

Deployment Guide

Deploying Microsoft Operations Manager with the BIG-IP system and iControl

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support.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



Deploying Microsoft Operations Manager with the BIG-IP system and iControl

Welcome to the BIG-IP LTM system - Microsoft® Operations Manager (MOM) Deployment Guide. This guide is designed to help you get the most out of your network by allowing your MOM installation to seamlessly integrate with your BIG-IP system. This is done using the power of iControl, F5's SOAP API exposed on each BIG-IP LTM system. Acting as a Web Services endpoint, these devices can be programmatically controlled using the iControl API to perform nearly any task on the system.

MOM 2005 delivers enterprise-class operational management by providing comprehensive event management, proactive monitoring and alerting, reporting and trend analysis, and system and application specific knowledge to improve the manageability of Windows Server System environments.

For more information on Microsoft Operations Manager, see <http://www.microsoft.com/mom/default.msp>.

For more information on iControl, see the F5 Developer Community, DevCentral: <http://devcentral.f5.com/>

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ A MOM 2005 installation, including all sub-components.
- ◆ The BIG-IP system must be running version 9.1 or later. We recommend version 9.2 or later.
- ◆ F5's iControl v9 SDK. If you do not already have the iControl SDK, you can download it (requires free registration) from DevCentral <http://devcentral.f5.com/Default.aspx?tabid=31>
- ◆ Microsoft.NET Framework (with C# compiler).
- ◆ Write access to the file system on the MOM system.
Note: Write access is required to follow the procedures in this guide, although it is not required for the functionality. A small change in the way your MOM/iControl integration is configured would allow you to store all necessary files on the nodes, rather than the MOM system.
- ◆ You need to download this **iControl-Mom.zip** file, which contains the files necessary for this configuration.

◆ Note

This document is written with the assumption that you are familiar with the BIG-IP LTM system, iControl and Microsoft Operations Manager 2005. Consult the appropriate documentation for detailed information.

Configuration example

In this Deployment Guide, we configure a monitored pool that is conscious of the memory available on the nodes, which adjusts the ratio of connections the servers will receive accordingly, thereby allowing the intelligent network to tune its own performance.

This Deployment Guide demonstrates a small portion of the capabilities of iControl and the way that it can be integrated with MOM to help build a smarter, more efficient network by integrating monitoring with automated responses to make sure as much work is done by the servers as possible, even when it comes to tuning their own performance, by building an intelligent network.

The following diagram represents our example configuration.

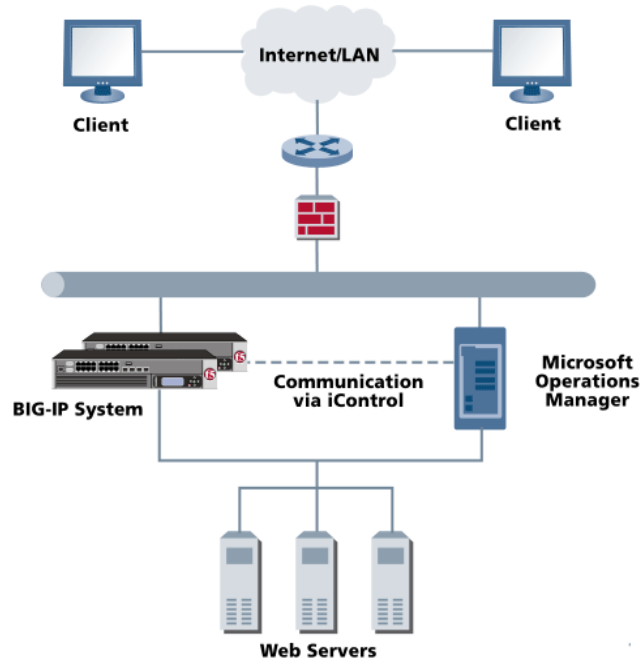


Figure 1 Configuration example

Configuring the BIG-IP LTM system

For this deployment, we first configure the BIG-IP LTM system for the web servers (nodes). The following procedures show how to configure the base BIG-IP configuration, which includes a health monitor, pool and virtual server. You may already have these items configured on your BIG-IP LTM system; in this case, you can skip this section and continue to *Configuring the SDK and the iControl application*.

