Load Balancing IBM WebSphere Servers with F5 Networks BIG-IP System

• Introducing BIG-IP load balancing for IBM WebSphere Server

• Configuring the BIG-IP for load balancing WebSphere servers

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support.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

The BIG-IP load balancing solution for IBM® WebSphere® servers is a highly effective way to direct traffic for WebSphere application servers with the BIG-IP® application traffic manager. The BIG-IP system also provides the top-level distribution that allows for simple and effective scalability of WebSphere servers and ensures that customers maximize their investment.

IBM WebSphere Application Server provides the core software needed to deploy, integrate and manage e-business applications. F5 Networks BIG-IP system is a secure, highly available and scalable application traffic management device.

This strong interoperability and integration between WebSphere and BIG-IP provides a solution that delivers unparalleled load balancing functionality for those deploying services and applications on the WebSphere platform.

This solution is powered by F5 Network’s patented cookie persistence feature, which uses an HTTP cookie stored on a client’s computer to allow the client to reconnect to the same server previously visited at a web site.

Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system.

The WebSphere server should be running version 5.0 or later. The BIG-IP system must be running version 4.2 or later.

Configuration example

Using the configuration in this guide, the BIG-IP system is optimally configured to load balance traffic to IBM WebSphere servers. Figure 1.1 shows a typical configuration with a redundant pair of BIG-IP devices, a cluster of WebSphere servers, and a WebSphere administration node. Figure 1.1 also shows an optional pool of Web servers which host static content for traffic that does not need to be sent to the WebSphere application servers.
For the rest of this document, we use the IP addresses shown in Figure 1.1 in our examples.

Configuring the BIG-IP for load balancing WebSphere servers

To configure the BIG-IP product to load balance WebSphere servers, you need to complete the following tasks:

- Defining the pool
- Defining the virtual server
- Enabling persistence on the pool
- Configuring an optional health monitor
Defining the pool

The first step is to define a load balancing pool for the WebSphere servers. You can define a pool from the Configuration utility (see Figure 1.2) or the command line.

To create a pool using the Configuration utility

1. In the navigation pane, click Pools.
   The Pools screen opens.
2. Click the Add button.
   The Add Pool screen opens.
3. In the Pool Name box, enter a name for your pool. In our example, we use websphere_pool.
4. In the Load Balancing Method box, enter your preferred load balancing method. We recommend one of the following load balancing methods, although different load balancing methods may yield optimal results for a particular network.
   - **Least Connections**
     In Least Connections mode, the BIG-IP system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.
   - **Fastest**
     In Fastest mode, the BIG-IP system passes a new connection based on the fastest response of all currently active nodes. Fastest mode may be particularly useful in environments where nodes are distributed across different logical networks, or where the servers have varying levels of performance.
5. In the Resources section, you add the WebSphere servers to the pool.
   a) In the Member Address box, type the IP address of the WebSphere server. In our example, the first IP address we type is 10.10.10.1.
   b) In the Service box, type the service number you want to use for this node (for example 9080), or specify a service by choosing a service name from the list (for example http). In our example, we use the default service for WebSphere, 9080.
   c) The Member Ratio and Member Priority boxes are optional.
   d) Click the Add button (>>) to add the member to the Current Members list.
   e) Repeat Steps a-d for each WebSphere server.
   f) The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the Help button.)
6. Click the **Done** button.

7. **Optional:** If your configuration includes Web servers to serve static content, repeat the procedure above to create a new pool for these Web servers. You will then create a **rule** that sends the static content to the Web server pool.

   For information on how to configure this rule, see the **Configuring a rule to send static content to the Web servers** section at the end of this guide.

**To define the pool from the command line**

To define a pool from the command line, use the following syntax:

```
b pool <pool_name> {member <member_definition> ... member <member_definition>}
```

In our example, the command is:

```
b pool websphere_pool { \
```

![Add Pool screen](image_url)

*Figure 1.2 Add Pool screen*
Defining the virtual server

The next step is to define a virtual server that references the pool. Again, you can define the virtual server from the Configuration utility or the command line.

