Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support.

Deployment Guide

Document version 1.1

For a list of current guides, see https://f5.com/solutions/deployment-guides.

Deploying the BIG-IP System v11 with Microsoft Internet Information Services

Welcome to the F5 and Microsoft® Internet Information Services (IIS) Deployment Guide. This document contains guidance on configuring the BIG-IP system version 11 for Microsoft IIS versions 7.0, 7.5 and 8.0, resulting in a secure, fast, and available deployment.

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy way to configure the BIG-IP system for Microsoft IIS.

Why F5?

The BIG-IP system provides a number of ways to accelerate, optimize, and scale Microsoft IIS deployments. When BIG-IP LTM relieves IIS 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.

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

Visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: *http://devcentral.f5.com/Microsoft/*.

Products and versions tested

Product	Version
BIG-IP LTM	v11
Microsoft IIS Server	7.0, 7.5, 8.0

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/microsoft-iis-iapp-dg.pdf*

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for Microsoft IIS acts as the single-point interface for building, managing, and monitoring IIS.

Microsoft® Partner Network

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network: http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

➤ You must be familiar with both F5 devices and Microsoft IIS. For more information on configuring these devices, consult the appropriate documentation.

➤ For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.

➤ This document provides guidance for using the iApp for Microsoft IIS 7 and 7.5 found in version 11.0 and later. The same iApp can be used for Microsoft IIS 8 without modification. For users familiar with the BIG-IP, there is a manual configuration table at the end of this guide. However, we recommend using the iApp template.

➤ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, and it is installed on the BIG-IP LTM system.

➤ After completing the iApp, there are optional procedures in *Appendix A: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 11* and *Appendix B: Configuring WMI monitoring for IIS Servers (optional) on page 13.*

➤ This deployment guide contains guidance on optional modules, including Application Visibility Reporting and WebAccelerator. To take advantage of these modules, they must be licensed and provisioned before starting the iApp template. For more information on licensing modules, contact your sales representative. Note that AVR is licensed on all systems, but must be provisioned before beginning the iApp template.

Configuration example

In this Deployment Guide, the BIG-IP system is optimally configured to optimize and direct traffic to IIS servers. The following traffic flow diagram shows a logical configuration example with a redundant pair of BIG-IP LTM devices running the optional WebAccelerator module, in front of a group of IIS servers.
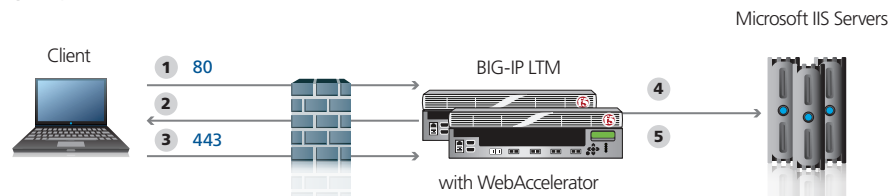
Traffic Flow*:*

1. The client makes a connection to the BIG-IP virtual server IP Address for Microsoft IIS.

2. Depending on the configuration, the BIG-IP LTM may use an iRule to redirect the client to an encrypted (HTTPS) form of the resource.

3. The client machines makes a new connection to the BIG-IP virtual server IP address of the Microsoft IIS server to access the resource over an encrypted connection.

4. The BIG-IP LTM chooses the best available IIS server based on the load balancing algorithm and health monitoring.

5. The BIG-IP LTM uses persistence to ensure the clients persist to the same server if applicable.

Preparation Worksheet

In order to use the iApp for Microsoft IIS, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

You might find it useful to print this table and then enter the information.

➲ **Note:** *Although we show space for 10 pool members, you may have more or fewer members in each pool.*

IP Addresses/FQDN	SSL Offload	Pool Members	Sync/Failover Groups*	TCP request queuing*	WAN or LAN clients
IP address you will use for the LTM virtual server: FQDN that will resolve to the virtual server address:	*Offloading SSL?* Yes | No If offloading SSL, import a certificate and key into the BIG-IP LTM before running the template. Certificate: Key:	IIS server IP addresses: 1: 2: 3: 4: 5: 6: 7: 8: 9: 10: Port used by IIS:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node. Request queue length: Timeout: Node Connection limit:	Most clients connecting through BIG-IP to IIS are coming over a: LAN WAN

Optional Modules (you must have provisioned modules before running the template)	
*Application Visibility Reporting (AVR)**	*WebAccelerator**
If using AVR, we strongly recommend you first create an custom Analytics profile before running the template. Analytics profile name:	All FQDNs for IIS: 1: 2: 3: 4: 5:

* Optional

3

Configuring the BIG-IP iApp for Microsoft IIS

Use the following guidance to help you configure the BIG-IP system for Microsoft IIS using the BIG-IP iApp template.

