F5 Networks Training

Getting Started with BIG-IP

Part Two: Application Delivery

Lab Guide

July, 2017

Getting Started with BIG-IP Lab Guide

Part Two: Application Delivery

Lab Guide

Fourth Printing; July, 2017

This manual was written for BIG-IP® products version 13.0.

Support and Contact Information

Obtaining Technical Support

Web	support.f5.com (Ask F5)
Phone	(206) 272-6888
Email (support issues)	support@f5.com
Email (suggestions)	feedback@f5.com

Contacting F5 Networks

Web	www.f5.com
Email	sales@f5.com & info@f5.com

F5 Networks, Inc.

Corporate Office
401 Elliott Avenue West
Seattle, Washington 98119
T (888) 88BIG-IP
T (206) 272-5555
F (206) 272-5557
Training@f5.com

F5 Networks, Ltd.

United Kingdom
Chertsey Gate West
Chertsey Surrey KT16 8AP
United Kingdom
T (44) 0 1932 582-000
F (44) 0 1932 582-001
EMEATraining@f5.com

F5 Networks, Inc.

Asia Pacific
5 Temasek Boulevard
#08-01/02 Suntec Tower 5
Singapore, 038985
T (65) 6533-6103
F (65) 6533-6106
APACTraining@f5.com

F5 Networks, Inc.

Japan
Akasaka Garden City 19F
4-15-1 Akasaka, Minato-ku
Tokyo 107-0052 Japan
T (81) 3 5114-3200
F (81) 3 5114-3201
JapanTraining@f5.com

Legal Notices

Copyright

F5 Networks; Inc. (F5) believes the information it furnishes to be accurate and reliable. However; F5 assumes no responsibility for the use of this information; nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent; copyright; or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, AskF5, ASM, BIG-IP, BIG-IP EDGE GATEWAY, BIG-IQ, Cloud Extender, Cloud Manager, CloudFucious, Clustered Multiprocessing, CMP, COHESION, Data Manager, DDoS Frontline, DDoS SWAT, Defense.Net, defense.net [DESIGN], DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, ENGAGE, Enterprise Manager, F5, F5 [DESIGN], F5 Agility, F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FCINCO, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, iCall, iControl, iHealth, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, LineRate, LineRate Point, LineRate Precision, LineRate Systems [DESIGN], Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Ready Defense, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAS (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Applications Services, Silverline, SSL Acceleration, SSL Everywhere, StrongBox, SuperVIP, SYN Check, SYNTHESIS, TCP Express, TDR, TechXchange, TMOS, TotALL, TDR, TMOS, Traffic Management Operating System, Traffix, Traffix [DESIGN], Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent. All other product and company names herein may be trademarks of their respective owners.

Materials

The material reproduced on this manual; including but not limited to graphics; text; pictures; photographs; layout and the like ("Content"); are protected by United States Copyright law. Absolutely no Content from this manual may be copied; reproduced; exchanged; published; sold or distributed without the prior written consent of F5 Networks; Inc.

Patents

This product may be protected by one or more patents indicated at: http://www.f5.com/about/policies/patents

Table of Contents

Labs **1**

Lab 1: Processing Traffic 1

Lab 2: Resolving Routing Issues with SNAT Auto Map 7

Lab 3: Monitoring Application Health 11

Lab 4: Modifying Traffic Behavior with Profiles 15

Getting Started with BIG-IP Lab Guide

Lab 1: Processing Traffic

This lab corresponds with the activities presented in **Lesson 1** of *Getting Started with BIG-IP: Part 2 – Application Delivery*.

Estimated time for completion: 20 minutes

Lab Objectives

- Configure a virtual server that will load balance traffic to a back-end web application.
- Access the virtual server to ensure it is correctly delivering the web application.
- View traffic statistics on the BIG-IP system to confirm traffic flow.

Lab Requirements

You must have successfully completed the instructions entitled “Starting up the Lab Environment” in the *Getting Started Lab Introduction* document.

Access the BIG-IP System

1. Click the **Firefox Web Browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at https://192.168.1.31.)
2. Log in to your BIG-IP system as the **admin** user and with password **admin.**
3. Navigate to **System » Archives**.
4. Click the **BIGIP2_Lab1_pool.ucs** file from the list, and then click the **Restore** button.
5. The restore process will take about a minute or two. Please wait until the **Operation Status** message indicates **Saving active configuration…** Be patient.
6. Then click the **OK** button.

Continue with Step 1 on the next page.