This Deployment Guide does not contain procedures on how to configure other features available on the BIG-IP LTM system, such as Profiles, Persistence modes, and iRules. For more information on how to configure the BIG-IP LTM system, see the product documentation.

To configure the base BIG-IP LTM system, you must complete the following procedures:

- *Connecting to the BIG-IP device*
- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating the virtual server*

Connecting to the BIG-IP device

Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Creating the HTTP health monitor

The next step is to set up a health monitor for the web servers (nodes). This procedure is optional, but very strongly recommended. In our example, we use an HTTP monitor which checks nodes (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes. We configure the health monitors first in version 9.0 and later, as health monitors are now associated at the pool level.

To configure a health monitor

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

3. In the **Name** box, type a name for the Monitor.
In our example, we type **http_monitor**.
4. From the **Type** list, select **http**
The HTTP Monitor configuration options appear.
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**.
6. *Optional:* In the **Send String** and **Receive Rule** sections, you can add an optional Send String and Receive Rule specific to the device being checked.

General Properties	
Name	http_monitor
Type	HTTP
Import Settings	http
Configuration: Basic	
Interval	5 seconds
Timeout	16 seconds
Send String	GET /
Receive String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 2 Creating the HTTP monitor

7. Click the **Finished** button.
The new monitor is added to the Monitor list.

Creating the pool

The next step in this configuration is to create a pool on the BIG-IP system for the web servers. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. For this deployment, we use the Ratio load balancing method, in which each pool member is

assigned a ratio based on the amount of traffic it should handle in comparison to other members (although these could all be identical if you want connections to be evenly distributed).

To create the 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.

*Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

3. In the **Name** box, enter a name for your pool. In our example, we use **web_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 **http_monitor**.
5. From the **Load Balancing Method** list, select **Ratio (member)**.
6. For 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 server to the pool. In our example, we type **10.133.20.1**
9. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **80**.
10. In the **Ratio** box, type a ratio number. Members with a higher ratio number receive more traffic. In our example, we type **3**.
11. Click the **Add** button to add the member to the list.
12. Repeat steps 8-11 for each server you want to add to the pool. In our example, we repeat these steps twice for the remaining servers, **10.133.22.2** and **10.133.22.3**, with a ratio of **2** and **1** respectively.
13. Click the **Finished** button (see Figure 3).