Getting Started with the iApp for Microsoft IIS

To begin the Microsoft IIS iApp Template, use the following procedure.

1. Log on to the BIG-IP system.

2. On the Main tab, expand **iApp**, and then click **Application Services**.

3. Click **Create**. The Template Selection page opens.

4. In the **Name** box, type a name. In our example, we use **Microsoft-iis_**.

5. From the **Template** list, select **f5.microsoft_iis**.
    The Microsoft IIS template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**
    If you want to configure the Application for Sync or failover groups, select **Yes** from the list.

    a. **Device Group**
        If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.

    b. **Traffic Group**
        If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Analytics

This section of the template asks questions about Analytics. The Application Visibility Reporting (AVR) module allows you to view statistics specific to your Microsoft IIS implementation. AVR is available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. Note that these are only for application visibility reporting, you can view object-level statistics from the BIG-IP without provisioning AVR.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile before beginning the template. To create a new profile, from the Main tab, select Profiles and then click Analytics. Click New and then configure the profile as applicable for your configuration. See the online help or product documentation for specific instructions.

1. **Enable Analytics**
    Choose whether you want to enable AVR for Analytics.

2. **Analytics Profile**
    You must decide whether to use the default Analytics profile, or create a new one. As

mentioned previously, we recommend creating a new profile to get the most flexibility and functionality out of AVR. If you choose to create a new profile after starting the template, you must exit the template, create the profile, and then restart the template.

To use the default Analytics profile, choose Use **Default Profile** from the list.

To choose a custom profile, leave the list set to **Select a Custom Profile**, and then from the Analytics profile list, select the custom profile you created.

Virtual Server Questions

The next section of the template asks questions about the BIG-IP virtual server. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions.

1. **IP address for the virtual server**
    This is the address clients use to access Microsoft IIS (or a FQDN will resolve to this address). You need an available, external IP address to use here.

2. **Routes or secure network address translation**
    If the IIS servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, the BIG-IP uses Secure Network Address Translation (SNAT) Automap (exception in #3) to translate the client's source address to an address configured on the BIG-IP. The servers then use this new source address as the destination address when responding to traffic originating through the BIG-IP.

    If you indicate the IIS servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the IIS servers.

    We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.

    If you are configuring your BIG-IP LTM in a "one-armed" configuration with your IIS servers -- where the BIG-IP virtual server(s) and the IIS servers have IP addresses on the same subnet – you must choose No.

3. **More than 64,000 simultaneous connections**
    If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #4.

    If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.

4. **NTLM**
    If you have configured the IIS servers to use NTLM authentication, select Yes from the list. If the IIS servers do not use NTLM, leave the list set to No.

SSL Encryption questions

Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the **Configuration Guide for BIG-IP Local Traffic Manager** *available at http://support.f5.com/kb/en-us.html*.

To configure the BIG-IP to offload SSL, select **Yes** from the list.

1. **Certificate**
   Select the certificate for you imported for IIS from the certificate list.

2. **Key**
   Select the associated key from the list.

Server Pool, Load Balancing, and Service Monitor questions

In this section, you add the Microsoft IIS servers, and configure the health monitor and pool.

1. **New Pool**
   Choose **Create New Pool** unless you have already made a pool on the LTM for the IIS devices.

2. **Load balancing method**
   While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

   (i) Tip ➝ If you want to implement the Windows Management Interface (WMI) monitor, as described in *Appendix B: Configuring WMI monitoring for IIS Servers (optional) on page 13*, you must select **Dynamic Ratio (Node)**.

3. **Address/Port**
   Type the IP Address and Port for each IIS server. You can optionally add a Connection Limit (see note on the left). Click **Add** to add additional servers to the pool.

4. **TCP Request Queuing**
   TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the **BIG-IP Local Traffic Manager: Implementations** guide, available on Ask F5.

   Important ➝ *TCP Request Queuing is an advanced feature and should be used only if you understand how it will affect your deployment, including application behavior and BIG-IP performance. If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port for the Client Access Server nodes.*

   If you want the BIG-IP to queue TCP requests, select **Yes** from the list. Additional options appear.

    a. Type a queue length in the box. We do not recommend 0 for unlimited.

    b. Type a number of milliseconds for the timeout value.