**To define the virtual servers using the Configuration utility**

1. In the navigation pane, click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Add** button. The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, then click the **NEXT** button. In our example, we use **192.168.12.85** with service of **80**. (See Figure 1.3) The Configure Basic Properties screen displays.

![Figure 1.3 Adding a virtual server](image-url)
4. On the Configure Basic Properties screen, leave Enable Address Translation and Enable Port Translation boxes checked. The other fields are optional, configure these fields as applicable to your network. Click the NEXT button. The Select Physical Resources screen displays.

5. Click the Pool option button, and from the list, select the pool you created in the Defining the pool section above.

![Select Physical Resources](image)

**Figure 1.4 Selecting the Resources for the virtual server**

6. You can click Done or Next. If you click the Next button, you have the option of configuring redundant and outbound properties of the virtual server. For additional information about configuring a virtual server, click the Help button.

**To define the virtual servers from the command line**

Use the bigpipe virtual command as shown below. You can use standard service names in place of port numbers. If you have DNS configured, you can also use host names in place of IP addresses.

```
b virtual <virt IP>:<port> use pool <pool_name>
```

In our example, we use:

```
b virtual 192.168.12.85:80 use pool websphere_pool
```
Enabling persistence on the pool

The next step in configuring the BIG-IP system to load balance WebSphere Servers is to configure persistence on the pool. For optimal load balancing, we recommend the Insert mode of F5’s cookie persistence for BIG-IP versions 4.0 and later. You can configure cookie persistence from the Configuration utility (see Figure 1.5) or the command line.

◆ Note

*The cookie used in cookie persistence Insert mode resides in memory, and is not written to disk.*

**To enable cookie persistence, Insert mode on the pool using the Configuration utility**

1. In the navigation pane, click **Pools**. The Pools screen opens.
2. In the **Pool Name** list, click the name of the pool you created in the Defining the pool section above. This displays the properties of that pool.
3. Click the Persistence tab at the top of the screen. The persistence properties screen opens.
4. In the Persistence Type section, click the **Active HTTP Cookie** button. Type the following information:
   - **Method**
     From the **Method** list, select **Insert**.
   - **Expiration**
     In the **Expiration** section, you can specify an expiration value in days, hours, minutes, and seconds that a cookie remains valid on the client computer. If you do not enter anything, the cookie expires when the client’s browser closes.
5. Click the **Apply** button.
To enable cookie persistence, Insert mode on the pool from the command line

To active cookie persistence Insert mode from the command line, use the following syntax:

```
b pool <pool_name> { <lb_mode_specification> \ persist cookie \ cookie_mode insert \ cookie_expiration <timeout> \ <member definition> }
```

The `<timeout>` value for the cookie is written using the following format:

```
<days>d hh:mm:ss
```

In our example, the command would be:

```
b pool websphere_pool { fastest \ persist cookie \ cookie_mode insert \ cookie_expiration 0 08:00:00 \ member 10.10.10.1:9080 member 10.10.10.2:9080 member 10.10.10.3:9080 }
```
Configuring an optional health monitor

You can choose to configure an optional Extended Content Verification (ECV) health monitor on the BIG-IP system. The ECV monitor goes much further than a standard ICMP health check, by actually using `send` and `recv` statements in an attempt to retrieve explicit content from nodes.

**To configure a health monitor for the WebSphere server using the BIG-IP Configuration utility.**

1. In the navigation pane, click **Monitors**. The Network Monitors screen opens.
2. Click the **Add** button. The Add Monitor screen opens.
3. In the Add Monitor screen, type the name of your monitor (it must be different from the monitor template name), in our example, we type **websphere_monitor**. In the **Inherits From** box, select the **http** monitor template from the list. Click the **Next** button.
4. In the Configure Basic Properties section, type an Interval and Timeout value. We recommend 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. Note that if you are performing very complex ECV checks, the default setting of a five second interval could overload the servers. In this case we would recommend a longer interval). Click the **Next** button.
5. In the Configure ECV HTTP Monitor section, enter the appropriate information for your configuration.