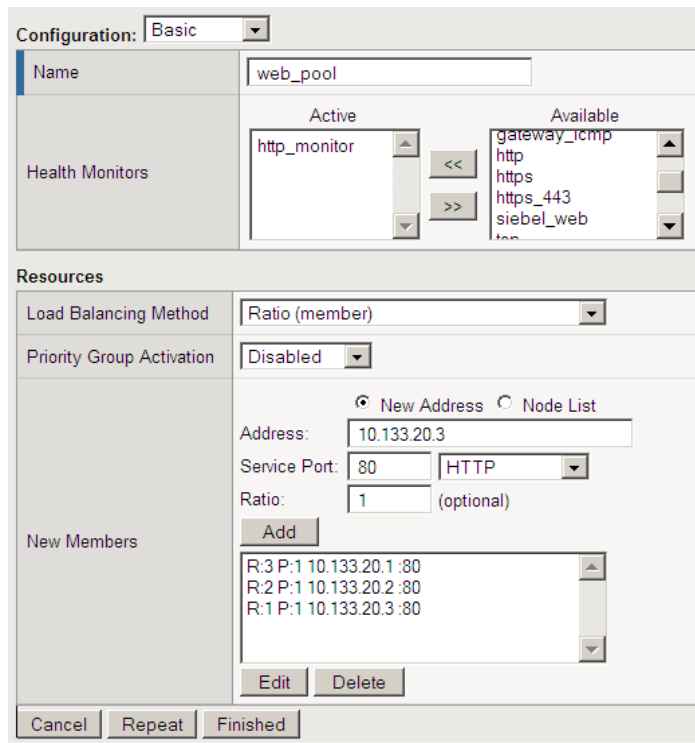


Figure 3 Creating the pool in the BIG-IP Configuration utility

Creating the virtual server

The next task is to create a virtual server that references the pool. For the purposes of the Deployment Guide, we configure an HTTP virtual server.

To create the HTTP 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 **web_virtual**.
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 **172.27.90.110**.
6. In the **Service Port** box, type **80**.
7. Modify the options in the Configuration section as applicable for your deployment.

-
8. In the Resources section, from the **Default Pool** list, select the name of the pool you created in the *Creating the pool* section. In our example we select **web_pool**.
 9. Modify the other options in the Resources section as applicable for your configuration.
 10. Click the **Finished** button.

Configuring the SDK and the iControl application

With the BIG-IP LTM system configuration complete, we now configure the iControl SDK and application. For this section, you need to download the **iControl-Mom.zip** file. This ZIP file includes everything necessary to perform the integration with MOM, and allow for some automatic management functionality on the BIG-IP system via MOM events and alerts.

To configure the base SDK and iControl application, you must complete the following procedures:

- *Downloading and extracting the ZIP file*
- *Modifying and running the PMMgr.cs file*
- *Preparing the PMMgr.exe file for execution*

Downloading and extracting the ZIP file

The first step is download and extract the zip file onto the MOM system. For ease of use, we recommend you extract the contents of the ZIP file into the directory where you downloaded the BIG-IP version 9 Windows SDK. In our example, we downloaded the SDK into a directory named iControl (**C:iControl**). We then extracted the contents of the ZIP file into a directory named pool (**C:iControl\pool**).

Important

Wherever you extract the contents of the ZIP file, it is important that you remember this path, as we use it later in the MOM configuration.

Modifying and running the PMMgr.cs file

Included in the ZIP file is a file named **PMMgr.cs**. The next task is to modify four variables in the **PMMgr.cs** script. They are:

Variable	Description
<code>private string sHostname = "";</code>	The host name or IP address of the BIG-IP system
<code>private string sHPort = "";</code>	The port on which the BIG-IP is connected (443 is default)
<code>private string sUsername = "";</code>	The user name needed to administer the BIG-IP system
<code>private string sPassword = "";</code>	The accompanying password for the Admin user name

Table 1.1 PMMgr.cs file variables and descriptions

To modify the variables in the PMMgr.cs file

1. Open the **PMMgr.cs** file in an editor, such as Visual Studio or notepad.
2. Find the variables in the file (located near the top) and modify each variable with the appropriate information as described in the preceding table.
3. Save the file.
4. Recompile the **PMMgr.cs** file with an output of **PMMgr.exe** in the same directory.

You need to include both **LocalLBPoolMember.cs** and **LocalLBPool.cs** as dependencies, as functions they contain are used. This can be done in Visual Studio or manually, depending on your preference.

Note: It is outside the scope of this document to provide instructions on how to recompile the file and include files as dependencies. If you need help, consult your system administrator.

Preparing the PMMgr.exe file for execution

The syntax for the PMMgr.exe application is shown in the following example (this can also be seen when you run the application from the command line with no arguments):

```
PMMgr.exe <poolName> <memberAddress> <memberPort> "status" | "session_enable"
|"session_disable" | "enable" | "disable" | "limit" <limit_value> | "ratio" "incr"
|"decr"
```

In our deployment, we are configuring the BIG-IP LTM system to decrement the ratio of a node in the pool by 1. The syntax to do this is:

```
PMMgr.exe <poolName> <memberAddress> 80 ratio decr
```

There is no need to run the application now, but we recommend you have this command ready, as we use this syntax in the MOM configuration.