Create and Test the Application Delivery Configuration

Create a load balancing pool

1. Create a Round Robin load balancing pool with three pool members.

Configuration utility		
Local Traffic » **Pools** » **Pool List**, then click **Create**		
Configuration section		
	Name	**http_pool**
Resources section:		
	New Members	Address: **172.16.20.1** Service Port **80**, then click **Add** Address: **172.16.20.2** Service Port **80**, then click **Add** Address: **172.16.20.3** Service Port **80**, then click **Add**
When complete, click…		**Finished**

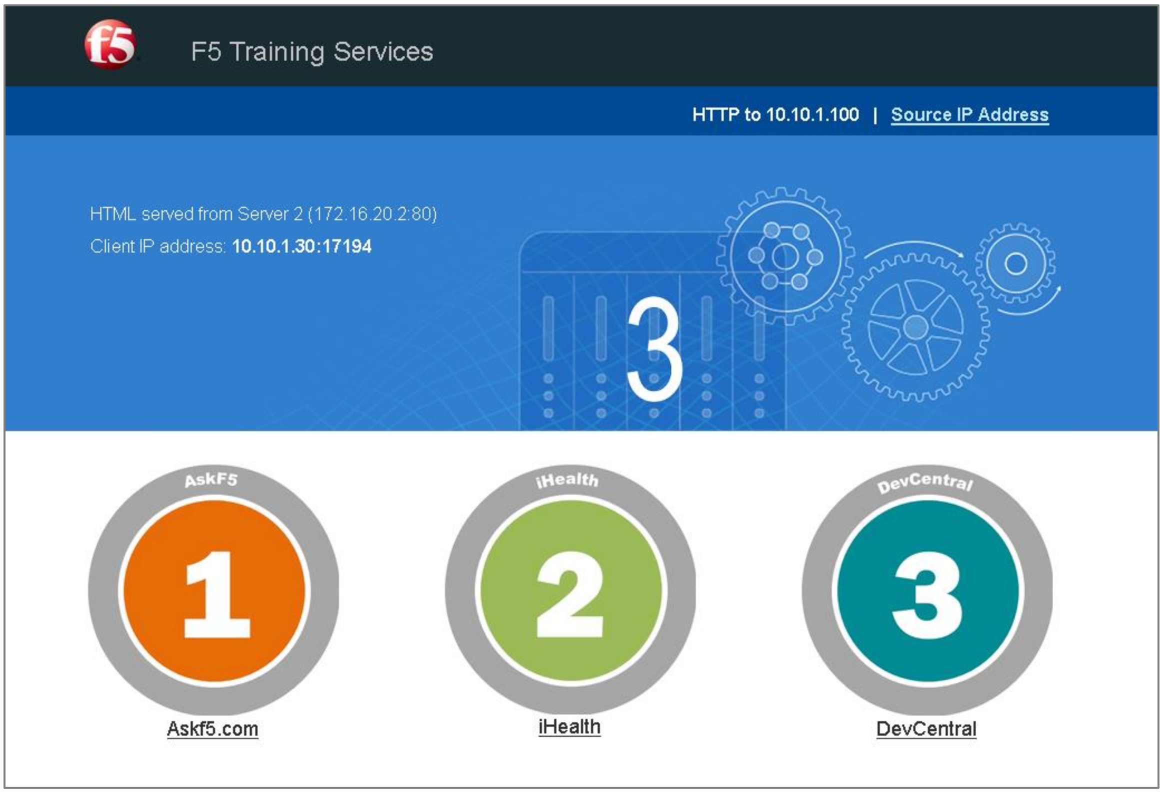
Create a virtual server

2. Create a virtual server at the destination address 10.10.1.100 that load balances to http_pool.

Configuration utility		
Local Traffic » **Virtual Servers** » **Virtual Server List**, then click **Create**		
General Properties section		
	Name	**http_vs**
	Destination Address:	**10.10.1.100**
	Service Port	**80** (or type or select **HTTP**)
Resources section:		
	Default Pool	**http_pool**
When complete, click…		**Finished**

Access the virtual server to test application delivery

3. Open a new tab on your Firefox browser, and connect to the virtual server at **http://10.10.1.100**. You should see a page similar to this:



F5 Training Services

HTTP to 10.10.1.100 | Source IP Address

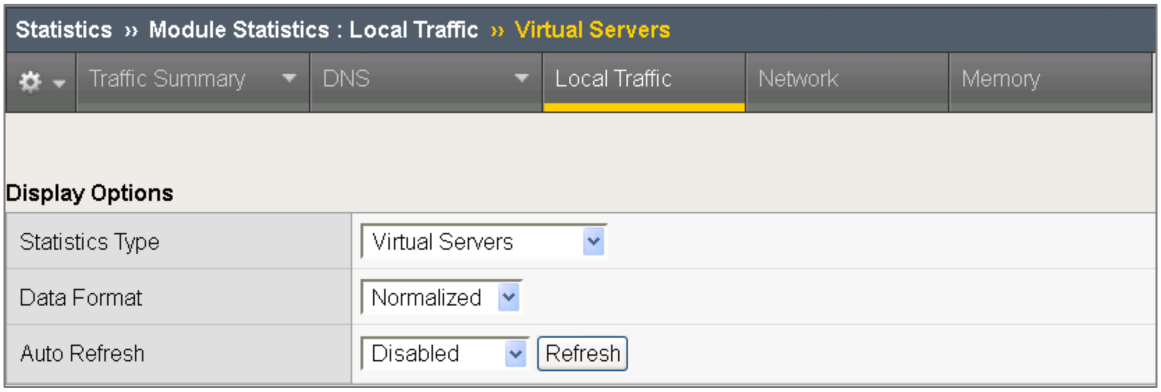
HTML served from Server 2 (172.16.20.2:80)

Client IP address: **10.10.1.30:17194**

4. Hard refresh the screen 5-10 times using **Ctrl** + **F5**. (This bypasses your browser's cache and forces content to be returned from the server again.) You should see the values on the page change, depending on how your requests are load balanced.
5. Scroll down on the page to read a little about this web application. It is used throughout the Getting Started Series labs.

View statistics to confirm traffic flow patterns

6. Back on your BIG-IP system, navigate to **Statistics** » **Module Statistics** » **Local Traffic**, and set **Statistics Type** to **Virtual Servers**, as shown below:


Statistics » Module Statistics : Local Traffic » Virtual Servers
Traffic Summary
DNS
Local Traffic
Network
Memory
Refresh

Display Options

Statistics Type	Virtual Servers
Data Format	Normalized
Auto Refresh	Disabled

   a. Do you see traffic going both into and out of the virtual server?

   b. What is the total number of connections made to the virtual server from the client?

   c. What is the total number of bits sent out from the virtual server to the client?

7. Change the **Statistics Type** to **Pools**.

   a. Do you see traffic going both into and out of the pool?

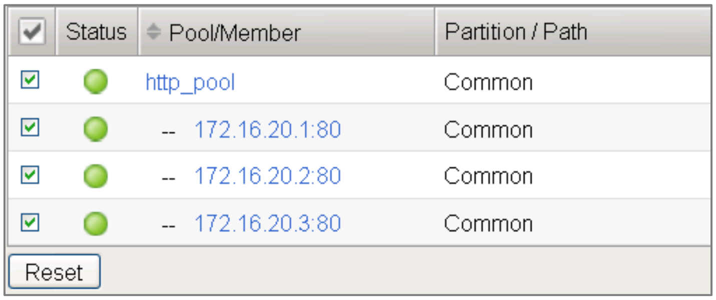
   b. What is the total number of connections made to the pool as a whole, and how does that compare with the total number of connections made to the virtual server?

   c. What is the total number of connections to each pool member? Are the totals roughly the same? Why?

   d. What is the total number of bits sent out from the pool member to the BIG-IP system, and how does that compare with the total bits sent out from the virtual server to the client?

   e. Did each pool member send out the same number of bits? Why?

8. Reset the traffic statistics for the pool by selecting the checkboxes at the left of each pool member entry, then clicking the **Reset** button, as shown below:



☑	Status	Pool/Member	Partition / Path
☑	●	http_pool	Common
☑	●	-- 172.16.20.1:80	Common
☑	●	-- 172.16.20.2:80	Common
☑	●	-- 172.16.20.3:80	Common

Disable a pool member to see how traffic flow is affected

9. Navigate to **Local Traffic > Pools** and select pool **http_pool** to view its configuration.
10. Click on the **Members** tab to view the pool members in this pool.
11. Disable pool member **172.16.20.1:80** by clicking the checkbox to the left of its entry, and then clicking the **Disable** button below. (Its **Status** icon should change from green to black.)
12. On your browser session to the virtual server at **http://10.10.1.100**, hard refresh (Ctrl-F5) the page again several times. You should no longer see any of the page elements being delivered from the disabled pool member.
13. On your BIG-IP system, refresh the pool statistics by clicking the **Refresh** button.
    a. Were any connections load balanced to 172.16.20.1:80?
14. Enable pool member 172.16.20.1:80, and confirm that it is being load balanced to again.

Expected Results

You should see the same amount of traffic going in and out of the virtual server as going in and out of the pool as a whole. You should also see the same total number of connections on both the virtual server and the pool as a whole.