5. **Health Monitor**
Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the IIS devices.

6. **Interval**
Specifies how often the system checks the health of the servers. We recommend the default of 30 seconds.

7. **HTTP Request**
This is optional. You can configure the template to retrieve a specific page by typing the path here. Leaving the default (GET /) marks the node up if anything is returned from the web page.

8. **HTTP version**
Unless the majority of your users are using HTTP 1.0 (not common), we recommend selecting **Version 1.1** from the list.

- FQDN: When you select Version 1.1, a new row appears asking for the FQDN the clients use to access Microsoft IIS. Type it here.

9. **Monitor response string**
Optional. If you configured a unique HTTP Request, this is where you enter the expected response.

Protocol Optimization Questions

In this section, you configure protocol optimizations.

1. **WAN or LAN**
Specify whether most clients are connecting over a WAN or LAN. Because most IIS clients are likely to be coming over the WAN, we recommend selecting WAN (the default).

2. **WebAccelerator**
If you have licensed and provisioned the WebAccelerator module, you have the option of using it for Microsoft IIS. The WebAccelerator provides application acceleration for remote users.

  a. *DNS names*
If you select Yes, an additional row appears in the template asking for the fully qualified domain names used for Microsoft IIS. The BIG-IP system uses these entries for the Requested Hosts field, allowing the WebAccelerator module to accelerate the traffic to these virtual hosts.

In the **Host** box, type the **FQDN**. If you have additional FQDNs, click the **Add** button.

  b. *X-WA-info Header*
By default, the WebAccelerator X-WA-info header is not included in the response from the BIG-IP. This header is useful for debugging WebAccelerator behavior. There are two additional options:
   - Standard: If you choose Standard, the BIG-IP inserts a HTTP header that includes numeric codes which indicate if and how each object was cached.

- Debug: If you choose Debug, the BIG-IP includes extended information which may help for extended troubleshooting.

c. *WebAccelerator Performance monitor*
While the BIG-IP Dashboard provides statistics and performance graphs related to WebAccelerator, you can choose to enable the WebAccelerator performance monitor for legacy WebAccelerator performance monitoring for debugging purposes. The results can be found in the Main tab of the navigation page, under WebAccelerator, by clicking Traffic Reports.
In our example, we leave the performance monitor **Disabled**.

d. *WebAccelerator policy*
For this template, F5 recommends the **Generic Policy - Enhanced** policy to achieve the best results for Web acceleration of IIS traffic. Should F5 publish an updated policy to DevCentral that you have downloaded and imported, or if a custom policy is created for your environment (locally), you can select that custom policy from the list. In our example, we leave the default.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for Microsoft IIS.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the Microsoft IIS service you just created. To see the list of all the configuration objects created to support Microsoft IIS, on the Menu bar, click **Components**. The complete list of all Microsoft related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying the IIS authentication token timeout value

The iApp template configures most health monitors to check service health every 30 seconds. However, to reduce traffic between the IIS servers and domain controllers, IIS virtual directories configured to use Basic authentication cache authentication tokens for up to 15 minutes before re-authenticating the user with Active Directory. This may result in the BIG-IP pool members for these services being marked UP incorrectly while Basic authentication tokens are cached.

You can decrease the length of (or disable) this token caching period by editing the registry on the IIS server. The length of time configured for the token cache combined with the timeout value of the monitor will determine how long it will take until a resource is marked down. For example, setting a token cache period of 60 seconds, combined with a monitor using a timeout value of 91 seconds, will result in a resource being marked down after 151 seconds.

For instructions on modifying the registry, see the following Microsoft article (while this article says IIS 6.0, we tested it on IIS 7.5 with no modifications):

Critical ⟶ *Use extreme caution any time you are editing the registry. Contact Microsoft for specific instructions and/or help editing the registry values.*

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/6b2e7fcd-5fad-4ac8-ac0a-dcfbe771e9e1.mspx

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the Microsoft IIS implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Microsoft IIS Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the IIS configuration objects created by the iApp template. You can get statistics specific to the Application Service if you have provisioned AVR. Otherwise, you can always get object-level statistics.

AVR statistics
If you have provisioned AVR, you can get application-level statistics for your IIS application service.