◆ **Tip**

Although this Deployment Guide shows only how to configure the BIG-IP system to decrement the ratio of a node in the pool, as you can see from the syntax of the PMMgr.exe application, there are a number of possibilities you could configure.

Configuring Microsoft Operations Manager

The final task in this deployment is to configure MOM. There are two procedures that we configure on Microsoft Operations Manager:

- *Creating a custom Provider*
- *Creating a Server Performance rule*

Creating a custom Provider

The first step for configuring MOM is to configure a custom Provider to provide available memory information from remote servers.

◆ **Tip**

Although we are using memory information in our example, you can choose other objects or counters for the Provider.

To configure a custom provider

1. Open the MOM 2005 Administrator Console.
2. From the navigation pane, expand the **Management Packs**.
3. From the **Management Packs** directory, right-click **Providers**. From the list that appears, select **Create Provider**. The Select Data Provider Type dialog opens.
4. From the Select Data Provider Type dialog box, select **Windows NT Performance Counter**. The Windows NT Performance Counter Provider properties box opens.
5. In the Name box, type a name for this Provider. In our example, we type **iControl - Server Mem Available**.
6. In the **Computer** box, make sure the proper device is selected.
7. From the **Object** list, select **Memory**.
8. From the **Counter** box, select **Available MBytes**.

9. In the **Sample Every** section, choose how often to synchronize with the Agent machine. In our example, we use 5 minutes (see Figure 4).
10. Click the **OK** button.
The Provider is added to the list.

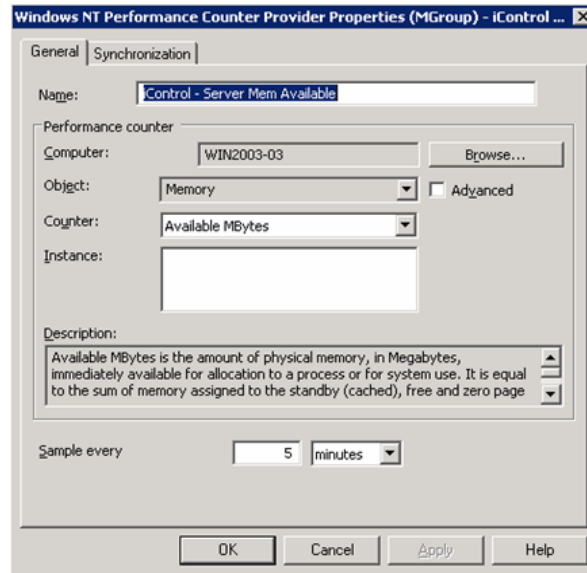


Figure 4 Creating a custom Provider

Creating a Server Performance rule

Next, we configure a Server Performance Rule to create an alert when the available memory information goes below a certain limit (in our example, 100MB). Because we are monitoring the amount of memory available on the system, the Server Performance Rule is a **Threshold** rule. A Threshold rule compares the current available memory, delivered by the Provider we just created, to a hard set threshold that we configure in the following procedure.

This Server Performance rule triggers an alert and response. We configure the response to use the iControl application you created to decrement the ratio of the node by 1.

To create a Server Performance rule

1. Open the MOM 2005 Administrator Console.
2. From navigation pane, expand **Management Packs**, and then expand **Rule Groups**.
3. Expand **Microsoft Operations Manager, Operations Manager**, and then **Server**.

