM SYSTEM WITH THE ANGEL LEARNING MANAGEMENT SUITE

Version: 1.0

Deploying the BIG-IP LTM with the ANGEL Learning Management Suite

Welcome to the F5 - ANGEL deployment guide. This guide gives step-by-step procedures on configuring the F5 BIG-IP® Local Traffic Manager™ (LTM) with the ANGEL® Learning Management Suite (LMS) for both HTTP and HTTPS traffic.

The ANGEL Learning Management Suite (LMS) of teaching and learning tools enables efficient and effective development, delivery and management of courses, course content and learning outcomes. Engaging communication and collaboration capabilities enhance instruction to deliver leading edge teaching and learning.

The BIG-IP LTM is an application delivery networking system that provides the most intelligent and adaptable solution to secure, optimize, and deliver applications, enabling organizations to effectively and competitively run their business.

For more information on the ANGEL Learning Management Suite, see **www.angellearning.com/products/lms/**

For more information on the BIG-IP LTM system, see **www.f5.com/products/big-ip/product-modules/local-traffic-manager.html**

Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- The ANGEL Learning Management Suite must be running version 7.2, 7.3, or 7.4.
- For this Deployment Guide, the BIG-IP LTM system must be running version 9.0 or later.
- We assume that the BIG-IP LTM device is already installed in the network, and objects like Self IPs and VLANs have already been created. For more information on configuring these objects, see the BIG-IP LTM manuals.

Product Tested	Version Tested
BIG-IP Local Traffic Manager (LTM)	9.3.1
ANGEL LMS	7.2, 7.3 and 7.4

Configuration example

In this Deployment Guide, the BIG-IP system is optimally configured to optimize and direct traffic to an ANGEL LMS deployment. The following is a simple configuration diagram.

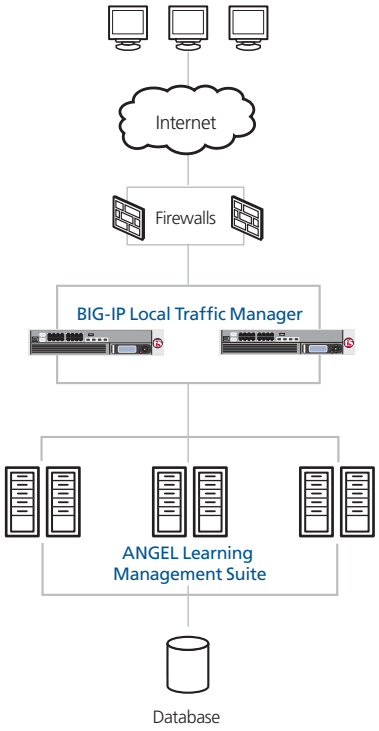

Figure 1 *Logical configuration example*

Configuring the BIG-IP LTM system for ANGEL LMS

To configure the BIG-IP LTM system to load balance your LMS deployment, you need to complete the following tasks:

- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating profiles*
- *Creating the virtual server*
- *Configuring the BIG-IP LTM to offload SSL* (optional)

Creating the HTTP health monitor

The first step is to set up health monitors for the ANGEL LMS devices. This procedure is optional, but very strongly recommended. In our example, we create custom HTTP health monitor that uses a specific Send String to check the ANGEL LMS devices. Use the procedure applicable to your LMS version.

Important

The Send String you configure depends on the version of ANGEL LMS you are using. Only configure the monitor applicable to your version.

To create the health monitor for LMS version 7.2

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **lms-v72-http**.
4. From the **Type** list, select **http**.
5. In the **Interval** box, type **30**.
6. In the **Timeout** box, type **91**.
   In the **Send String** box, type