To view AVR statistics

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the Application Service List, click the Microsoft IIS service you just created.
3. On the Menu bar, click **Analytics**.
4. Use the tabs and the Menu bar to view different statistics for your IIS iApp.

Object-level statistics
If you haven't provisioned AVR, or want to view object-level statistics, use the following procedure.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics, see the online help or product documentation.

Disabling Strict Updates

If you need to manually modify any of the configuration objects created by the template, you must first disable the Strict Updates feature. By disabling Strict Updates, if you re-enter the iApp template and modify the configuration within the iApp, you must make all changes again manually.

You only need to turn off the Strict Updates feature once, unless you have re-enabled it.

To disable Strict Updates

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Microsoft IIS Application service from the list.
3. From the **Application Service** list, select **Advanced**.
4. In the **Strict Updates** row, clear the check from the box to disable Strict Updates.
5. Click the **Update** button.
6. You must restart bigd after making changes that require disabling Strict Updates. You only need to restart bigd once, after making all modifications. See *Restart bigd after making changes that require disabling Strict Updates on page 15*.

Appendix A: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional)

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. The iApp produces an HTTP profile on the BIG-IP system which inserts an X-Forwarded-For header, so 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.

Modifying the HTTP profile to enable X-Forwarded-For

The first task is to modify the HTTP profile created by the template to enable the X-Forwarded-For header. This requires disabling the Strict Updates feature.

To modify the HTTP profile

1. If you have not already disabled Strict Updates, follow *Disabling Strict Updates on page 10*

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

3. From the HTTP profile list, select the profile created by the template. This profile is preceded by the name you gave the iApp, followed by **_http_profile**.

4. In the Settings section, on the **Insert X-Forwarded-For** row, click the **Custom** box. From the list, select **Enabled**.

5. Click the **Update** button.

6. You must restart bigd after making changes that require disabling Strict Updates. You only need to restart bigd once, after making all modifications. See *Restart bigd after making changes that require disabling Strict Updates on page 15*.

Deploying the Custom Logging role service

The first 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. If you receive this error, ensure that you are editing the log definition at the server level in IIS Manager.

The configuration is slightly different depending on which version of IIS you are running. Use the procedure applicable to your version of IIS.

To deploy the Custom Logging role service for IIS 7.0 and 7.5 (Windows Server 2008)

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 **Next**.

5. On the Confirmation page, click **Install**.

6. After the service has successfully installed, click the **Close** button.

To deploy the Custom Logging role service for IIS 8.0 (Windows Server 2012)

1. From your Windows Server 2012 device, open Server Manager.

2. Click **Manage** and then **Add Roles and Features**.

3. Select Role-based or feature-based installation.

4. On the Roles screen, expand **Web Server (IIS)** and **Health and Diagnostics** and then check the box for **Custom Logging**.

5. Click **Next** and then on the Features screen, click **Next** again.

6. Click **Install**.

7. 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

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*

The following procedure is the same for IIS versions 7.0, 7.5, and 8.0.

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

1. From your Windows Server device, open the Internet Information Services (IIS) Manager.

2. From the Connections navigation pane, click the appropriate server 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.

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 **Select Fields**, 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 Advanced Logging logs, the client IP address is included.

Appendix B: Configuring WMI monitoring for IIS Servers (optional)

If you find your IIS servers are under high performance load, you can dynamically load balance between them using F5's Windows Management Interface (WMI) monitor. This monitor checks the CPU, memory, and disk usage of the nodes and, in conjunction with Dynamic Ratio load balancing mode, sends the connection to the server most capable of processing it.

For an overview of the WMI performance monitor, see
http://support.f5.com/kb/en-us/solutions/public/6000/900/sol6914.html.

Installing the F5 WMI handler

The first task is to copy the F5 WMI handler to the Windows Server and configure IIS to use the F5 Data Gathering Agent.

