DEPLOYMENT GUIDE
Version 1.2

Deploying the BIG-IP System v10 with Microsoft IIS 7.0 and 7.5

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see https://f5.com/solutions/deployment-guides.

Microsoft® Partner

Table of Contents

1

Deploying the BIG-IP System v10 with Microsoft Internet Information Services 7.0

- Configuring the BIG-IP LTM system for IIS
- Running the Microsoft IIS application template
- Creating the OneConnect profile
- Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5
- SSL Certificates on the BIG-IP system

Deploying the BIG-IP system v10 with Microsoft IIS

F5's BIG-IP system can increase the existing benefits of deploying Microsoft's Internet Information Services (IIS) to provide enterprises, managed service providers, and e-businesses an easy-to-use solution for deploying, managing and securing global and local area traffic.

The BIG-IP system provides a number of ways to accelerate, optimize, and scale Microsoft IIS deployments. When BIG-IP LTM relieves IIS 7.0 and 7.5 servers from tasks such as compression, caching, and SSL processing, each server is able to devote more resources to running applications and can service more user requests.

New in version 10.0 of the BIG-IP system are Application Ready Templates. These application templates ease the process of configuring the BIG-IP system. Instead of having to individually create each object that pertains to the type of application traffic you want the BIG-IP system to manage, you can run an application template. The application template automatically creates BIG-IP system objects that are customized for that application. These objects can be either local traffic objects, TMOS objects, or both.

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

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:

- We recommend the latest version of Microsoft IIS. This Deployment Guide has been tested with IIS 7.0 and 7.5.
- For this deployment guide, the BIG-IP LTM system must be running version 10.0 or later. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.
- If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *SSL Certificates on the BIG-IP system*, on page 13.

- While we strongly recommend using the application template, you can also manually configure the BIG-IP system. For more information, see chapter 2, *Manually configuring the BIG-IP LTM for IIS*, on page 2-1 and chapter 3, *Manually configuring the WebAccelerator module for IIS*, on page 3-1.

Important

All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM and WebAccelerator)	10.0
Microsoft IIS	7.0, 7.5

Revision history:

Version	Description
1.0	New deployment guide
1.1	Added support for BIG-IP v10.1
1.2	Added optional procedure for enabling **X-Forwarded-For** on the BIG-IP LTM, and the section *Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5*, on page 1-11 for instructions on configuring IIS to log the client IP address.
1.3	Modified the optional section on using X-Forwarded-For to log the client IP address in IIS 7 and 7.5 to include installing the Custom Logging service role, and steps for editing the IIS Log Definition to include the X-Forwarded-For header (3-13-2012)

Configuration example

In this Deployment Guide, the BIG-IP system is optimally configured to optimize and direct traffic to IIS servers. Figure 1.1 shows a logical configuration example with a redundant pair of BIG-IP LTM devices running the WebAccelerator module, in front of a group of IIS servers.

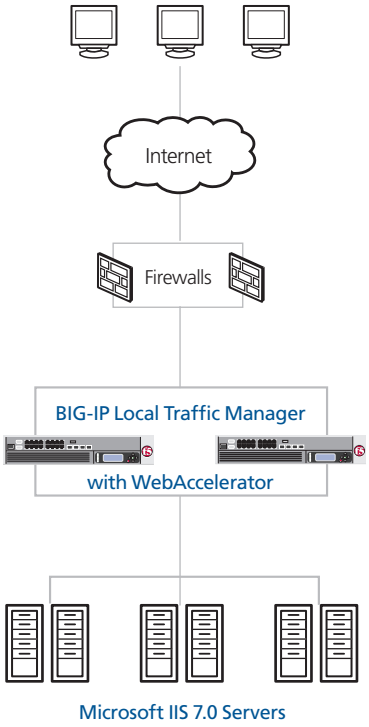

Figure 1.1 *Logical configuration example*

Configuring the BIG-IP LTM system for IIS

You can use the new application template feature on the BIG-IP system to efficiently configure a set of objects corresponding to Microsoft IIS. The template uses a set of wizard-like screens that query for information and then creates the required objects. For example, depending on the settings you specify, this template creates two virtual servers, one HTTPS profile, two TCP profiles, one Persistence profile, one Client SSL profile, one iRule, one pool, and one HTTP monitor. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

Important

Although the template version only states 7.0 for IIS, the template works for IIS version 7.5 without modification.

Note

Depending on which modules are licensed on your BIG-IP system, some of the options in the template may not appear.

Running the Microsoft IIS application template

To run the Microsoft IIS application template, use the following procedure.

To run the Microsoft IIS application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **Microsoft IIS**. The Microsoft IIS application template opens.
4. In the Virtual Server Questions section, complete the following:
   a) You can type a unique prefix for your Microsoft IIS objects that the template will create. In our example, we leave this setting at the default, **my_iis**.
   b) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step a>_virtual_server**. In our example, we type **192.168.10.120**.
   c) If the servers use a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

   If the BIG-IP system should translate the client's source address

to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system will use SNAT automap. See the Online Help for more information.
In our example, we leave this at the default setting: **No**.

