



Using F5 BIG-IP LTM with Adobe LiveCycle Data Services ES2

July 28, 2010

Introduction

This document contains some essential channel configurations and a configuration which was used for near real time messaging testing. This configuration was optimized for low message latency in our lab. The devices which we used are listed. All devices were in different subnets in a 1 gigabit network.

- LCDS server – HP ProLiant DL380
- LCDS Edge server - HP ProLiant DL380 G6
- BigIP LTM – F5 3600

Using F5 BIG-IP LTM with Adobe LiveCycle Data Services ES2

This document describes how to connect and enable the use of LiveCycle Data Services ES2, LiveCycle Data Services ES2 Edge server, and BigIP LTM together. In this configuration, the BigIP LTM machine performs load balancing, SSL termination (thereby optionally offloading the SSL decryption for RTMPS or HTTPS to the F5 BigIP machine), and HTTP-based authentication. BigIP LTM is capable of handling traffic volumes from 1 to 12 Gigabits per second, depending on which model is used.

LiveCycle Data Services ES2 Edge Server can pre-authenticate connections before it proxies connections back to a LiveCycle Data Services instance. If authentication is enabled between the edge and server tiers, anonymous connections are prohibited. If authentication is disabled between edge and server tiers, there is effectively no functional difference between an F5 BigIP LTM to edge tier to server tier configuration, compared to an F5 BigIP LTM to server tier (ie no edge tier) configuration.

For the load balancing considerations, the F5 BigIP LTM should not become a bottleneck for real-time systems. Planning for load balancing should test your hardware throughput. You can measure the throughput with the load-testing tool, client and message generator included with the LiveCycle Data Services ES2 product.

Edge Server Architecture

The LiveCycle Data Services ES2 Edge Server is placed in the DMZ to route authenticated or authorized connections to the LiveCycle Data Services ES2 server. With SSL termination, the F5 BIG-IP LTM System is placed in front of the LiveCycle Data Services ES2 Edge Server. If you want to use the F5 BIG-IP LTM System for load balancing, you cannot use the LCDS reliable messaging feature. This means the F5 BIG-IP LTM System must use a pool with a single LCDS server or LiveCycle Data Services ES2 Edge Server to use Reliable Messaging.

Architecture Overview

Architecturally, a LiveCycle Data Services ES2 Edge Server fits into enterprise network topology as Figure 1. Clients connect to Edge server or to the F5 BigIP LTM. The channel classes need to match their protocol. The class defined in channel definition is used by actionscript clients. The endpoint class is used by server. If SSL termination is happened on F5 BigIP, the channel class is secure channel while the endpoint is not. Flash player security doesn't allow application to connect any location other than the place which the application is loaded. You have to make sure to have crossdomain.xml specified either in channel definition or nio server in order to get client load balancing or failover to work. Using the BigIP LTM for SSL termination not only offloads processing to the BigIP LTM away from the server, but also aids troubleshoots because traffic is decrypted and thus not requiring you to catch the three-way tis handshake and operations processing the certificate's key to decrypt the traffic. The rest of BigIP LTM functions, you can reference to its documentation. However, it is recommended to have BigIP health monitor when you configure the profiles. It is because a port being open doesn't mean the endpoint are functioning and accepting connections.

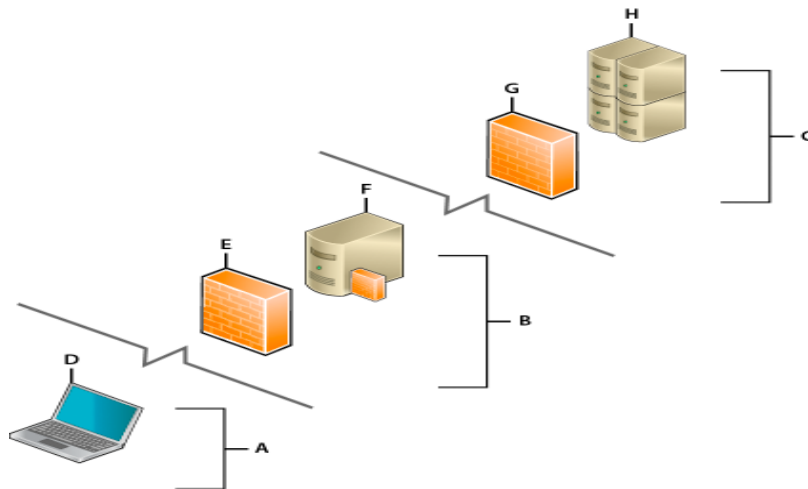


Figure 1: Deployment Tiers. A) Client, B) Edge Tier, C) Server Tier

Configuration for SSL Termination

The following diagram shows use of client side load balancing and SSL termination. Clients pick a channel randomly in the client load balancing channels. These channels connect to the F5 BigIP LTM for SSL termination. The F5 BigIP LTM also acts as a load balancer to 2 different LiveCycle Data Services ES2 Edge Servers. Edge server connect to LCDS server through amf connection for every RTMP connection.

