



DEPLOYMENT GUIDE

DEPLOYING THE BIG-IP LTM SYSTEM WITH ADOBE FLASH MEDIA SERVER

Version: 1.0

Deploying the BIG-IP LTM system with Adobe Flash Media Server 3

Welcome to the F5 - Adobe® Flash Media Server 3™ Deployment Guide. This guide provides step-by-step procedures for configuring the BIG-IP LTM system with Adobe Flash Media Server 3.

Flash Media Server 3 (FMS3) can be licensed in three ways, which determine the features that are available for you to use. These options are Flash Media Interactive Server, Flash Media Streaming Server and Flash Media Development Server. Flash Media Interactive Server is the most feature complete offering of FMS3 and can be used to stream video, audio, interactive content and can be deployed in an edge and origin design for full scalability.

The other two licensing options are limited as follows: With Adobe Flash Media Streaming Server, only video and audio can be streamed and with the Adobe Flash Media Development Server, there is a 10 concurrent user limit and cannot be used in a production environment.

As a product guide intended for scalable, secure and accelerated deployments, this guide is based on the Flash Media Interactive Server (FMIS3). While many of the concepts here are applicable to the other formats the configurations have only been tested with FMIS3.

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:

- ◆ Adobe Media Interactive Server 3 should be running on the system (or systems) you are intending to place behind the BIG-IP LTM. See the Flash Media Server *[Installation Guide](#)* and the *[Configuration and Administration Guide](#)* for FMIS3 installation and configuration information.
- ◆ The BIG-IP LTM must be running version 9.0 or later. We strongly recommend version 9.4 or later.
- ◆ We assume that the BIG-IP LTM is on the network, and has already been initially configured.
- ◆ In this guide, we provide procedures for configuring the BIG-IP LTM system to offload SSL from the Adobe Flash Media Interactive Servers that use RTMPS.

For information on configuring Adobe FMIS3 for SSL, see the section titled **Configure SSL** in Chapter 3 of the FMIS3 Configuration and Administration Guide, available from the Adobe web site:

<http://www.adobe.com/support/documentation/en/flashmediaserver/>

Product Tested	Version Tested
BIG-IP Local Traffic Manager (LTM)	9.4.5
Adobe Flash Media Server	3.0

Configuration example

FMIS3 provides for real-time streaming of audio, video and interactive content using the Real Time Messaging Protocol (RTMP). RTMP has several variants and it is important to distinguish the variants when deciding how to deploy BIG-IP LTM in front of the server. These variants include RTMPT, RTMPE and RTMPS.

- ◆ **RTMP** is the basic protocol of FMIS3. RTMP contains streams of information with no HTTP headers. BIG-IP can not apply HTTP based optimization to basic RTMP traffic, but basic RTMP traffic can still be load balanced and optimized at the TCP layer.
- ◆ **RTMPT** is RTMP encapsulated within HTTP requests in order to traverse firewalls. RTMPT also allows for cookie insertion to maintain session persistence. While regular RTMP traffic is designed to use a default TCP port of 1935, RTMPT is designed to use a default HTTP port of 80.
- ◆ **RTMPE** is an encrypted form of RTMP, which can work over either port 1935 or 80, is turned on by default in FMIS3 installations and allows the server to encrypt the traffic without the need for SSL certificates.
- ◆ **RTMPS** is another form of encrypted RTMP which uses standard SSL encryption and is designed to work over port 443.

Adobe recommends RTMPE for encryption on server deployments because it has less configuration and maintenance overhead and reduces the server load by up to 15% when compared to SSL encryption with RTMPS. However, in a BIG-IP LTM deployment scenario, all encryption load on the server can be offloaded to the BIG-IP LTM by using RTMPS. Because of the benefits of offloading encryption on the BIG-IP LTM, F5 recommends using RTMPS, and not RTMPE when encryption is required.

This deployment guide contains procedures for two possible scenarios for deploying Adobe Flash Media Server: Flash Media origin servers, and a combination of both origin and edge servers. If you are deploying in an origin/edge scenario, be sure to see *Appendix A: Configuring the Origin/Edge Server deployment scenario*, on page 21 for additional configuration procedures.