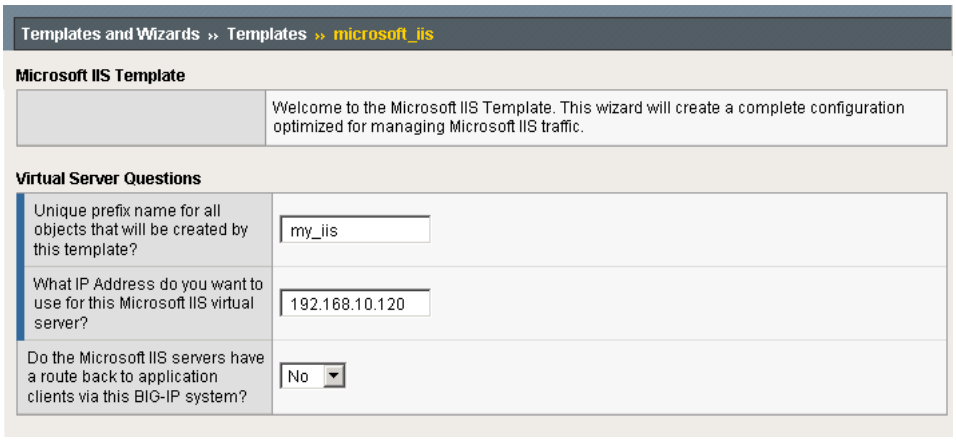

Figure 1.2 *Running the Microsoft IIS application template*

5. In the SSL Offload section, complete the following

   a) If you are not using the BIG-IP system to offload SSL, leave this setting at the default, **No**. Continue with Step 6.

   If you are using the BIG-IP system to offload SSL from the IIS devices, select **Yes** from the list. The SSL options appear.

   b) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-13.

   c) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-13.

   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***.

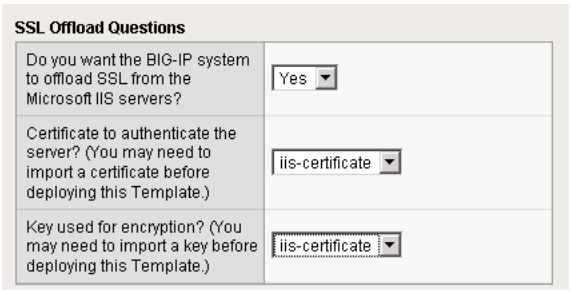

Figure 1.3 *Configuring the BIG-IP system for SSL Offload*

6. In the Load Balancing Questions section, complete the following:

   a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.

   b) Next, add each of the Microsoft IIS devices that are a part of this deployment.
   In the **Address** box, type the IP address of the first IIS device. In our example, we type **10.132.81.100**.
   In the **Service Port** box, type the appropriate port, or select it from the list. In our example, we select **HTTP** from the list.
   Click the **Add** button. Repeat this step for each of the IIS devices.

   c) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.

   d) If you have a specific HTTP request you would like to add to the health check, type it in the box after **GET /**. This is optional. Note that HTTP 1.1 headers are added to the GET by default

   e) Select the HTTP version that the Microsoft IIS servers expect clients to use. In our example, we **Version 1.1**.

   A new row appears asking for the fully qualified DNS name (FQDN) that clients use to access IIS. In the box, type the FQDN for your IIS deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **iis.siterequest.com**.

   f) If you entered an HTTP request in step d, and want to enter a response string, type it here. This is optional.

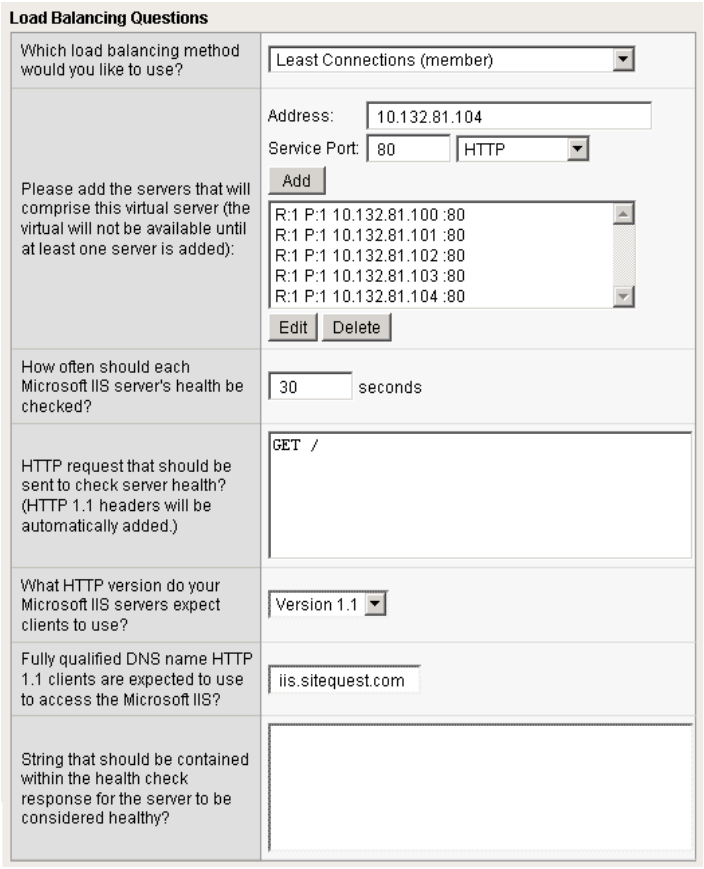

Figure 1.4 *Configuring the Load Balancing options*

7. In the Protocol and Security Questions section, complete the following

   a) If most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list.
   This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.