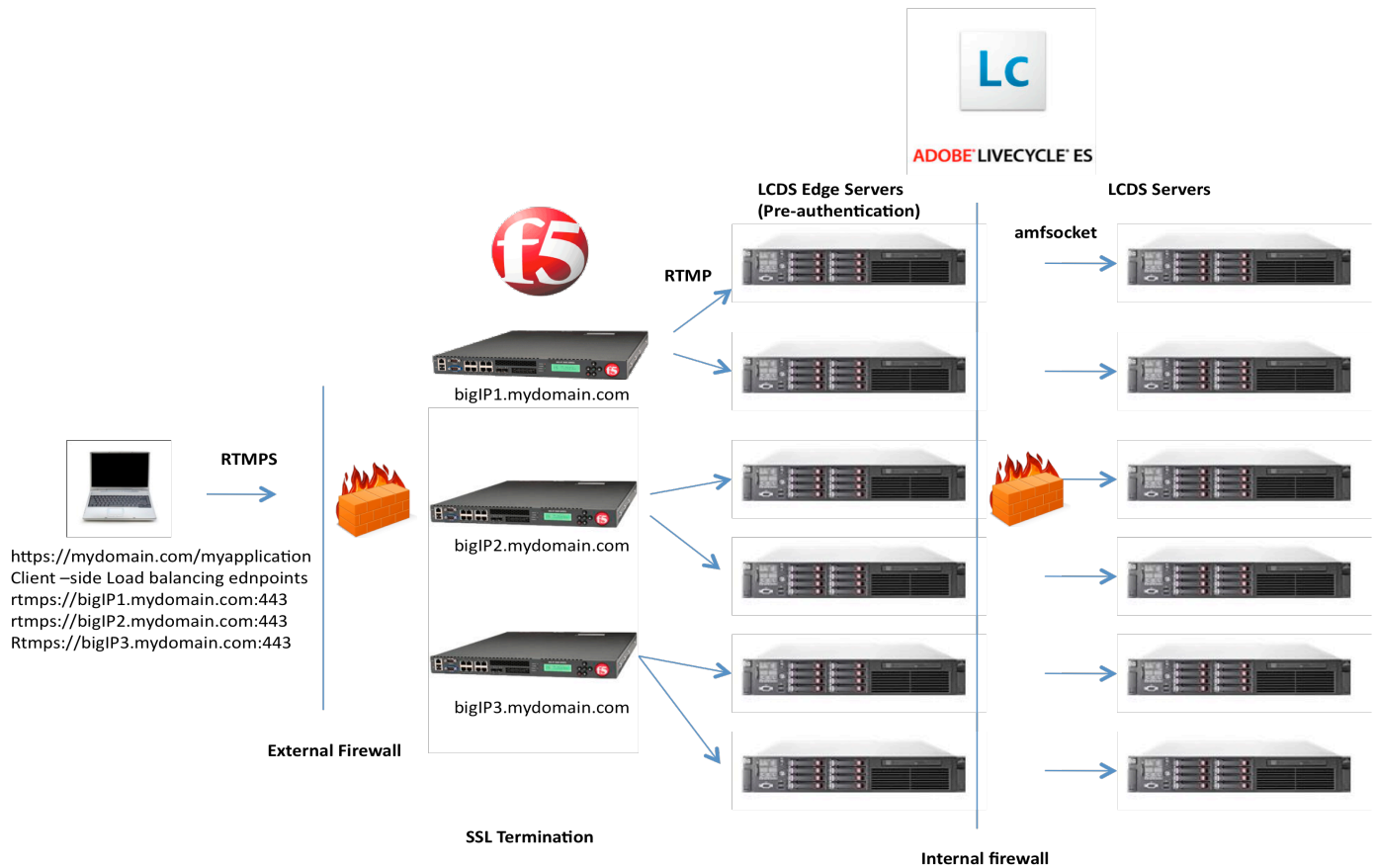


Figure 2: Client side load balancing and F5 BigIP-based SSL termination

Channel definitions

Channel definitions are defined in `services-config.xml`. LCDS server instantiate the channels in this configuration file if they are not marked as `remote="true"`. Flex applications are also compiled with `services-config.xml` to have connectivity information. It is not necessary to have same configuration file for both server and application compilation. There are two tokens which can be used in the channel definition. They are `{server.name}` and `{server.port}`. When these two tokens appear in the channel definition, clients use the loaded application's URL domain and port to construct the endpoint URL.