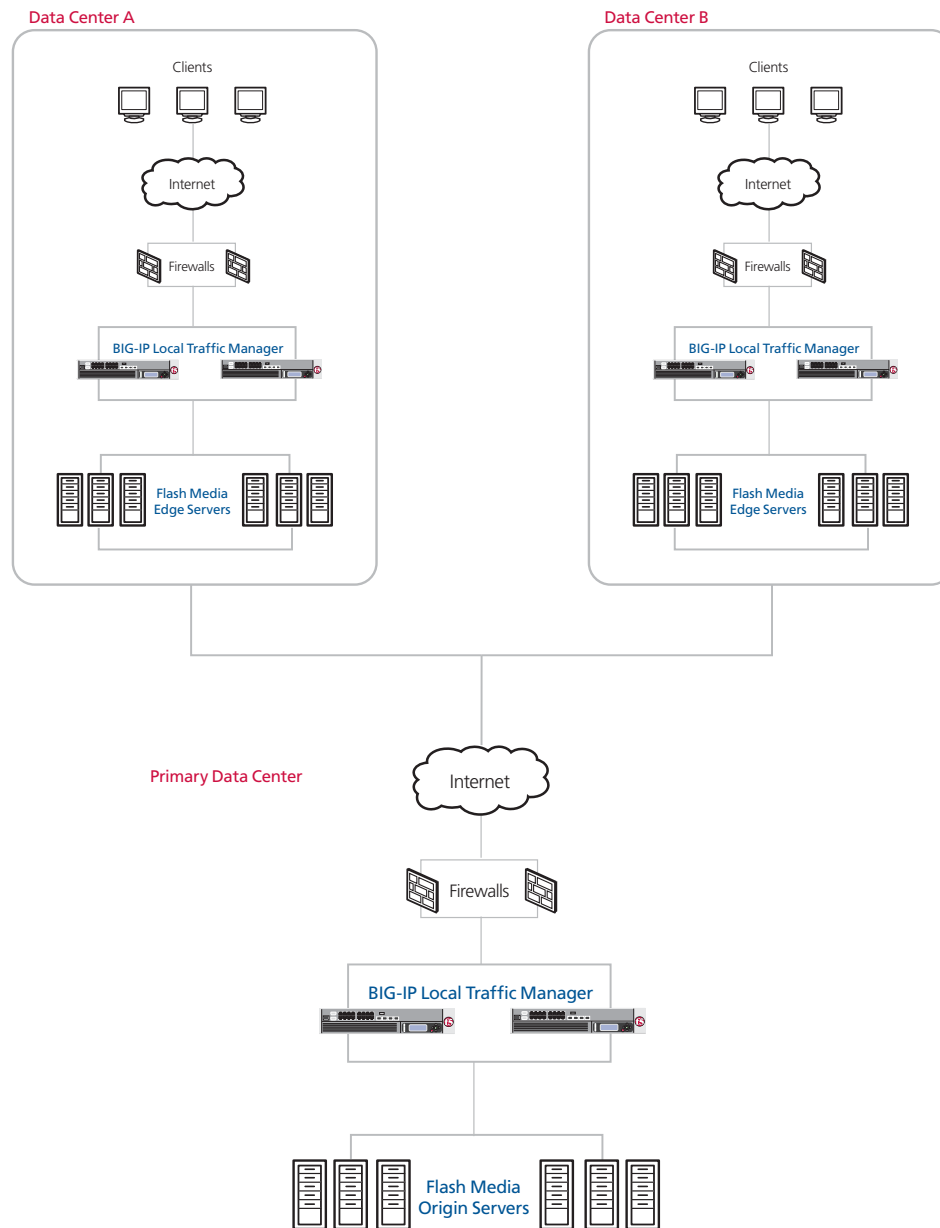


Figure 1 Logical configuration example

Configuring the BIG-IP LTM system

In this section, we configure the BIG-IP LTM system for the Flash Media devices. This section is broken up into the following sections:

- *Configuring the BIG-IP LTM for Flash Media Server using RTMPT*, following
- *Configuring the BIG-IP LTM for Flash Media Server using RTMPS*, on page 12
- *Configuring the BIG-IP LTM for Flash Media Server using RTMP*, on page 16
- *Configuring the BIG-IP LTM for Flash Media Server using RTMPE*, on page 17

The last section of this guide contains configuration modifications to the Adobe Flash Media Interactive Server that must be made in order for the deployment to function properly.