-
4. From the **Server** directory, right-click **Performance Rules**. From the list that appears, select **Create Performance Rule**.
 5. From the Performance Rule Type dialog box, select **Compare Performance Data [Threshold]**.
 6. From the **Provider Name** list, select the provider that you created in the preceding procedure. In our example, we select **iControl - Server Mem Available**.
Click the **Next** button.
 7. In the **Threshold Rule Properties - Schedule** dialog box, configure the schedule as applicable for your configuration. This is an optional step, if you do not configure a schedule, the rule always runs.
Click the **Next** button.
 8. In the **Threshold Rule Properties - Criteria** dialog box, configure the schedule as applicable for your configuration. In our example, we leave the settings at the default, and click the **Next** button.
 9. In the **Threshold Rule Properties - Threshold** dialog box, from the **Match when the threshold meets the following condition** section, click the **Less than the following value** option, and type **100** in the box. This is the minimum amount of RAM that you'd like to have available on the monitored system before it invokes a response from MOM.
Note: You can enter another value for the Threshold limit, we use 100MB as an example.
Click the **Next** button.
 10. In the **Threshold Rule Properties - Alert** dialog box, check the **Generate Alert** box.
From the **Alert Severity** list, select **Warning**. In the Description box, configure as applicable for your deployment. In our example, we type **\$Object\$: \$Counter\$: \$Instance\$ value = \$Value\$**.
Click the **Next** button.
 11. In the **Threshold Rule Properties - Alert Suppression** dialog box, make sure the **Suppress duplicate alerts** box is checked.
In the Fields section, configure as applicable for your deployment. In our example, we check all boxes except for **Alert Description**.
Click the **Next** button.
 12. In the **Threshold Rule Properties - Responses** dialog box, click the **Add** button to add a new response. From the list that opens, select **Execute a command or batch file**.
The Configure Response Command box opens.
 13. In the **Application** box, type the full path to the iControl application you created earlier in this guide (see the *Downloading and extracting the ZIP file* section).
In our example, we type **C:\iControl\pool\PMMgr.exe**.

14. In the **Command Line** box, type the command you prepared in the *Preparing the PMMGr.exe file for execution* section. In our example, we type

```
PMMGr.exe web_pool 10.133.20.1 80 ratio decr
```

15. In the **Initial Directory** box, type the initial directory where the **PMMGr.exe** file is located.
In our example, we type **C:**.
16. In the **Run Location** section, choose whether to run the command on the Agent Computer or the Management Server.

We recommend you run the command on the Management Server. This allows you to have just a single copy of the PMMGr.exe file on the Management Server. If you choose the Agent Computer option, you must copy the **PMMGr.exe** file, as well as the necessary libraries, on to each managed system.

To run the command on the Management Server, you also need to enable running scripts on the Management server. This setting can be found from the Administration console in the Administration --> Global Settings --> Security section.

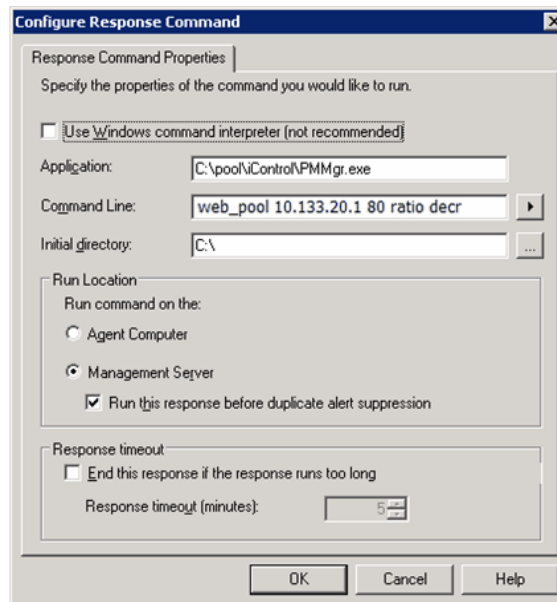


Figure 5 Configuring the MOM Response command to use the iControl application

◆ **Tip**

If you want to monitor other nodes, repeat this procedure, using the IP address of the other node in Step 4.