   b) If you want to use the WebAccelerator module to accelerate the Microsoft IIS traffic, select **Yes** from the list. If you do not want to use the WebAccelerator, select **No**. This option does not appear if you do not have the WebAccelerator module licensed. The WebAccelerator module can significantly improve performance for IIS deployments.

   c) If you are using the WebAccelerator module, in the **Host** box, type the fully qualified DNS name (FQDN) that your users will use to access the Microsoft IIS deployment (the WebAccelerator

application object's Requested Hosts field). Click the **Add** button. If you have additional host names, type each one in the **Host** box, followed by clicking the **Add** button.
In our example, we type **iisapplication.f5.com** and click the **Add** button.

8. Click the **Finished** button.

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created, similar to the following. If you are not offloading SSL, or using WebAccelerator, you do not have all of these items in your list.:

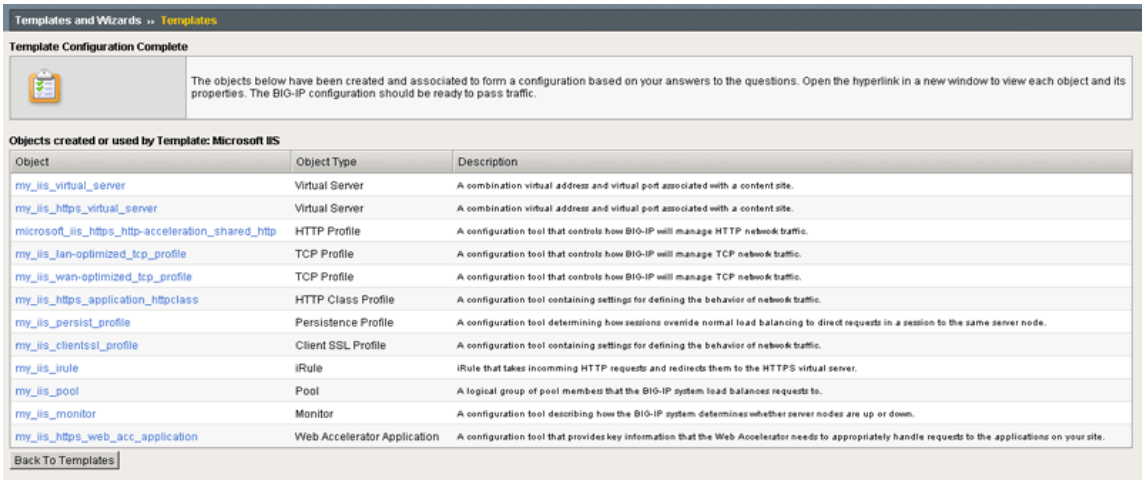

Figure 1.5 *The Summary page of the IIS Application Template showing the items created*

Creating the OneConnect profile

One profile we recommend using for Microsoft IIS that is not yet part of the application template is the OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. This can provide significant performance improvements for IIS implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

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

In this section, we first create the OneConnect profile, then associate it with the virtual servers that were created by the Application template.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **iis-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

The next task is to associate the OneConnect profile you just created with the virtual server(s) that were created by the Application Template. If you are not using the BIG-IP system to offload SSL, there is only one virtual server to modify; if you are offloading SSL, there are two.

To modify the existing IIS 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, find the HTTP virtual server that begins with the prefix you specified in step 4a. In our example, we left the prefix at the default, so we click **my_iis-virtual_server**.
3. In the Configuration section, from the **OneConnect Profile** list, select the name of the profile you just created. In our example, we select **iis-oneconnect**.
4. Click the **Update** button.

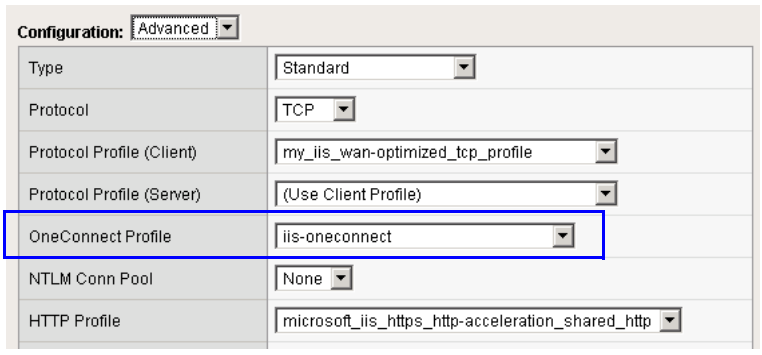

Figure 1.6 *Updating the virtual server to use the OneConnect profile*

If you are using the BIG-IP system to offload SSL, repeat this procedure, but in step 2 select the HTTPS virtual server (it includes both the prefix you specified earlier, and is followed by **_https_**). In our example, we click **my_iis_https_virtual_server**, and add our OneConnect profile.

Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5

When you configure BIG-IP LTM to use SNAT, the BIG-IP system replaces the source IP address of an incoming connection with its local self IP address (in the case of SNAT **Automap**), or an address you have configured in a SNAT pool. As a result, Microsoft IIS logs each connection with its assigned SNAT address, rather than the address of the client. By configuring an HTTP profile on the BIG-IP to insert an ***X-Forwarded-For*** header, the original client IP address is sent as well; however, in default IIS configuration, this information is not logged.

Beginning with IIS 7, Microsoft provides an optional Advanced Logging Feature for IIS that allows you to define custom log definitions that can capture additional information such as the client IP address included in the X-Forwarded-For header.

You must first enable X-Forwarded-For in the BIG-IP HTTP profile, and then add the log field to IIS.

Modifying the HTTP profile to enable X-Forwarded-For

The first task is to modify the HTTP profile created by the application template to enable the X-Forwarded-For header.

To modify the HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. From the HTTP profile list, select the profile created by the template. It is one of the following: **microsoft_sharepoint_http-wan-optimized-caching_shared_http** **microsoft_sharepoint_http-lan-optimized-caching_shared_http**.
3. In the Settings section, on the **Insert X-Forwarded-For** row, click the **Custom** box. From the list, select **Enabled**.
4. Click the **Update** button.

Deploying the Custom Logging role service

The next task is to deploy the Custom Logging role service. If you do not deploy this role service, you may receive a "Feature not supported" error when trying to edit the log definition in the next section.

To deploy the Custom Logging role service

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open Server Manager.
2. In the Navigation pane, expand **Roles**.
3. Right-click **Web Server**, and then click **Add Role Services**.

4. Under *Health and Diagnostics*, check the box for **Custom Logging**, and then click the **Next** button.
5. On the Confirmation page, click **Install**.
6. After the service has successfully installed, click the **Close** button.

Adding the X-Forwarded-For log field to IIS

Before beginning the following procedure, you must have installed IIS Advanced Logging. For installation instructions, see ***http://www.iis.net/community/files/media/advancedlogging_readme.htm***

◆ Note

If you are using IIS version 6, F5 has a downloadable ISAPI filter that performs a similar function to the Advanced Logging Feature discussed here. For information on that solution, see the DevCentral post at ***http://devcentral.f5.com/weblogs/Joe/archive/2009/08/19/x_forwarded_for_log_filter_for_windows_servers.aspx***

To add the X-Forwarded-For log field to IIS

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open the Internet Information Services (IIS) Manager.
2. From the Connections navigation pane, click the appropriate server, web site, or directory on which you are configuring Advanced Logging. The Home page appears in the main panel.
3. From the Home page, under IIS, double-click **Advanced Logging**.
4. From the Actions pane on the right, click **Edit Logging Fields**.
5. From the Edit Logging Fields dialog box, click the **Add Field** button, and then complete the following:
   a) In the **Field ID** box, type **X-Forwarded-For**.
   b) From the **Category** list, select **Default**.
   c) From the **Source Type** list, select **Request Header**.
   d) In the **Source Name** box, type **X-Forwarded-For**.
   e) Click the **OK** button in the Add Logging Field box, and then click the **OK** button in the Edit Logging Fields box.
6. Click a Log Definition to select it. By default, there is only one: %COMPUTERNAME%-Server. The log definition you select must have a status of Enabled.
7. From the Actions pane on the right, click **Edit Log Definition**.
8. Click the **Select Fields** button, and then check the box for the **X-Forwarded-For** logging field.
9. Click the **OK** button.
10. From the Actions pane, click **Apply**.

11. Click **Return To Advanced Logging**.
12. In the Actions pane, click **Enable Advanced Logging**.

Now, when you look at the logs, the client IP address is included.

SSL Certificates on the BIG-IP system

This section is optional, you only need to perform these procedures if you are using the BIG-IP system to offload SSL from the IIS deployment, and have not yet imported a certificate and key.

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 Microsoft IIS 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.

2

Manually Configuring the BIG-IP LTM for Microsoft IIS

- Creating the HTTP health monitor
- Creating the pool
- Creating profiles
- Creating the virtual server
- Using SSL certificates and keys
- Configuring the BIG-IP LTM to offload SSL

Manually configuring the BIG-IP LTM for IIS

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system, perform the following procedures.

Creating the HTTP health monitor

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

To create a health monitor

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 **iis-http-monitor**.
4. From the **Type** list, select **http**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a (1:3) +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91** (see Figure 2.1).
6. In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.
   The new monitor is added to the Monitor list.