Configuring the BIG-IP LTM for Flash Media Server using RTMPT

As mentioned previously, RTMPT is RTMP encapsulated within HTTP requests in order to traverse firewalls. To configure the BIG-IP LTM, you must complete the following tasks:

- *Creating the TCP health monitor*, following
- *Creating the load balancing pool*, on page 5
- *Creating profiles*, on page 7
- *Creating the virtual server*, on page 9

Creating the TCP health monitor

For the Flash Media devices, we create a simple TCP health monitor.

To configure a TCP 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 **flash-rtmpt-tcp**.
4. From the **Type** list, select **tcp**.
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. In our example, we use an **Interval** of **30** and a **Timeout** of **91**.

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

Local Traffic >> Monitors >> New Monitor...

General Properties

Name	flash-rtmpt-tcp
Type	TCP
Import Settings	tcp

Configuration: Basic

Interval	30 seconds
Timeout	91 seconds
Send String	
Receive String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No

Cancel Repeat Finished

Figure 2 Configuring the TCP health monitor

Creating the load balancing pool

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

To create the LMS pool

- On the Main tab, expand **Local Traffic**, and then click **Pools**.
The Pool screen opens.
- In the upper right portion of the screen, click the **Create** button.
The New Pool screen opens.
- From the **Configuration** list, select **Advanced**.
- In the **Name** box, type a name for your pool.
In our example, we use **flash-rtmpt**.
- In the **Health Monitors** section, select the name of the monitor you created in the *Creating the TCP health monitor* section, and click the Add (<<) button. In our example, we select **flash-tcp**.
- In the **Slow Ramp Time** box, type **300**. For this pool, we use the Least Connections load balancing method. We set the Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the Least Connections load

balancing algorithm does not send all new connections to that member (a newly available member will always have the least number of connections).

7. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
In our example, we select **Least Connections (member)**.
8. In this pool, we leave the Priority Group Activation **Disabled**.
9. In the New Members section, make sure the **New Address** option button is selected.
10. In the **Address** box, add the first Flash device to the pool. In our example, we type **10.132.81.110**.
11. In the **Service Port** box, type **1935**.
12. Click the **Add** button to add the member to the list.
13. Repeat steps 10-12 for each server you want to add to the pool. In our example, we repeat these steps twice for the remaining servers, **10.132.81.111** and **112**.
14. Click the **Finished** button (see Figure 3).