To install the Data Gathering Agent F5.IsHandler.dll on an IIS 7.0, 7.5, or 8.0 server

1. Create a **scripts** directory under the directory **C:\Inetpub**. (**C:\Inetpub\scripts**).

2. Create a **\bin** directory under the scripts directory (**C:\Inetpub\scripts\bin**).

3. Copy the file **F5.IsHandler.dll** to the directory **C:\Inetpub\scripts\bin**.

4. In the **C:\Inetpub\scripts** directory, create the file **web.config**. The following shows an example of this file.

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <configuration>
   <system.webServer>
   <handlers>
   <clear />
   <add name="F5IsHandler" path="F5Isapi.dll" verb="*" type="F5.IsHandler" mod
   ules="ManagedPipelineHandler" scriptProcessor="" resourceType="Unspecified"
   requireAccess="Script" preCondition="" />
   </handlers>
   <security>
   <authentication>
   <anonymousAuthentication enabled="false" />
   </authentication>
   </security>
   </system.webServer>
   </configuration>
   ```

5. Allow anonymous authentication to be overridden by using the **appcmd** command to set the override mode in the machine-level **applicationHost.config** file. **appcmd.exe** is located in %systemroot%\system32\inetsrv\.
   For example:

   ```
   appcmd set config "Default Web Site/scripts" /section:anonymousAuthentication /
   overrideMode:Allow /commit:APPHOST
   ```

6. Set up a new application pool for the file **F5.IsHandler.dll**:

   a. From the **Start** menu, choose Control Panel.

   b. Choose Administrative Tools

   c. Choose Internet Information Services (IIS) Manager.

      d. From **Connections**, expand **<MachineName>** (**MachineName\UserName**).

      e. Right click the Application Pools menu and choose Add Application Pool.

      f. In the **Name** box, type **F5 Application Pool**.

      g. Click **OK**.

7. Create a new application named **scripts**:

      a. Expand **<MachineName> and Sites**.

      b. Right click **"Default Web Site"** (or the applicable web site), and choose **Add Application**.

      c. In the **Alias** box, type **scripts**.

      d. To change the application pool, click **Select**.

      e. For the physical path, type the directory you created in step 1 (**C:\Inetpub\scripts**).

      f. Click **OK**.

8. Change the **Authentication** setting to **Basic Authentication**:

      a. Select **scripts**.

      b. In the center pane, double click **Authentication**.

      c. Verify that the status of all items under **Authentication** is **Disabled**, except for the Basic Authentication item. To enable or disable an authentication item, right click the name and choose Enable or Disable.

Creating the WMI Monitor on the BIG-IP LTM

The next task is to create the WMI monitor on the applicable BIG-IP LTM systems. Use the following table:

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	*Name*	Type a unique name
	Type	**WMI**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the appropriate user name
	Password	Type the associated password
	URL:	**/scripts/F5Isapi.dll** (for IIS 6, 7, and 7.5)

Create this monitor on all applicable BIG-IP LTM systems.

Apply the monitor on the BIG-IP LTM devices

Next, we apply the monitor to the IIS nodes on the BIG-IP LTM system.

To apply the monitor to the nodes

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

2. From the list of nodes, click the IP address of one of your IIS server.

3. In the Configuration section, from the **Health Monitor** list, select **Node Specific**.

4. From the Available list, select the WMI monitor you created, and then click the Add (<<) button.

5. Click **Update**.

6. Repeat for all appropriate nodes.

Modifying the pool to use the Dynamic Ratio load balancing method

The next task is to modify the BIG-IP LTM pool created by the template to use the Dynamic Ratio load balancing method.

Important ———►

If you have already disabled Strict Updates and manually modified the iApp configuration, reconfiguring the template as described in the following procedure overwrites those changes. In this case, you have two options for modifying the load balancing method: reconfigure the iApp as described below, and then re-implement any manual changes you made, or do not reconfigure the iApp, and manually modify the load balancing method on the Pool (Strict Updates must still be disabled).

To modify the load balancing method on the pool

1. On the Main tab, expand **iApp** and then click **Application Services**.

2. Click the name of your Microsoft IIS Application service from the list.

3. On the Menu bar, click **Reconfigure**.

4. From the **Which load balancing method do you want to use?** list, select **Dynamic Ratio (Node)**.

5. Click the **Finished** button.

6. You must restart **bigd** after making changes that require disabling Strict Updates. However, you should only restart **bigd** after making all modifications. See the following section.

Restart bigd after making changes that require disabling Strict Updates

If using BIG-IP version 11.0 through 11.1.x, after performing any modification that requires disabling Strict Updates feature on the Application Service, you must restart the bigd daemon from the BIG-IP command line. We recommend restarting bigd during a maintenance window or other scheduled downtime. This is not necessary if using BIG-IP version 11.2 or later.