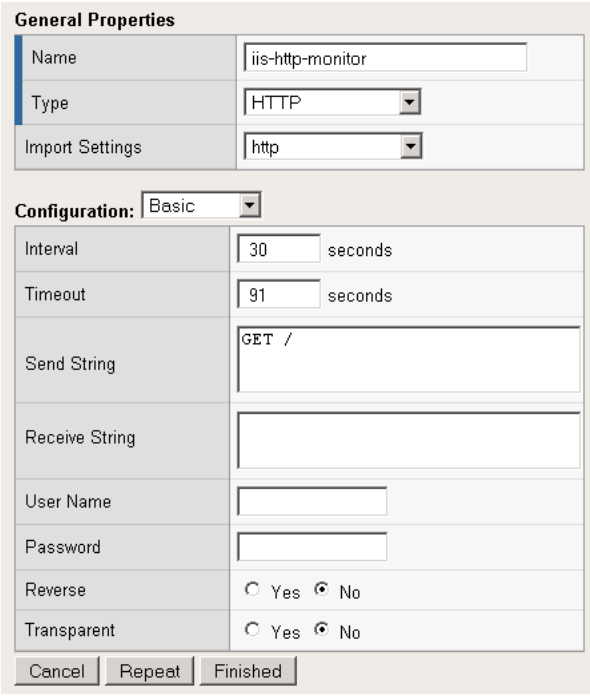

Figure 2.1 *Creating the HTTP Monitor*

Creating the pool

The first step is to define a load balancing pool for the IIS servers. A BIG-IP 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 IIS 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. In the **Name** box, type a name for your pool.
   In our example, we use **iis-http-pool**.
4. 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 **iis-http-monitor**.
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 our example, we select **Least Connections (node)**.
6. In this pool, we leave the Priority Group Activation **Disabled**.

7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the first Microsoft IIS server to the pool. In our example, we type **10.132.81.100**.
9. In the **Service Port** box, type **80** or select **HTTP** from the list.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each server you want to add to the pool. In our example, we repeat these steps five times for the remaining servers, **10.132.81.101 - .105**.
12. Click the **Finished** button (see Figure 2.2).

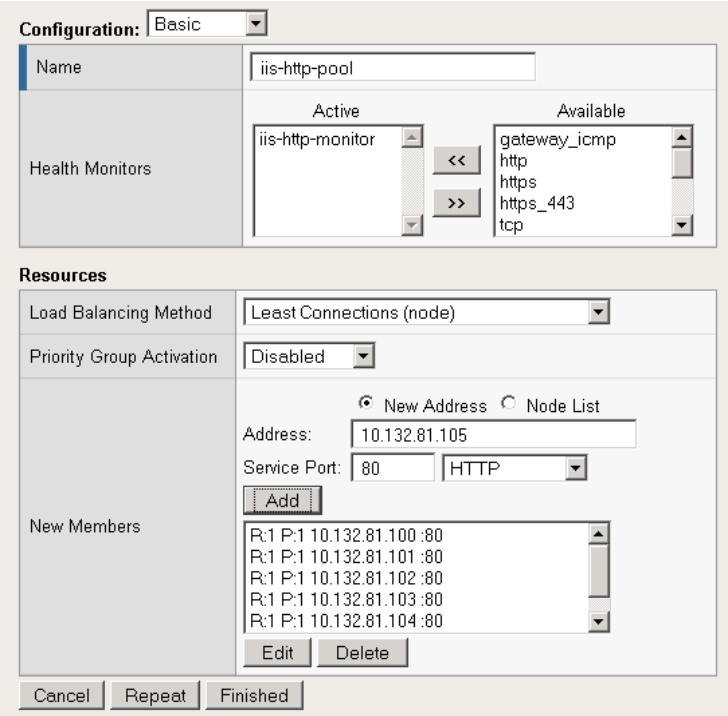

Figure 2.2 *Creating the pool for the IIS servers*

Creating profiles

The BIG-IP system use configuration objects called 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. In the following example, we base our HTTP profile off of the **http-acceleration** parent profile, as we are using the WebAccelerator. If you are not using the WebAccelerator, we recommend using the **http-wan-optimized-compression-caching** parent.

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 **iis-http-opt**.
4. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**.
   If you are using the WebAccelerator module, select **http-acceleration**.
5. *Optional:* If you 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 2-9 for more information.
6. *Optional:* If you want to enable the X-Forwarded-For header for accurate logging, check the Custom box for **Insert X-Forwarded-For**, and from the list, select **Enabled**. See *Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5*, on page 1-11 for detailed information, including modifications to IIS to accurately log the client IP address.
7. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Microsoft IIS users are accessing the devices via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the users are accessing the system from

remote or home offices, we recommend using an additional TCP profile, called **tcp-wan-optimized** (for client side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the LAN optimized TCP profile

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

To create a new 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 **iis-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the WAN optimized TCP profile

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

To create a new TCP WAN optimized 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 **iis-tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating persistence profile

The next profile we create is a Persistence profile. We recommend using persistence for Microsoft IIS devices, although the type of persistence depends on your configuration. In our example, use 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**.
   The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
   The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **iis-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.

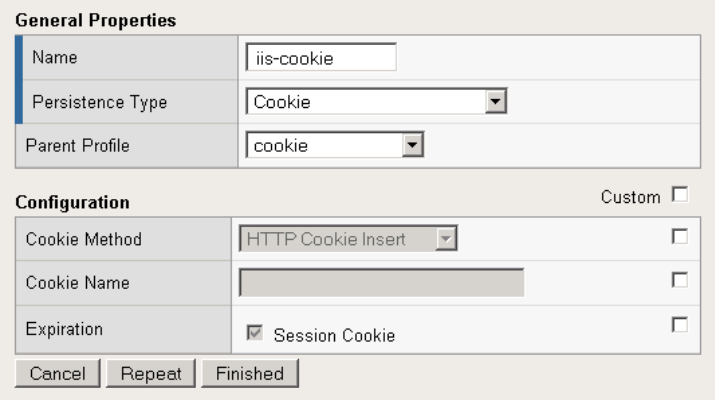

Figure 2.3 *Creating the cookie persistence profile*

Creating a OneConnect profile

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

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

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
   The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**.
   The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
   The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **iis-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating 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 **iis-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.