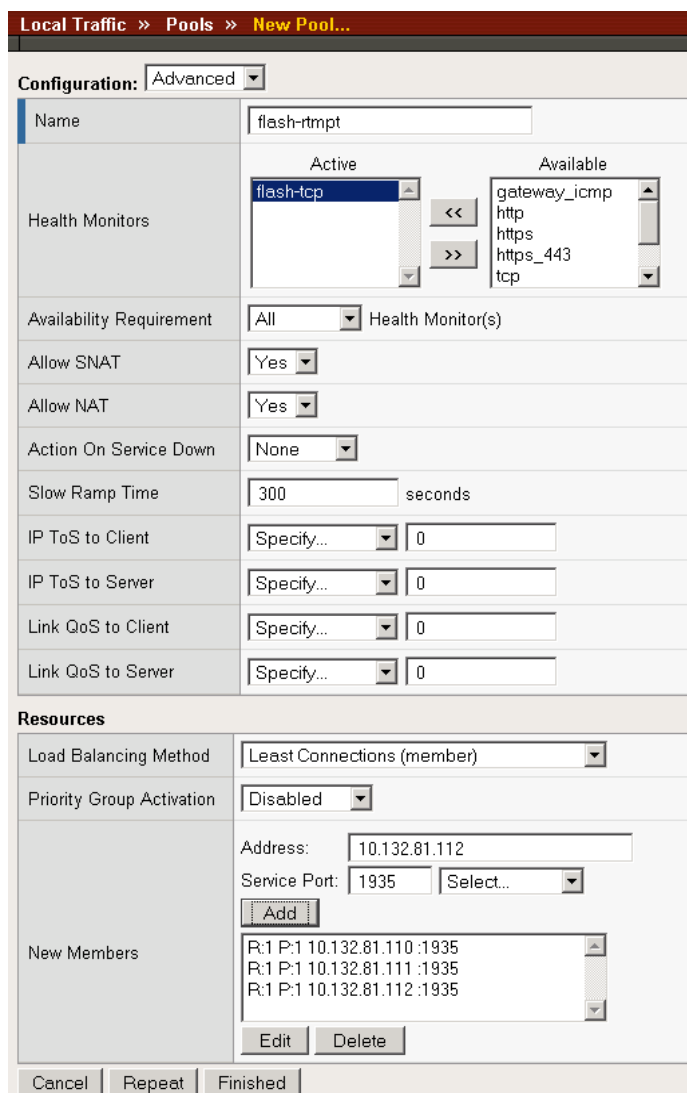


Figure 3 Configuring the Flash Media Server pool

Creating profiles

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

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

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. For this example, we use a simple HTTP profile.

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 **rtmpt-http**.
4. From the **Parent Profile** list, select **http**.
5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Adobe Flash Media users are accessing the portal via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the Portal 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.

◆ Tip

*If you are using a version of BIG-IP LTM previous to v9.4, the **Configuration Guide for BIG-IP Local Traffic Management** for version 9.4 (available on AskF5) shows the configuration differences between the base TCP profile and the optimized profile types. Use the Configuration Guide to manually configure the optimization settings.*

Creating the WAN optimized TCP profile

First we configure the WAN optimized profile. Remember, if most users are accessing the portal via the LAN, use the base TCP profile instead of this WAN optimized 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 **rtmpt-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 the LAN optimized TCP profile

Now we configure the LAN optimized profile. If you have already created a simple TCP profile, based off the default TCP profile (and not the WAN optimized profile above), you do not need to create another TCP profile, continue with the next procedure.

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 **rtmpt-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

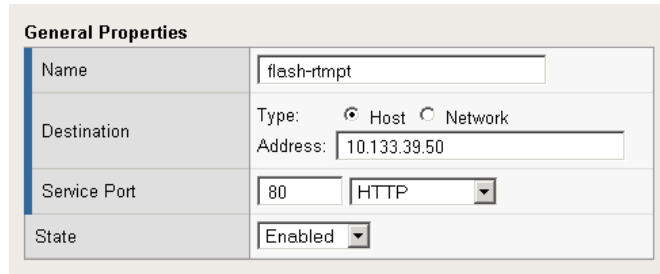
Creating the virtual server

Next, we configure a virtual server that uses 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 **flash-rtmpt**.

4. In the **Destination** section, click the **Host** button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.39.50**.
6. In the **Service Port** box, type **80**, or select **HTTP** from the list.



General Properties	
Name	flash-rtmpt
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.133.39.50
Service Port	80 HTTP
State	Enabled

Figure 4 Creating the new virtual server

7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. Leave the **Type** and **Protocol** lists at their default settings:
Standard and **TCP**.
9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **rtmpt-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 **rtmpt-tcp-lan**.
11. 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 **flash-rtmpt**.

Configuration: Advanced

Type	Standard
Protocol	TCP
Protocol Profile (Client)	rtmpt-tcp-wan
Protocol Profile (Server)	rtmpt-tcp-lan
OneConnect Profile	None
HTTP Profile	rtmpt-http
FTP Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None
	Enabled Available

Figure 5 Selecting the profiles for the virtual server

12. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the load balancing pool* section. In our example, we select **flash-pool**.
13. Click the **Finished** button.

Resources

iRules	Enabled	Available
	<<	>>
	Up	Down
Default Pool	+	flash-rtmpt
Default Persistence Profile		None
Fallback Persistence Profile		None

Cancel Repeat Finished

Figure 6 Resources section of the add virtual server page

This completes the BIG-IP LTM configuration for RTMPT. Be sure to continue to *Configuring Adobe Flash Media Interactive Server 3 for load balancing with the BIG-IP LTM system*, on page 18 for important changes that need to be made on the Flash Media Servers.