Standard Channel

Clients connect to the server from which the application was loaded and use port 1935. On the server side, this endpoint binds to all NICs using port 1935.

```
<channel-definition class="mx.messaging.channels.RTMPChannel" id="my-rtmp">
  <endpoint class="flex.messaging.endpoints.RTMPEndpoint" url="rtmp://{server.name}:1935"/>
</channel-definition>
```

Channel using bind-port

Clients connect to the server using the endpoint URL, but the endpoint actually listens on the port number specified as the value of the bind-port property. The bind-port configuration is useful when the server and client services-configuration.xml are the same file. Clients connect to a load balancer at port 1935 when the actual LCDS channel port is 2215.

```
<channel-definition class="mx.messaging.channels.RTMPChannel"
  id="my-bigIP-rtmp" remote="true">
  <endpoint class="flex.messaging.endpoints.RTMPEndpoint" url=" rtmp://bigIP.adobe.com:1935"/>
  <properties>
    <bind-port>2215</bind-port>
  </properties>
</channel-definition>
```

Channel using bind-port with SSL termination

Clients connect to the F5 BIG-IP LTM System through SSL channel and have SSL termination. The channel definition class is mx.messaging.channels.SecureRTMPChannel, and the endpoint class is flex.messaging.endpoints.RTMPEndpoint.

```
<channel-definition class="mx.messaging.channels.SecureRTMPChannel" id="my-bigIP-rtmps">
  <endpoint class="flex.messaging.endpoints.RTMPEndpoint" url=" rtmps://bigIP.adobe.com:443"/>
  <properties>
    <bind-port>2215</bind-port>
  </properties>
</channel-definition>
```

Using separate Server and Client side services-config.xml

Server side:

```
<channel-definition class="mx.messaging.channels.RTMPChannel" id="my-bigIP-rtmps">
  <endpoint class="flex.messaging.endpoints.RTMPEndpoint" url=" rtmps://bigIP.adobe.com: 2215"/>
</channel-definition>
```

Client side:

```
<channel-definition class="mx.messaging.channels.SecureRTMPChannel" id="my-bigIP-rtmps">
  <endpoint class="flex.messaging.endpoints.SecureRTMPEndpoint " url=" rtmps://bigIP.adobe.com: 443"/>
</channel-definition>
```

Edge server channel

The LiveCycle Data Services Edge Server communicates with the LCDS server over amf socket connections.

LCDS server:

```
<channel-definition class="mx.messaging.channels.RTMPChannel" id="my-edge-rtmp" remote="true">
  <endpoint class="flex.messaging.endpoints.RTMPEndpoint" url=" rtmp://edge.adobe.com: 2215"/>
</channel-definition>
```

Edge Server

```
<channel-definition class="mx.messaging.channels.RTMPChannel" id="my-edge-rtmp">
  <endpoint class="flex.messaging.endpoints.RTMPEndpoint " url=" rtmp://edge.adobe.com: 2215"/>
</channel-definition>
```

Edge server pre-authentication: set require-authentication property to true. Only successfully authenticated connections are routed to the LCDS server

```
<service class="flex.messaging.services.GatewayService" id="perf-edge-auto-GatewayService">
  <properties>
```

```

<gateway-endpoint>
<require-for-startup>true</require-for-startup>
<require-authentication>true</require-authentication>
  <urls>
    <url>amfsocket://lcds.adobe.com:4321</url>
  </urls>
</gateway-endpoint>
</properties>
</service>

```

Edge server pre-authorization: apply a security constraint to the gateway service. Only the users in the required role are allowed to connect to the LCDS server.

```

<service class="flex.messaging.services.GatewayService" id="perf-edge-auto-GatewayService">
  <default-security-constraint ref="traders-and-admins"/>
  <properties>
    <gateway-endpoint>
      <require-for-startup>true</require-for-startup>
      <urls>
        <url>amfsocket://lcds.adobe.com:4321</url>
      </urls>
    </gateway-endpoint>
  </properties>
</service>