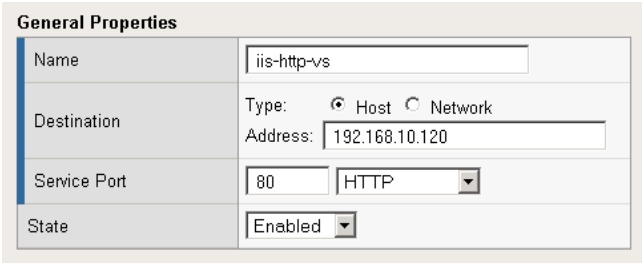

Figure 2.4 *Creating the IIS virtual server*

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 WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **iis-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **iis-tcp-lan**.
11. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*. In our example, we select **iis-oneconnect**.
12. 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 **iis-http-opt**.

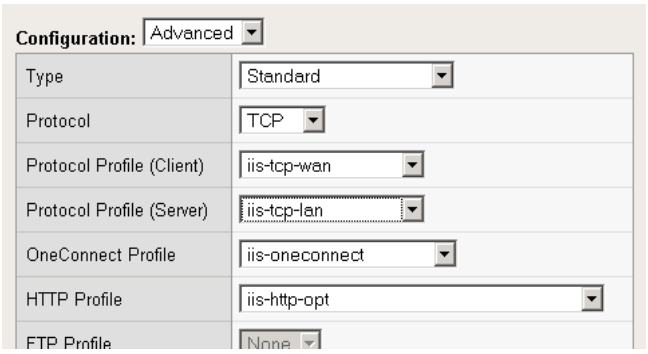

Figure 2.5 *Selecting the Microsoft IIS profiles for the virtual server*

13. 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 **iis-http-pool**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profile* section. In our example, we select **iis-cookie**.

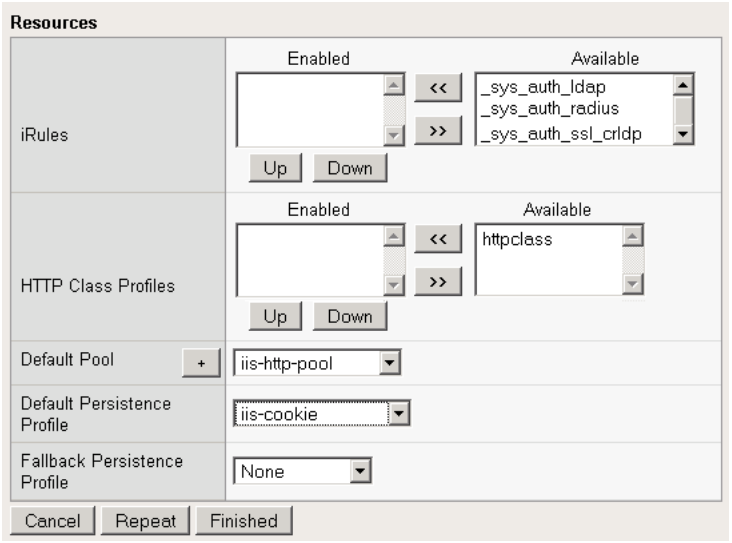

Figure 2.6 *Adding the Pool and Persistence profile to the virtual server*

15. Click the **Finished** button.
The BIG-IP LTM HTTP configuration for the Microsoft IIS 7.0 deployment is now complete. If you are using the BIG-IP system to offload SSL, continue with the following section.

Configuring the BIG-IP LTM to offload SSL

If you are using the BIG-IP LTM system to offload SSL from the Microsoft IIS devices, 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 configure the iRule or 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 Microsoft IIS 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 **iis-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 **iis-httptohttps**.
4. In the Definition section, copy and paste the following iRule:

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

5. Click the **Finished** button (see Figure 2.7).

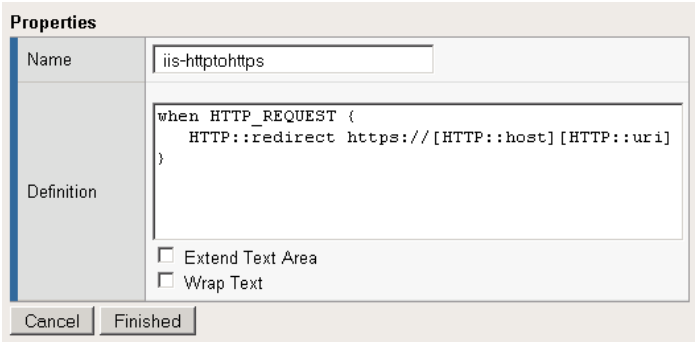

***Figure 2.7** Creating the iRule*

Modifying the HTTP virtual server

The next task is to modify the HTTP virtual server you created in *Creating the virtual server*, on page 2-7 to use the iRule you just created.