Configuring the BIG-IP LTM for Flash Media Server using RTMPS

If you are using encryption for your Flash Media Servers, F5 recommends using RTMPS, and not RTMPE when encryption is required, because of the performance benefits of offloading encryption on the BIG-IP LTM.

For RTMPS, the BIG-IP LTM system is first terminating SSL and directing traffic to one of the Adobe FMIS3 servers. The FMIS3 server assigns a cookie to each user session in order to achieve persistence. When the client returns to the BIG-IP LTM after the session has been defined, the LTM offloads the SSL and sends the traffic on to the server that hosts the appropriate session.

In this section, in addition to a few new procedures and steps, we refer to procedures used in the previous section.

◆ Important

*For information on configuring Adobe FMIS3 for SSL, see the section titled [Configure SSL in the FMIS3 Configuration and Administration Guide](#), available from the Adobe web site:
<http://www.adobe.com/support/documentation/en/flashmediaserver/>*

Creating the health monitor

The first step is to configure a TCP health monitor. Follow *Creating the TCP health monitor*, on page 4. Use a unique name, such as **flash-rtmpts-tcp**.

Creating the load balancing pool

The next step is to create the load balancing pool. Follow *Creating the load balancing pool*, on page 5. Use a unique name, such as **flash-rtmpts**, and the appropriate IP addresses.

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 Adobe Flash Media 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 the profiles

In this section, create the following profiles for RTMPTS.

Creating the HTTP profile

To create the HTTP profile, follow *Creating an HTTP profile*, on page 8. Use a unique name, such as **rtmpts-http**. All other fields are optional.

Creating the TCP profiles

To create the TCP profiles, follow *Creating the WAN optimized TCP profile*, on page 8 and *Creating the LAN optimized TCP profile*, on page 9. Use unique names, such as **rtmpts-tcp-wan** and **rtmpts-tcp-lan**. All other fields are optional.

Creating the persistence profile

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

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
3. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **rtmpts-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.

General Properties	
Name	rtmpts-cookie
Persistence Type	Cookie
Parent Profile	cookie

Configuration		Custom
Cookie Method	HTTP Cookie Insert	<input type="checkbox"/>
Cookie Name		<input type="checkbox"/>
Expiration	<input checked="" type="checkbox"/> Session Cookie	<input type="checkbox"/>

Cancel Repeat Finished

Creating a Client SSL profile

The next step 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 **rtmpts-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 virtual server

The final step is to create the BIG-IP LTM virtual server for RTMPTS. Follow *Creating the virtual server*, on page 9, using the new objects you created in this section, with the following additions/modifications:

- Step 3: Give the virtual server a unique name, such as **flash-rtmpts**.
- Step 5: Use the appropriate IP address.
- Step 6: Type **443**, or select **HTTPS** from the list.
- Addition 1: After selecting the HTTP profile in Step 11, from the **SSL Profile Client** list, select the name of the profile you created in *Creating a Client SSL profile*, on page 14. In our example, we type **rtmpts-clientssl**.
- Addition 2: After selecting the Default Pool in Step 12, from the **Default Persistence Profile** list, select persistence profile you created in *Creating the persistence profile*, on page 13. In our example, we type **rtmpts-cookie**.

This completes the BIG-IP LTM configuration for RTMPTS. Be sure to continue to *Configuring Adobe Flash Media Interactive Server 3 for load balancing with the BIG-IP LTM system*, on page 18 for important changes that need to be made on the Flash Media Servers.

Configuring the BIG-IP LTM for Flash Media Server using RTMP

If you are simply using RTMP for your Flash Media Server, use the following procedures. Note that F5 recommends you use RTMPS or RTMPT if you require security and session persistence, or if you are traversing a firewall. Offloading SSL encryption to the BIG-IP LTM will eliminate all encryption and decryption overhead from your servers.

Creating the health monitor

The first step is to configure a TCP health monitor. Follow *Creating the TCP health monitor*, on page 4. Use a unique name, such as **flash-rtmp-tcp**.

Creating the load balancing pool

The next step is to create the load balancing pool. Follow *Creating the load balancing pool*, on page 5. Use a unique name, such as **flash-rtmp**, and the appropriate IP addresses.