   ```
   GET /signon/login.asp HTTP/1.1\r\nHost: \r\nConnection: Close\r\n
   ```

7. In the Receive String box, type

   ```
   username
   ```

8. Click the **Finished** button (see Figure 2).

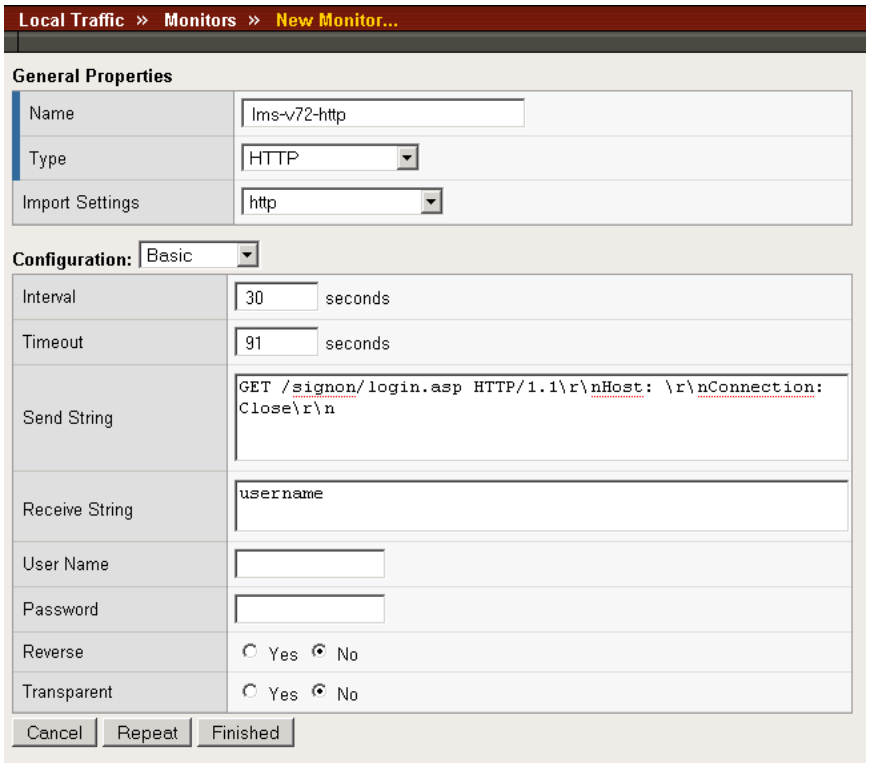

Figure 2 *Creating the HTTP Monitor*

To create the health monitor for LMS version 7.3 and 7.4

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **lms-v73-http**.
4. From the **Type** list, select **http**.
5. In the **Interval** box, type **60**.
6. In the **Timeout** box, type **91**.
7. In the **Send String** box, type

   ```
   GET /default.asp HTTP/1.1\r\nHost: \r\nConnection: Close\r\n
   ```

8. In the Receive String box, type

   ```
   fullname
   ```

9. Click the **Finished** button.

Creating the pool

The next step is to define a load balancing pool for the LMS devices. A BIG-IP LTM pool is a set of devices grouped together to receive traffic according to a load balancing method. This pool uses the monitor you just created.

To create the LMS pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
   The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Pool screen opens.
3. From the **Configuration** list, select **Advanced**.
4. In the **Name** box, type a name for your pool.
   In our example, we use **lms-http-pool**.
5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (**<<**) button. In our example, we select **lms-v72-http**.
6. In the **Slow Ramp Time** box, type **300**. For this pool, we use the Least Connections load balancing method. We set the Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the Least Connections load balancing algorithm does not send all new connections to that member (a newly available member will always have the least number of connections).
7. In the **IP ToS to Server** and **Link QoS to Server** rows, make sure **Pass Through** is selected.
8. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Least Connections (member)**.
9. In this pool, we leave the Priority Group Activation **Disabled**.
10. In the New Members section, make sure the **New Address** option button is selected.
11. In the **Address** box, add the first LMS device to the pool. In our example, we type **10.132.81.100**.
12. In the **Service Port** box, type **80** or select **HTTP** from the list.
13. Click the **Add** button to add the member to the list.
14. Repeat steps 11-13 for each server you want to add to the pool.
    In our example, we repeat these steps twice for the remaining servers, **10.132.81.101** and **102**.
15. Click the **Finished** button (see Figure 3).