```

Client load balancing channel

You can use client load balancing to distribute client connections across available LCDS servers in the absence of a load balancer. Client applications compiled against an endpoint configuration with client-load-balancing uses this set of URLs for connectivity rather than the URL specified for the endpoint. The endpoint URL value will not be compiled into the SWF file. Before the client initially connects, it shuffles this full set of URLs and assigns one at random as the primary URL for its channel, and assigns the remainder to the failover URLs property on its Channel. If you use SSL termination on the F5 BIG-IP LTM system, change the channel definition class to SecureRTMPChannel. You also have to consider the Flash Player security. Without the crossdomain.xml, clients cannot connect to any server other than the location of the application is loaded.

Client side services-config.xml file

```

<channel-definition id="my-http" class="mx.messaging.channels.RTMPChannel " >
  <endpoint url=" rtmp://lcds1.adobe.com:2215" class=" flex.messaging.endpoints.RTMPEndpoint"/>
  <properties>
    <client-load-balancing>
      <url>rtmp://lcds1.adobe.com:2215</url>
      <url> rtmp://lcds2.adobe.com:2215</url>
      <url> rtmp://lcds3.adobe.com:2215</url>
    </client-load-balancing>
  </properties>
</channel-definition>

```

Gateway Endpoint Tuning on LCDS server

If the gateway-endpoint endpoint in the LCDS server configuration doesn't have a server-ref value, the endpoint creates a server with the default settings. For high message volume, you should define a server to be used by the gateway-endpoint and increase the buffer size and number of worker threads. Changing these settings can greatly improve performance. The message latency can be brought down from tens of milliseconds to several milliseconds. In testing, with a send rate of 60,000 messages per second and a 1 kilobyte payload size, the message latency was 72 ms using the default server settings. By increasing the buffer sizes, the message latency was brought down to 5 ms.

LCDS server services-config.xml file for gateway-endpoint

```

<server class="flex.messaging.socketserver.SocketServer" id="perf-nio-edge-server">
  <properties>

```

```

<connection-read-buffer-size>8192</connection-read-buffer-size>
<connection-write-buffer-size>65536</connection-write-buffer-size>
<socket-receive-buffer-size>8192</socket-receive-buffer-size>
<socket-send-buffer-size>65536</socket-send-buffer-size>
<connection-buffer-type>heap</connection-buffer-type>
<socket-tcp-no-delay-enabled>true</socket-tcp-no-delay-enabled>
<worker-thread-priority>5</worker-thread-priority>
<reactor-count>8</reactor-count>
<http>
  <session-timeout-minutes>1</session-timeout-minutes>
</http>
</properties>
</server>

<channel-definition id="gateway-endpoint" server-only="true" >
  <endpoint class="flex.messaging.endpoints.GatewayEndpoint" url="amfsocket://localhost:9807"/>
  <server ref="perf-nio-edge-server"/>
</channel-definition>

```

BIG-IP LTM system configuration for use with RTMP endpoints

To configure the F5 BIG-IP LTM System to direct requests to an RTMP endpoint, Complete these steps:

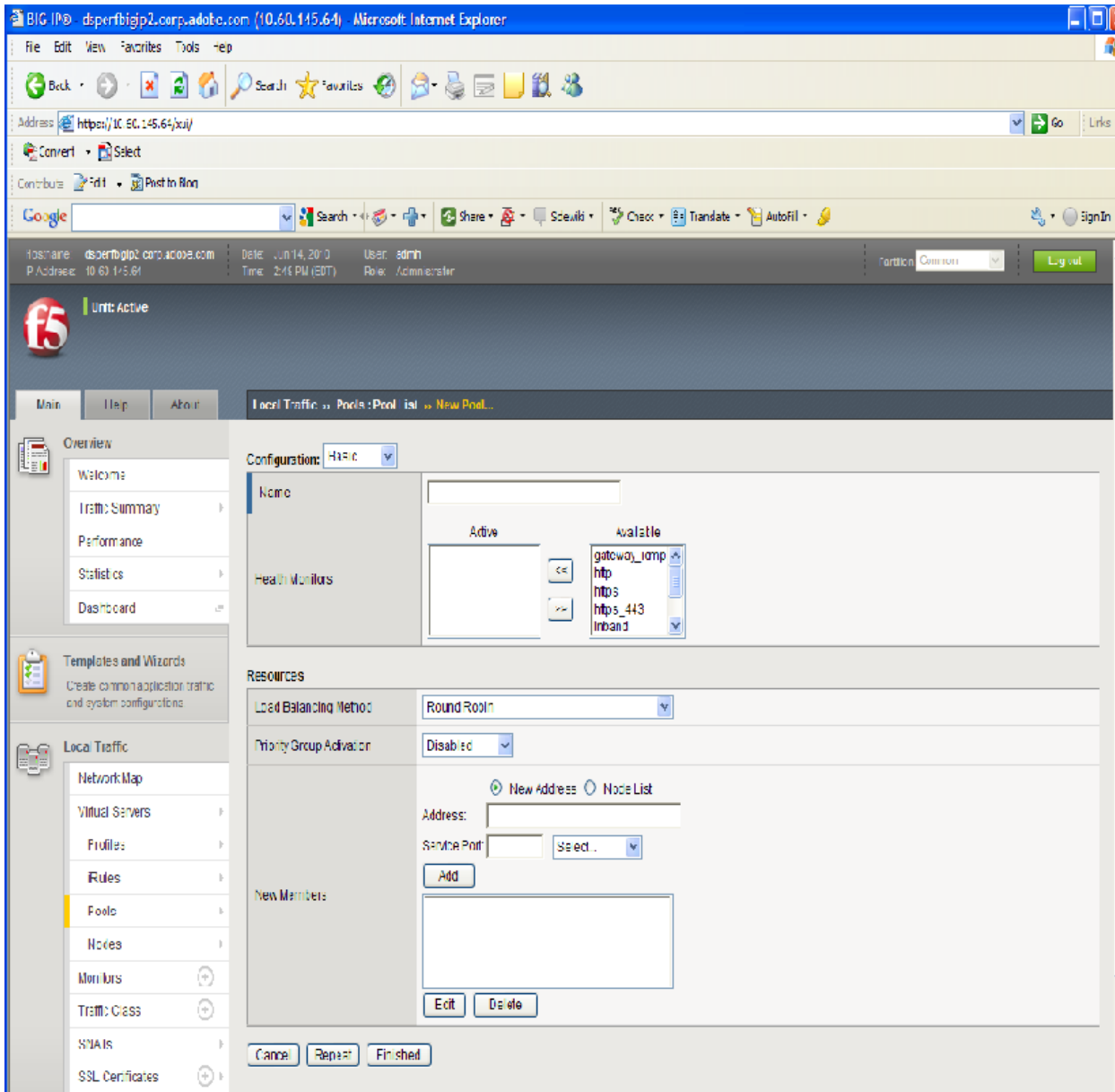
1. Create the health monitor(optional)
2. Create the LCDS RTMP pool
3. Create the profile
4. Create the virtual server

Create the TCP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor. For example, qa-perf-edge-rtmp.
4. From the **Type** list, select **tcp**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout
6. Click the **Finished** button.

Create the LCDS server pool

1. On the main tab, click Local Traffic to expand it.
2. Go to Pools and select Pool List.
3. Click the create button.
4. Enter the name. (ex. lcds-edge-pool)
5. Select the health Monitor.(optional, from previous example qa-perf-edge-rtmp)
6. Load Balancing Method : Round Robin (I use least Connection members, since rtmp is open connection. Round Robin cannot evenly distribute load)
7. Add LCDS server and endpoint port to address and Sevice Port for all LCDS servers
8. Click Finished



Create profile for low message latency

1. Expand Local Traffic.
2. Click on Profiles and select TCP protocol.
3. Click create.
4. Enter name. (ex lcds-edge-profile)
5. Parent profile select tcp-wan-optimized
6. Delay Acks: disabled
7. Selective Acks: disabled
8. Slow start: disabled
9. Bandwidth delay: disabled
10. Nagle's Algorithm: disabled
11. Click Finished

Delayed Acks	<input type="checkbox"/>	<input checked="" type="checkbox"/>
--------------	--------------------------	-------------------------------------

Selective ACKs	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Extended Congestion Notification	<input type="checkbox"/>	<input type="checkbox"/>
Extensions for High Performance (RFC 1323)	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Limited Transmit Recovery	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Slow Start	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Deferred Accept	<input type="checkbox"/>	<input type="checkbox"/>
Verified Accept	<input type="checkbox"/>	<input type="checkbox"/>
Bandwidth Delay	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Nagle's Algorithm	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Create a client SSL profile(SSL Termination)