Creating the TCP profiles

For RTMP, we only create two TCP profiles. To create the TCP profiles, follow *Creating the WAN optimized TCP profile*, on page 8 and *Creating the LAN optimized TCP profile*, on page 9. Use unique names, such as **rtmp-tcp-wan** and **rtmp-tcp-lan**. All other fields are optional.

Creating the virtual server

The final step is to create the BIG-IP LTM virtual server for RTMP. Follow *Creating the virtual server*, on page 9, using the new objects you created in this section, with the following additions/modifications:

- Step 3: Give the virtual server a unique name, such as **flash-rtmp**.
- Step 5: Use the appropriate IP address.

This completes the BIG-IP LTM configuration for RTMP. Be sure to continue to *Configuring Adobe Flash Media Interactive Server 3 for load balancing with the BIG-IP LTM system*, on page 18 for important changes that need to be made on the Flash Media Servers.

Configuring the BIG-IP LTM for Flash Media Server using RTMPE

If you are using RTMPE for your Flash Media Server, use the following procedures.

Creating the health monitor

The first step is to configure a TCP health monitor. Follow *Creating the TCP health monitor*, on page 4. Use a unique name, such as **flash-rtmpe-tcp**.

Creating the load balancing pool

The next step is to create the load balancing pool. Follow *Creating the load balancing pool*, on page 5. Use a unique name, such as **flash-rtmpe**, and the appropriate IP addresses.

Creating the TCP profiles

For RTMP, we only create two TCP profiles. To create the TCP profiles, follow *Creating the WAN optimized TCP profile*, on page 8 and *Creating the LAN optimized TCP profile*, on page 9. Use unique names, such as **rtmpe-tcp-wan** and **rtmpe-tcp-lan**. All other fields are optional.

Creating the virtual server

The final step is to create the BIG-IP LTM virtual server for RTMPTE. Follow *Creating the virtual server*, on page 9, using the new objects you created in this section, with the following additions/modifications:

- Step 3: Give the virtual server a unique name, such as **flash-rtmpe**.
- Step 5: Use the appropriate IP address.

This completes the BIG-IP LTM configuration for RTMPE. Be sure to continue to *Configuring Adobe Flash Media Interactive Server 3 for load balancing with the BIG-IP LTM system*, on page 18 for important changes that need to be made on the Flash Media Servers.

Configuring Adobe Flash Media Interactive Server 3 for load balancing with the BIG-IP LTM system

This section contains a brief description of how to modify the settings on your FMIS server to properly deploy BIG-IP LTM in front of it.

◆ Important

These settings are just an overview of some of the Adobe FMIS3 configuration details related to load balancing. For more detailed instructions on configuring your Adobe FMIS3 server, see the Adobe documentation or contact Adobe.

Adjusting the keepalive time

By default, the Adobe FMIS3 comes installed with a keep alive setting that holds open connections indefinitely, with cookies turned off and with no route entry, which assumes a single host deployment. While the nature of the RTMP protocol is to have persistent, long lived connections, holding open a connection indefinitely can lead to resource exhaustion on your servers and networking equipment

In this procedure, we adjust the keepalive time so that the Flash Media Server works properly in a load balanced environment.

To adjust the keepalive time

1. Login to your Flash Media Interactive Server and navigate to the configuration directory, depending on your deployment:
 - On Microsoft Windows: **c:\Program Files\Adobe\Flash Media Server 3\conf**
 - On Linux: **<install Root>/conf**
2. Open the file **server.xml** in a text editor.
3. Find the **AutoCloseIdleClients** setting. Change this setting from **false** to **true**.
4. Adjust the **CheckInterval** and **MaxIdleTime** settings to match your traffic patterns. In our example, we use **20** for both the **CheckInterval** and **MaxIdleTime**.
5. Save and close the **server.xml** file.

```

<!-- Configures automatic disconnecting of idle clients. A client is -->
<!-- idle if it has not sent or received any application data for -->
<!-- some time. Application data does not include low level control -->
<!-- msgs such as the built-in server ping mechanism. This is meant -->
<!-- to clean up clients that, for example, are not playing or not -->
<!-- publishing a stream, etc. To enable this feature, set the -->
<!-- enable attribute to true. It is disabled by default. This can -->
<!-- be overridden on a per-vhost basis. However, if disabled here, -->
<!-- it is disabled for all vhosts. But if enabled here, vhosts can -->
<!-- override it and disable it for that vhost. Vhosts can also -->
<!-- override the max idle time (for that vhost only). -->
<!-- <CheckInterval> is not overridable and applies to all vhosts. -->
- <AutoCloseIdleClients enable="true">
  <!-- How often to check for idle clients. Specified in seconds. -->
  <!-- Default is to check every 60 sec. (1 min) -->
  <CheckInterval>20</CheckInterval>
  <!-- How long a client can be idle before it is disconnected. -->
  <!-- Specified in seconds. Default is 3600 sec. (1 hr) -->
  <MaxIdleTime>20</MaxIdleTime>
</AutoCloseIdleClients>