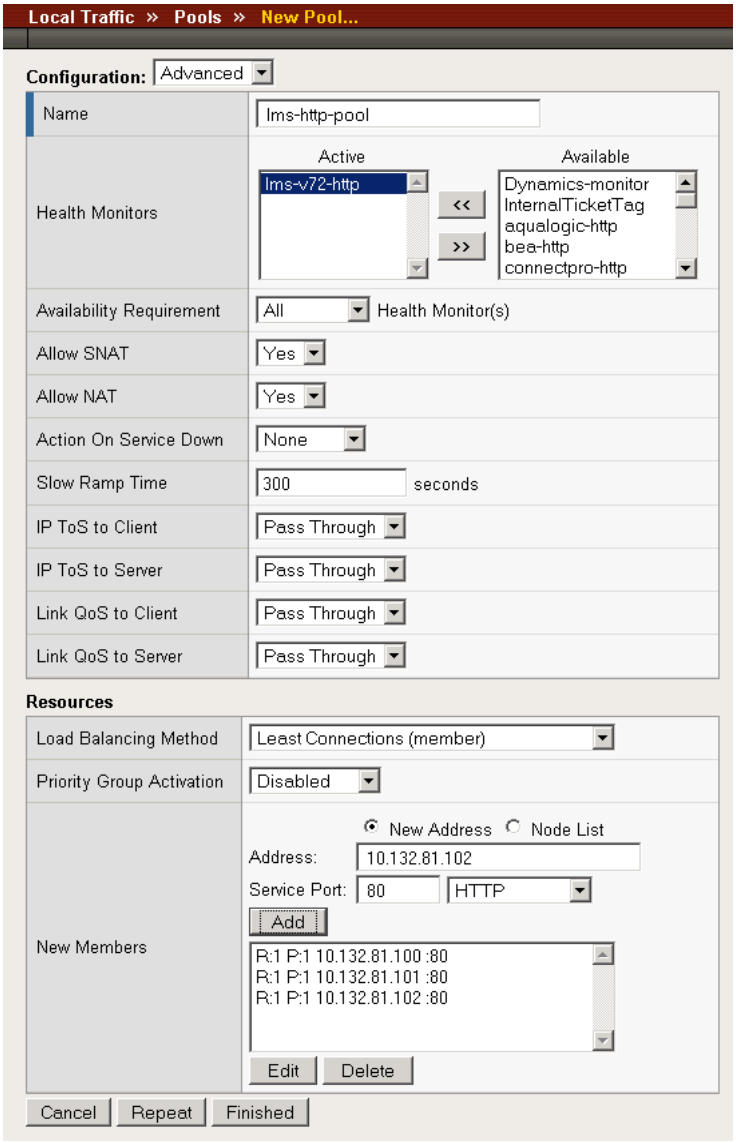

Figure 3 *Creating the pool for the LMS devices*

Creating profiles

BIG-IP version 9.0 and later use profiles. A ***profile*** is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

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

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. For this example, we use a simple HTTP monitor. There are also optimized HTTP parent profiles that include compression and caching that may improve overall performance.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **lms-http**.
4. From the **Parent Profile** list, select **http**.
5. *Optional:* If you are using the BIG-IP LTM to offload SSL, in the Settings section, check the **Custom** box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **Match**. See *Configuring the BIG-IP LTM to offload SSL*, on page 11 for more information.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the TCP profile

The next profile we create is the TCP profile.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **lms-tcp**.
5. From the **Parent Profile** list, select **tcp**.

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

Creating the persistence profile

The next profile we create is a Persistence profile. For this configuration, we recommend using cookie persistence (HTTP cookie insert).

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
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 **lms-cookie**.
5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

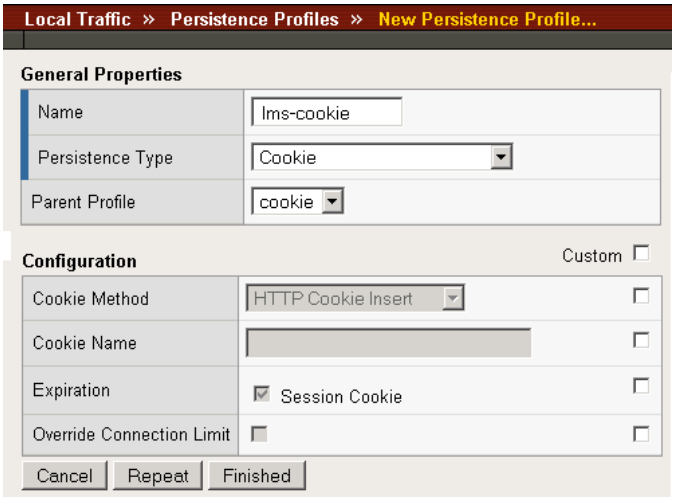

Figure 4 *Creating the cookie persistence profile*

Creating the virtual server

Next, we configure a virtual server that references the profiles 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** box, type a name for this virtual server. In our example, we type **lms-http-vs**.
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 **192.168.10.120.**
6. In the **Service Port** box, type **80**, or select **HTTP** from the list.