**Important Note:**

If you are using the **GET** send string, you must end the string by including the HTTP protocol at the end of the statement. Use the following syntax:

```
GET <fully qualified path name> HTTP/1.0
```

For example:

```
GET /www/support/customer_info_form.html HTTP/1.0
```

(see Figure 1.6)

After completing the applicable information, click the **Done** button.
6. After clicking the Done button on the Add Monitor box, in the navigation pane, click Monitors.
The Monitors screen opens.

7. Click the Node Associations tab.
The Node Association screen displays.

8. In the Choose Monitor box, select the monitor you created in step 3 from the list and click the Move (>>) button. In our example, we select websphere_monitor.

9. If you want to associate more than one monitor, repeat the previous step for each monitor you want to associate with a node.

10. From the list of Nodes, in the Associate Current Monitor Rule column, check the box for each WebSphere server you want to associate with this monitor. In our example, we check the box for 10.10.10.1:9080, 10.10.10.2:9080, and 10.10.10.3:9080. (see Figure 1.7)

11. Click the Apply button.
For additional information associating a monitor, click the Help button.

Figure 1.6 Configuring the Health monitor
Figure 1.7 Associating Monitors with nodes

Configuring a rule to send static content to the Web servers

Important

This section serves as an appendix, and is only necessary if your configuration includes Web servers for static content. If you do not have Web servers for static content, you do not need to follow the procedures below.
If your configuration includes Web servers to serve static content, you must create a rule on the BIG-IP system that sends the static content to the Web servers.

**Important**

You must already have a pool that contains the Web servers for static content before creating the rule. If you have not already created the Web server pool, follow the procedure in the Defining the pool section, substituting the information from the Web servers for static content.

**Tip**

In the procedure below, the rule uses the line `http_uri ends_with one of images`. `images` refers to a predefined rule class on the BIG-IP system that includes `.bmp`, `.jpg`, and `.gif` extensions. You can modify this rule class to include other types of files (such as `.html`), or create a new rule Class that contains the file types applicable to your configuration. For information on how to modify or create a rule class, see the BIG-IP Reference Guide, or the online help.

**To create a rule for static content using the Configuration utility**

1. In the navigation pane, click Rules. The Rules screen opens.
2. Click the Add button. The Add Rule screen opens.
3. In the Name box, type a 1 to 31 character name. In our example, we use `image_rule`.
4. In the Type box, select Text Input. A screen appears in which you type the complete text of the rule:

   ```
   if ( http_uri ends_with one of images ) {
     use pool image_pool
   }
   else {
     use pool websphere_pool
   }
   ```

   Where `image_pool` is the pool of Web servers that contains the static content (see Figure 1.8).
Figure 1.8 Creating a rule

5. Click Done.

To create a rule for static content from the command line

To create a rule using the command line, use the following syntax:

```plaintext
rule <rule_name> {
  if ( http_uri ends_with one of images ) {
    use pool <static_pool name>
  }
  else {
    use pool <websphere_pool name>
  }
}
```

In our example, the command would be:

```plaintext
rule image_rule {
  if ( http_uri ends_with one of images ) {
    use pool image_pool
  }
}
```
else {
    use pool websphere_pool
}

Changing the virtual server to use the rule

After you have completed the rule, you must configure the virtual server you created in the Defining the virtual server section above to use the rule you just created, and not the pool.

**To change the virtual server to use the rule**

6. In the navigation pane, click Virtual Servers. The Virtual Servers screen opens.

7. Click the virtual server you created in the Defining the virtual server section. The Virtual Server Properties screen opens.

8. In the Resources section, click the Rule option button.

9. In the box next to Rule, select the name of the rule you created from the list. In our example, we use image_rule.

10. Click the Apply button.

![Image of BIG-IP interface with highlighted Virtual Server Properties and Rule settings]