```

Figure 7 Excerpt from the server.xml file showing the keepalive settings

Turning on cookie support

By default the FMIS3 comes with cookie support turned off. In order to achieve persistence, cookies must be turned on in the FMIS3 server so that session persistence maps individual users back to the correct host. This setting also enables the HTTP protocol headers within the RTMP protocol.

To turn on cookie support

1. From the Flash Media Interactive Server configuration directory (as described in Step 1 of the preceding procedure), navigate down one directory to `_defaultRoot_`.
2. Open the file `adaptor.xml` in a text editor.
3. Find the `SetCookie` setting, and change the value from `false` to `true`.
4. Save and close the `adaptor.xml` file.

```

<!-- This specifies whether we should set a cookie. A cookie is -->
<!-- needed when dealing that load balancers, so that requests -->
<!-- corresponding to one net connection are always sent to the -->
<!-- same server. The cookie does add to the http header size so -->
<!-- will result in a higher bandwidth overhead. -->
<SetCookie>true</SetCookie>

```

Figure 8 Modifying the SetCookie value to true

Setting the route entry

The route entry setting controls the HOST header which the FMIS3 server sends in responses to the client. It is important for each FMIS3 server to respond with the IP address of the BIG-IP LTM virtual server.

To set the route entry

1. From the Flash Media Interactive Server configuration directory (as described in Step 1 of the preceding procedure), navigate down one directory to `_defaultVHost_`.
2. Open the file `vhost.xml` in a text editor.
3. Find the `RouteEntry` setting, and change the value to match the IP address and port number of the virtual server you created in *Creating the virtual server*, on page 9. In our example, our virtual server IP address is 10.133.39.50, and you have chosen to use the RTMPT protocol over port 443, your `RouteEntry` setting should be: `<RouteEntry>*:*; 10.133.39.50:443</RouteEntry>`
4. Save and close the `vhost.xml` file.
5. Stop and start your FMIS3 server.

```
- <RouteTable protocol="">
  <!-- Maps a host:port pair, to a different host:port pair. -->
  <!-- This tag is in the form <host1>:<port1>;<host2>:<port2> -->
  <!-- where host1:port1 is the host and port of the desired -->
  <!-- destination, and host2 and port2 is what should be used -->
  <!-- instead. In other words, connections to host1:port1 are -->
  <!-- routed to host2:port2 instead. For example, -->
  <!-- <RouteEntry>foo:1935;bar:80</RouteEntry> -->
  <!-- This says to route connections destined for host "foo" -->
  <!-- on port 1935, to host "bar" on port 80. -->
  <!-- We also allow the use of the wildcard character '*' to -->
  <!-- replace <host> and/or <port>. For example, -->
  <!-- <RouteEntry>*:*;foo:1935</RouteEntry> -->
  <!-- This says route connections destined for any host on -->
  <!-- any port to host "foo" on port 1935. -->
  <!-- '*' can also be used on the right-hand side. When used -->
  <!-- on the right-hand side, it means that the corresponding -->
  <!-- value on the left-hand side should be used. For example -->
  <!-- <RouteEntry>*:*:*:80</RouteEntry> -->
  <!-- This says route connections destined for any host on -->
  <!-- any port, to the same host on port 80. -->
  <!-- Additionally, you can also specify that a host:port -->
  <!-- combination be routed to null, which essentially means -->
  <!-- that connections destined for that host:port combo will -->
  <!-- be rejected. For example, -->
  <!-- <RouteEntry>foo:80;null</RouteEntry> -->
  <RouteEntry>*:*; 10.133.39.50:443</RouteEntry>
</RouteTable>
```