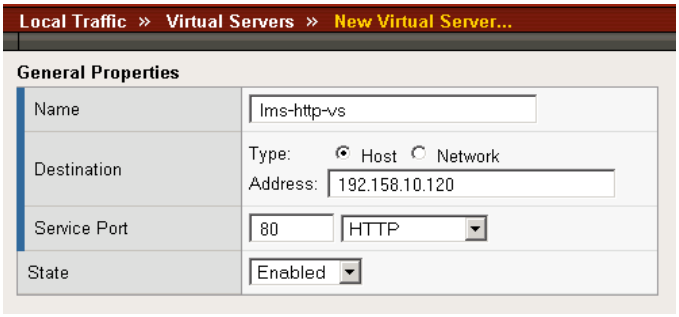

Figure 5 *Creating the virtual server*

7. From the Configuration list, select **Advanced**. The Advanced configuration options appear.
8. Leave 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 the TCP profile* section. In our example, we select **lms-tcp**.
10. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **lms-http**.
11. From the **SNAT Pool** list, select **Automap** (see Figure 6).

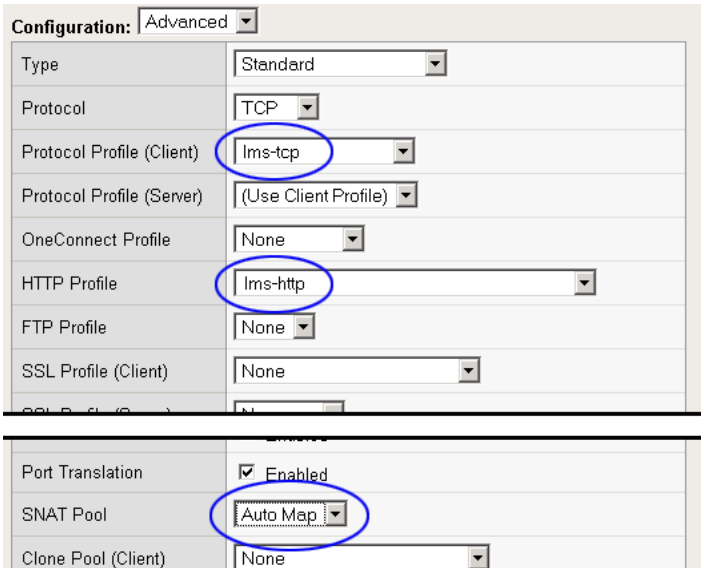

Figure 6 *Selecting the profiles for the virtual server - screenshot condensed*

12. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **lms-http-pool**.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating the persistence profile* section. In our example, we select **lms-cookie**.

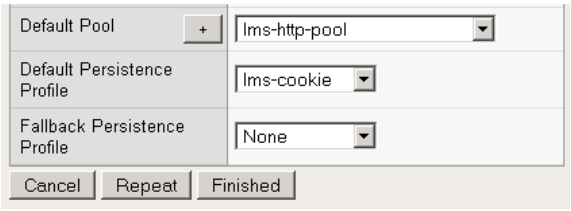

Figure 7 *Adding the Pool and Persistence profile to the virtual server*

14. Click the **Finished** button.

The BIG-IP LTM HTTP configuration for the ANGEL LMS deployment is now complete (if you are using a redundant system, see *Synchronizing the BIG-IP LTM configuration if using a redundant system*, on page 15).

If you are using the BIG-IP LTM to offload SSL, continue with following section.

Configuring the BIG-IP LTM to offload SSL

If you are using the BIG-IP LTM system to offload SSL from the ANGEL LMS deployment, there are additional configuration procedures you must perform on the BIG-IP LTM system. In the following configuration, the BIG-IP LTM redirects all incoming traffic to the HTTP virtual server to the HTTPS virtual server. This is useful if a user types a URL in a browser, but forgets to change the protocol to HTTPS.

If your deployment does not require ***all*** traffic to be redirected to HTTPS, you do not need to modify the HTTP virtual server as described below, nor configure the Rewrite Redirect setting in the HTTP profile in Step 5 of *Creating an HTTP profile*. You can have both an HTTP and HTTPS virtual server on the same address with the appropriate ports.