To restart bigd

1. From the command line, log into the BIG-IP system.

2. From the prompt, run the following command:

   ```
   bigstart restart bigd
   ```

3. Exit the command line interface.

Appendix C: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP LTM for Microsoft IIS. Advanced users extremely familiar with the BIG-IP system can use the following table to manually configure the BIG-IP system.

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	*Name*	Type a unique name
	Type	**HTTP** (see *Appendix B: Configuring WMI monitoring for IIS Servers (optional) on page 13* for an alternate monitor.
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
Pool (*Main tab-->Local Traffic -->Pools*)	*Name*	Type a unique name
	Health Monitor	Select the monitor you created above
	Slow Ramp Time¹	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of the IIS nodes
	Service Port	**80** (click **Add** to repeat Address and Service Port for all nodes)
Profiles (*Main tab-->Local Traffic -->Profiles*)	**HTTP** (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Rewrite Redirect²	**Matching**
		Insert X-Forwarded-For	**Enabled** (see *page 11* for adding the X-Forwarded-For log field to IIS)
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Persistence (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Cookie**
	OneConnect (*Profiles-->Other*)	Name	Type a unique name
		Parent Profile	**oneconnect**
	Client SSL² (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Web Acceleration (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**optimized-caching**
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
		Content List -->Include List *(Add each entry to the Content Type box and then click Include)*	application/vnd.ms-publisher
			application/(xls|excel|msexcel|ms-excel|x-excel|x-xls|xmsexcel|x-ms-excel|vnd.excel|vnd.msexcel|vnd.ms-excel)
			application/(word|doc|msword|winword|ms-word|x-word|x-msword|vnd.word|vnd.msword|vnd.ms-word)
			application/(xml|x-javascript|javascript|x-ecmascript|ecmascript)
			application/(powerpoint|mspowerpoint|ms-powerpoint|x-powerpoint|x-mspowerpoint|vnd.powerpoint|vnd.mspowerpoint |vnd.ms-powerpoint|vnd.ms-pps)
			application/(mpp|msproject|x-msproject|x-ms-project|vnd.ms-project)
			application/(visio|x-visio|vnd.visio|vsd|x-vsd|x-vsd)
			application/(pdf|x-pdf|acrobat|vnd.pdf)

¹ You must select **Advanced** from the **Configuration** list for these options to appear
² *Only required if offloading SSL on the BIG-IP LTM*

Configuration table, continued

BIG-IP LTM Object	Non-default settings/Notes	
	HTTP	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	Protocol Profile (client)[1,2]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1,2]	Select the LAN optimized TCP profile you created above
	HTTP Profile[2]	Select the HTTP profile you created above
	Web Acceleration profile[2]	Select the Web Acceleration profile you created above
	HTTP Compression profile[2]	Select the HTTP Compression profile you created above
	OneConnect[2]	Select the OneConnect profile you created above
	SNAT Pool [3]	**Automap** (optional; see footnote [3])
	Default Pool[2]	Select the pool you created above
	Persistence Profile[2]	Select the Persistence profile you created
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	*iRule*[4]	If offloading SSL only: Enable the built-in **_sys_https_redirect irule**
	HTTPS[5]	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	Web Acceleration profile	Select the Web Acceleration profile you created above
	HTTP Compression profile	Select the HTTP Compression profile you created above
	OneConnect	Select the OneConnect profile you created above
	SSL Profile (client)	Select the Client SSL profile you created above
	SNAT Pool [2]	**Automap** (optional; see footnote [3])
	Default Pool	Select the pool you created above
	Persistence Profile	Select the Persistence profile you created

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] *Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server, and only requires a name, IP address, Port, and the redirect iRule.*
[3] *If want to use SNAT, and you have a large IIS deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*
[4] *Only enable this iRule if offloading SSL*
[5] *Only create this virtual server if offloading SSL*

Document Revision History

Version	Description	Date
1.0	New Version	08/24/2011
1.1	- Added support for Microsoft IIS 8.0 - Added the procedure *Modifying the IIS authentication token timeout value on page 8.* - Added IIS 8 specific configuration to Appendix A for deploying the Custom Logging role service. - Added *Appendix A: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 11* - Added *Appendix B: Configuring WMI monitoring for IIS Servers (optional) on page 13.*	06/08/2012

F5 Networks, Inc.   401 Elliott Avenue West, Seattle, WA 98119   888-882-4447   www.f5.com

F5 Networks, Inc. **Corporate Headquarters**	**F5 Networks** **Asia-Pacific**	**F5 Networks Ltd.** **Europe/Middle-East/Africa**	**F5 Networks** **Japan K.K.**
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com