Appendix A: Configuring the Origin/Edge Server deployment scenario

For installations serving large numbers of connections or for audiences that may be geographically distributed, an Edge and Origin deployment is recommended. In this scenario, one group of servers acts as origin servers, containing the original content and another set of servers act as remote caches, which we refer to as edge servers.

In an Edge and Origin deployment scenario, high availability is maintained through the use of BIG-IP LTM Virtual Servers. Security can be offloaded by BIG-IP LTM as well. BIG-IP LTM devices are required at each physical site, or datacenter, which hosts edge servers and each site which hosts origin servers.

Edge deployments do not require any changes to the origin server configuration. During the installation of FMIS the default configuration is for an origin server. Use the instructions in the previous section of this FMIS deployment guide to setup your origin servers. There are two prerequisites in an Edge and Origin deployment:

- Only FMIS can handle Edge and Origin deployments. Flash Media development server or Flash Media streaming server cannot be used for Edge and Origin deployments.
- The operating system and disk format on the Edge server should be the same as the Origin server. Differences between operating systems or disk formats may cause filename conflicts or issues with upper and lowercase filenames which will break your deployment.

Configuring the BIG-IP LTM system

The BIG-IP LTM system configuration for the edge servers is identical to the configuration for the origin servers (although there are additional configuration procedures on the Adobe devices, see *Configuring the Flash Media Edge servers*, on page 22). To configure the BIG-IP LTM system for the edge devices, follow the appropriate origin section above (a list of the 4 sections follows), but use unique names and IP addresses for the objects where applicable.

- *Configuring the BIG-IP LTM for Flash Media Server using RTMPT*, on page 4
- *Configuring the BIG-IP LTM for Flash Media Server using RTMPS*, on page 12
- *Configuring the BIG-IP LTM for Flash Media Server using RTMP*, on page 16
- *Configuring the BIG-IP LTM for Flash Media Server using RTMPE*, on page 17

Configuring the Flash Media Edge servers

There are a few changes that need to be made to the `vhost.xml` file on each Flash Media edge server.

To modify the `vhost.xml` file

1. Login to your Flash Media Interactive Server and navigate to the configuration directory, depending on your deployment:
 - On Microsoft Windows: `c:\Program Files\Adobe\Flash Media Server 3\conf`
 - On Linux: `<install Root>/conf`
2. Navigate down one directory to `_defaultVHost_`.
3. Open the file `vhost.xml` in a text editor.
4. Find the **Mode** setting, and change the value to **remote**. This is the default and required setting for the edge servers.
5. Find the **Anonymous** setting, and change the value to **true**. This configures the FMIS server in an implicit installation. For explicit installations, set this to **false**. F5 recommends an implicit installation which requires no changes to the URL presented to the end user.
6. Find the **CacheDir** setting, and change the value to **true**. This turns on the local cache on the Edge server, which reduces bandwidth requirements. This step is optional.
7. Find the **RouteEntry** setting, and change the value to the Edge Server virtual server IP address and port and the Origin Server virtual server IP address and port. For example, if your new Edge Virtual IP is 10.10.1.1 and your protocol is RTMPS and your Origin Virtual IP Address is 10.133.39.50 and your protocol is RTMPS, the Route Entry would look like the following:


```
<RouteEntry>10.10.1.1:443;10.133.39.50:443</RouteEntry>
```

```
- <Proxy>
  <Mode>remote</Mode>
  <Anonymous>true</Anonymous>
  <CacheDir enabled="true" useAppName="true" />
- <RouteTable protocol="">
  <RouteEntry> 10.10.1.1:443 ; 10.133.39.50:443 </RouteEntry>
</RouteTable>
</Proxy>
```

Figure 9 Excerpt from the `vhost.xml` file, edited to show relevant settings

8. Save and close the `vhost.xml` file. This completes the edge server configuration.