Important

This section is optional, and only necessary if you are using the BIG-IP LTM system for offloading SSL.

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for ANGEL LMS connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the ***Configuration Guide for Local Traffic Management***.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand **Local Traffic**.
2. Click **SSL Certificates**. The list of existing certificates displays.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (Certificate or Key).

5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

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

Creating a Client SSL profile

The next step in this configuration is to create a Client SSL profile. This profile contains the SSL certificate and Key information for decrypting the SSL traffic on behalf of the servers.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the SSL menu, select **Client**. The Client SSL Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New Client SSL Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **lms-clientssl**.
5. In the Configuration section, check the **Certificate** and **Key Custom** boxes.
6. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
7. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
8. Click the **Finished** button.

Creating the Redirect iRule

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

To create the Redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.

3. In the **Name** box, enter a name for your iRule.
   In our example, we use **lms-httptohttps**.
4. In the Definition section, copy and paste the following iRule:

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

5. Click the **Finished** button.

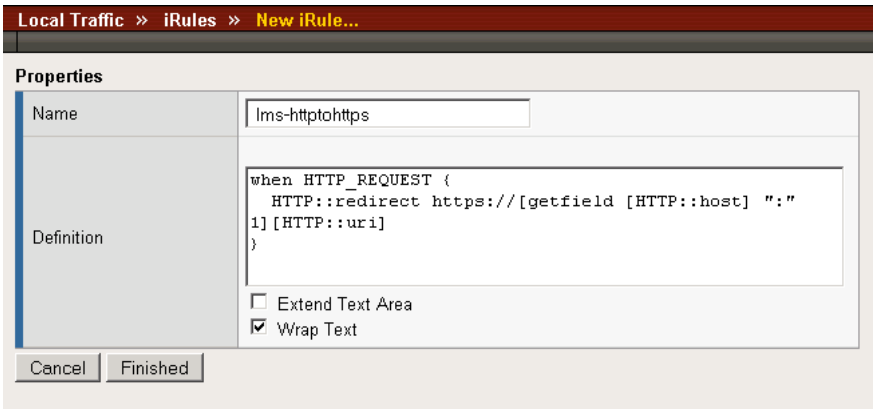

Figure 8 *Creating the iRule*

Modifying the HTTP virtual server

The next task is to modify the HTTP virtual server you created in *Creating the virtual server*, on page 9 to use the iRule you just created.

To modify the existing LMS virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the Virtual Server list, click the LMS virtual server you created in the *Creating the virtual server* section.
   In our example, we click **lms-http-vs**.
3. On the menu bar, click **Resources**.
   The Resources page for the virtual server opens.
4. From the **Default Pool** list, select **None**.
   This virtual server no longer requires the load balancing pool, as traffic is redirected to the HTTPS virtual server we create in the following procedure.
5. Click the **Update** button.
6. In the iRules section, click the **Manage** button.
   The Resource Management screen opens.

7. From the **Available** list, select the iRule you created in the *Creating the Redirect iRule* section, and click the Add (**<<**) button.
   In our example, we select **lms-httptohttps**.
8. Click the **Finished** button.

Creating the HTTPS virtual server

The final task in this section is to create a HTTPS virtual server.

To create a new HTTPS virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **lms-https-vs**.
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 **192.168.104.146**.
6. In the **Service Port** box, type **443** or select **HTTPS** from the list.
7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. Leave 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 the TCP profile* section. In our example, we select **lms-tcp**.
10. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **lms-http**.
    Make sure you have the Rewrite Redirect box checked in the HTTP profile as described in Step 5 of *Creating an HTTP profile*.
11. From the **SSL Profile (Client)** list, select the name of the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **lms-clientssl**.
12. From the **SNAT Pool** list, select **Automap**.
13. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **lms-http-pool**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating the persistence profile*. In our example, we select **lms-cookie**.
15. Click the **Finished** button.

Synchronizing the BIG-IP LTM configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration using the Configuration utility

1. On the Main tab, expand **System**.
2. Click **High Availability**.
   The Redundancy screen opens.
3. On the Menu bar, click **ConfigSync**.
4. Click the **Self --> Peer** button.
   The configuration synchronizes with its peer.