To modify the existing IIS 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 IIS virtual server you created in the *Creating the virtual server* section.
   In our example, we click **iis-http-vs**.
3. On the menu bar, click **Resources**.
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 **iis-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.
3. In the **Name** box, type a name for this virtual server. In our example, we type **iis-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**.
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 WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **iis-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **iis-tcp-lan**.
11. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*. In our example, we select **iis-oneconnect**.
12. 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 **iis-http-opt**.
    Make sure you have the Rewrite Redirect box checked in the HTTP profile as described in Step 5 of *Creating an HTTP profile*.
13. 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 **iis-clientssl**.
14. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **iis-http-pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profile*. In our example, we select **iis-cookie**.
16. Click the **Finished** button.

This completes the BIG-IP LTM configuration.

3

Manually Configuring the BIG-IP WebAccelerator for IIS 7.0

- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application

Manually configuring the WebAccelerator module for IIS

In this chapter, we provide procedures for manually configuring the WebAccelerator module for the IIS 7.0 devices to increase performance for end users. The F5 WebAccelerator is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

Note that we recommend using the application template as opposed to configuring the WebAccelerator manually.

For more information on the F5 WebAccelerator, see **www.f5.com/products/big-ip/product-modules/webaccelerator.html**.

Prerequisites and configuration notes

The following are prerequisites for this section:

- We assume that you have already configured the BIG-IP LTM system for directing traffic to the IIS deployment as described in this Deployment Guide.
- You must have purchased and licensed the WebAccelerator module on the BIG-IP system.
- You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (*Creating an HTTP profile*, on page 2-4) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (we recommend HTTP Acceleration) and associate it with the virtual server.
- This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Microsoft IIS 7.0. Consult the appropriate documentation for detailed information.

Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to Microsoft IIS servers. The BIG-IP LTM with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency accesses an IIS server via the WebAccelerator. The user's request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so that they can be served quickly without requiring the server to re-serve the same objects.

Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile and creating an Application. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the ***WebAccelerator Administrator Guide*** for more information.

Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

To create a new HTTP class profile

1. On the Main tab, expand **WebAccelerator**, and then click **Classes**. The HTTP Class Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Class Profile screen opens.
3. In the **Name** box, type a name for this Class. In our example, we type **iis-class**.
4. From the Parent Profile list, make sure **httpclass** is selected.
5. In the Configuration section, from the **WebAccelerator** row, make sure **Enabled** is selected.
6. In the Hosts row, from the list select **Match Only**. The Host List options appear.
   a) In the **Host** box, type the host name that your end users use to access the IIS devices. In our example, we type **iis-application.f5.com/** (see Figure 3.1).
   b) Leave the Entry Type at **Pattern String**.
   c) Click the **Add** button.
   d) Repeat these sub-steps for any other host names users might use to access the IIS deployment.
7. The rest of the settings are optional, configure them as applicable for your deployment.
8. Click the **Finished** button. The new HTTP class is added to the list.

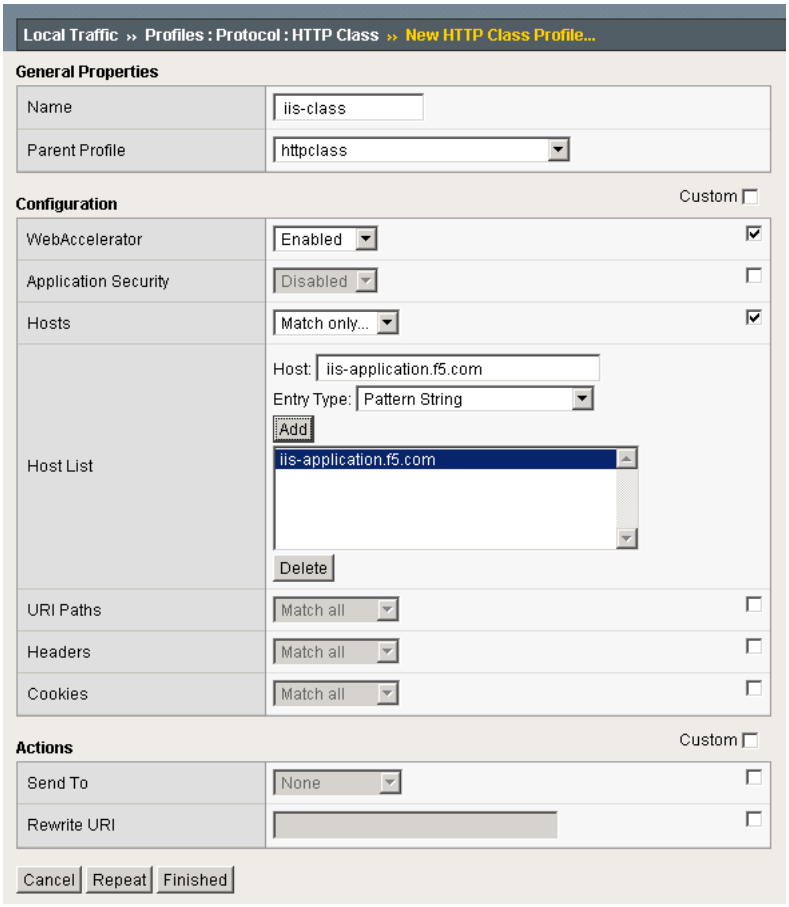

Figure 3.1 *Creating a new HTTP Class profile*

Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your IIS deployment on the BIG-IP LTM system to use the HTTP Class profile you just created.