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**
2. On the Menu bar, from the SSL menu, select **Client**.
3. In the upper right portion of the screen, click the **Create** button.
4. In the **Name** box, type a name for this profile.(ex: lcds-ssl-profile)
5. In the Configuration section, check the **Custom box**
6. Select your Certification (Please refer to BigIP documentation for keys and certifications create/import)
7. Select your Key
8. Click Finished

Creating a virtual Server

1. On the Main tab, expand Local Traffic, and then click Virtual servers
2. Click the Create button in the upper right portion of the screen.
3. Enter the server name into the name box(ex: lcds-server)
4. Enter the address for the virtual server and the port(LCDS channel endpoint)

General Properties	
Name	<input type="text" value="yourdomain.com"/>
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: <input type="text" value="10.60.144.99"/>
Service Port	<input type="text" value="2155"/> <input type="button" value="Select..."/>
State	<input type="button" value="Enabled"/>

5. Select Advanced in the Configuration dropdown box
6. Select Protocol Profile(client) and Protocol Profile(server) for the one which created(lcds-edge-profile)
7. OneConnect Profile should be None
8. SSL Profile (Client) : select your SSL profile if SSL termination is desired(lcds-ssl-profile)

Configuration: **Advanced** ▾

Type	Standard ▾
Protocol	TCP ▾
Protocol Profile (Client)	lcds-edge ▾
Protocol Profile (Server)	lcds-edge ▾
OneConnect Profile	None ▾
NTLM Conn Pool	None ▾
HTTP Profile	None ▾
FTP Profile	None ▾
Stream Profile	None ▾
XML Profile	None ▾
SSL Profile (Client)	None ▾
SSL Profile (Server)	None ▾

9. Select default pool using the created tcp pool(lcds-edge-pool)

10. Click Finished

Resources

iRules	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; width: 150px; height: 40px; margin-bottom: 5px;"></div> <div style="text-align: center;"> << << >> >> </div> <div style="border: 1px solid gray; padding: 5px; width: 150px;"> _sys_auth_krbdelegate _sys_auth_ldap _sys_auth_radius _sys_auth_ssl_cc_ldap _sys_auth_ssl_cridp </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> Up Down </div>
HTTP Class Profiles	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; width: 150px; height: 40px; margin-bottom: 5px;"></div> <div style="text-align: center;"> << << >> >> </div> <div style="border: 1px solid gray; padding: 5px; width: 100px;"> httpclass </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> Up Down </div>
Default Pool	+ qa-perf-edge-rtmp ▾
Default Persistence Profile	None ▾
Fallback Persistence Profile	None ▾

Cancel Repeat Finished

Test Results with and without Big-IP LTM using LCDS Load Testing Tool

The results below demonstrate that the additional hop added with an F5 BigIP LTM is negligible when properly configured.

Results without F5 Big-IP LTM:

[INFO] [RtmpTest] Virtual Consumer avg receive rate: 119.97 msg/s
[INFO] [RtmpTest] Virtual Consumer min receive rate: 119.87 msg/s (25201 msgs in 210.23s)
[INFO] [RtmpTest] Virtual Consumer max receive rate: 120.0 msg/s (25541 msgs in 212.85s)
[INFO] [RtmpTest] Virtual Consumer avg latency: 3.79 ms
[INFO] [RtmpTest] Virtual Consumer min latency: 0 ms
[INFO] [RtmpTest] Virtual Consumer max latency: 53 ms
[INFO] [RtmpTest] Virtual consumer std latency: 4.91 ms

Results with F5 Big-IP LTM:

[INFO] [RtmpTest] Virtual Consumer avg receive rate: 119.77 msg/s
[INFO] [RtmpTest] Virtual Consumer min receive rate: 119.69 msg/s (25323 msgs in 211.57s)
[INFO] [RtmpTest] Virtual Consumer max receive rate: 119.8 msg/s (25181 msgs in 210.19s)
[INFO] [RtmpTest] Virtual Consumer avg latency: 4.97 ms
[INFO] [RtmpTest] Virtual Consumer min latency: 2 ms
[INFO] [RtmpTest] Virtual Consumer max latency: 53 ms
[INFO] [RtmpTest] Virtual consumer std latency: 3.71 ms

Useful Links

http://help.adobe.com/en_US/LiveCycleDataServicesES/3.1/Developing/lcds31_using.pdf

<http://www.f5.com/pdf/deployment-guides/adobe-connectprofessional-dg.pdf>

http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip_getting_started_guide_10_1_0.html