To modify the Virtual Server to use the Class profile

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 name of the virtual server you created for the IIS servers. In our example, we click **iis-http-vs**. The General Properties screen for the Virtual Server opens.
3. On the Menu bar, click **Resources**.
4. In the HTTP Class Profiles section, click the **Manage** button.

5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (**<<**) button to move it to the Enabled box. In our example, we select **iis-class**.
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.

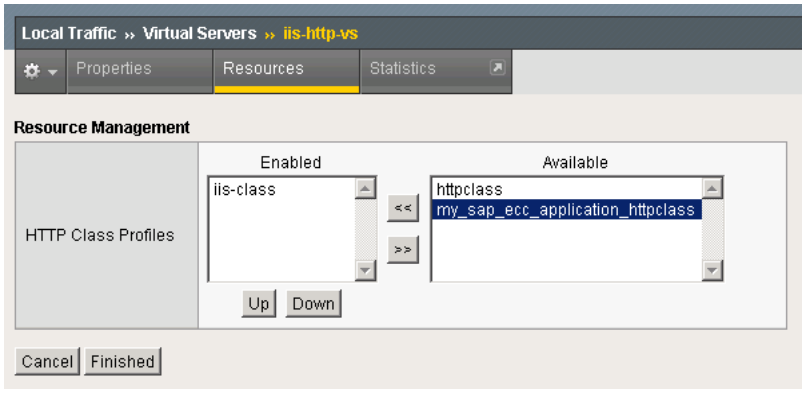

Figure 3.2 *Adding the HTTP Class to the Virtual Server*

Important

*You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (***Creating an HTTP profile***, on page 2-4) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (such as HTTP Acceleration), and modify the virtual server to use this new profile.*

To create the HTTP profile, use **Creating an HTTP profile***, on page 2-4, selecting the HTTP Acceleration parent profile. You must leave RAM Cache enabled; all other settings are optional. To modify the virtual server, follow Steps 1 and 2 from the preceding procedure to access the virtual server, and then from the HTTP Profile list, select the name of the new profile you just created and click* ***Update****.*

Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

To create a new Application

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**.
   The Application screen of the WebAccelerator UI opens in a new window.
2. Click the **New Application** button.
3. In the Application Name box, type a name for your application. In our example, we type **Microsoft IIS**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select **Microsoft Internet Information Services (IIS)**. This is a pre-defined policy created specifically for Microsoft IIS devices (see Figure 3.3).
6. In the **Requested Host** box, type the host name that your end users use to access the IIS deployment. This should be the same host name you used in Step 6a in the preceding procedure. In our example, we type **iisapplication.f5.com**.
   If you have additional host names, click the **Add Host** button and enter the host name(s).
7. Click the **Save** button.

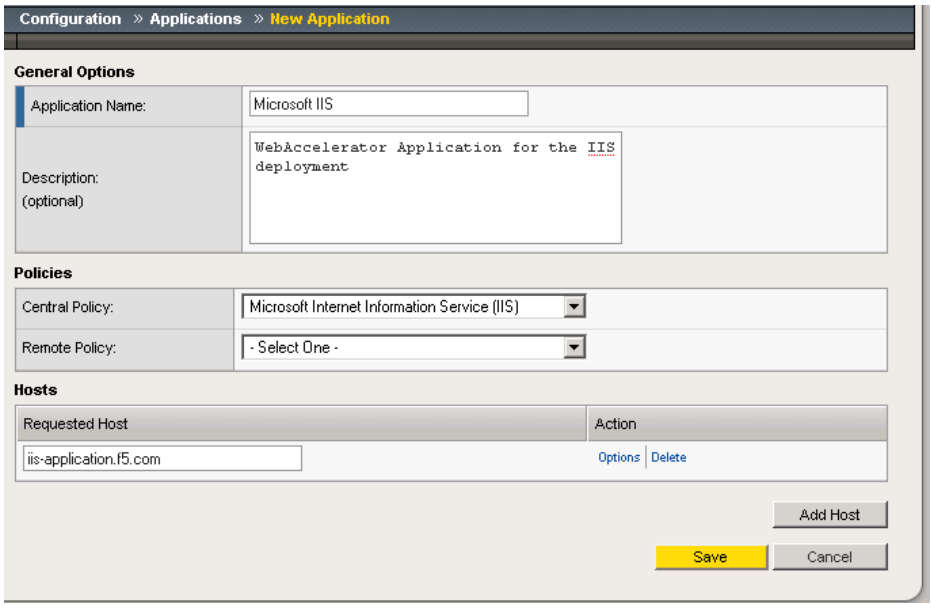

Figure 3.3 *Configuring an Application on the WebAccelerator*

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice a marked improvement in performance after their first visit.