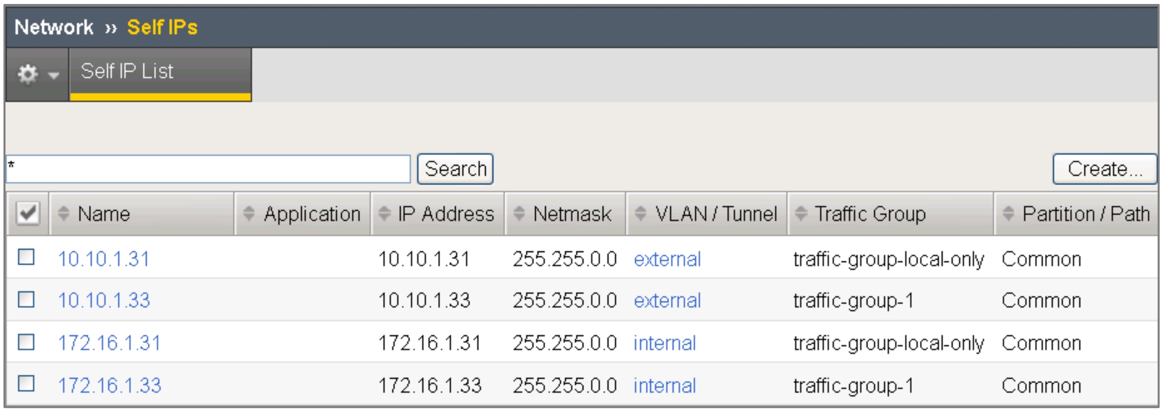
Connections should be roughly evenly distributed between the three pool members, due to the pool's load balancing method, Round Robin.

The amount of traffic processed by each pool member depends on the requests for content that were made to each pool member. Remember, a page is comprised of many elements – HTML, cascading style sheets, images, scripts, etc. Each of these requests may require a separate load balanced connection to the back end server. There is one image on the page – the blue gear image toward the top - that is exceptionally large, and the pool member that served it will almost certainly show more bits out than the other pool members.

Troubleshooting

If the BIG-IP local traffic statistics shows no connections to the virtual server:

- Look at your virtual server's configuration to ensure its destination is set to 10.10.1.100 and its service port is set to 80.
- Try to ping the virtual server from your Ubuntu client's Linux terminal. If you can ping the virtual server successfully, the issue is most likely associated with your BIG-IP configuration. Confirm that your lab environment was properly initialized by viewing the self IPs defined on your BIG-IP system. Navigate to **Network** > **Self IPs**. You should see the following:



☑	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
□	10.10.1.31		10.10.1.31	255.255.0.0	external	traffic-group-local-only	Common
□	10.10.1.33		10.10.1.33	255.255.0.0	external	traffic-group-1	Common
□	172.16.1.31		172.16.1.31	255.255.0.0	internal	traffic-group-local-only	Common
□	172.16.1.33		172.16.1.33	255.255.0.0	internal	traffic-group-1	Common

If statistics show no connections to the pool, look at your virtual server's configuration and ensure that its **Default Pool** setting points to **http_pool**.

You may continue with Lab 2, or end your lab session now.

Lab 2: Solving Routing Issues

This lab corresponds with the activities presented in **Lesson 2** of *Getting Started with BIG-IP: Part 2 – Application Delivery*.

Estimated time for completion: 20 minutes

Lab Objectives

- Solve a common routing issue in a BIG-IP application delivery environment that occurs when a node's default gateway does not pass traffic back through the BIG-IP system.

Lab Requirements

You must have successfully completed the instructions entitled "Starting up the Lab Environment" in the *Getting Started Lab Introduction* document.

Access the BIG-IP System

- Click the **Firefox Web Browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at https://192.168.1.31.)
- Log in to your BIG-IP system as the **admin** user and with password **admin.**

If you completed all of the previous labs in this guide within this same lab session, please skip forward to Step 1 on the next page. Otherwise, please complete the items below to restore the BIG-IP configuration.

Restore the BIG-IP Configuration

1. On your BIG-IP system, navigate to **System** » **Archives**.
2. Click the **BIGIP2_Lab2_SNAT.ucs** file from the list, and then click the **Restore** button.
3. The restore process will take about a minute or two. Please wait until the **Operation Status** message indicates **Saving active configuration…**
4. Then click the **OK** button.

Continue with Step 1 on the next page.

Create and Test the Application Delivery Configuration

Create a load balancing pool

1. Create a Round Robin load balancing pool with three pool members. The default gateway for the nodes associated with these pool members does not pass traffic back through the BIG-IP system. This creates a routing issue for application delivery.

Configuration utility		
Local Traffic » **Pools** » **Pool List**, then click **Create**		
Configuration section		
	Configuration	**Basic**
	Name	**http_pool2**
Resource section:		
	New Members	Address: **172.16.22.1** Service Port **80**, then click **Add** Address: **172.16.22.2** Service Port **80**, then click **Add** Address: **172.16.22.3** Service Port **80**, then click **Add**
When complete, click…		**Finished**

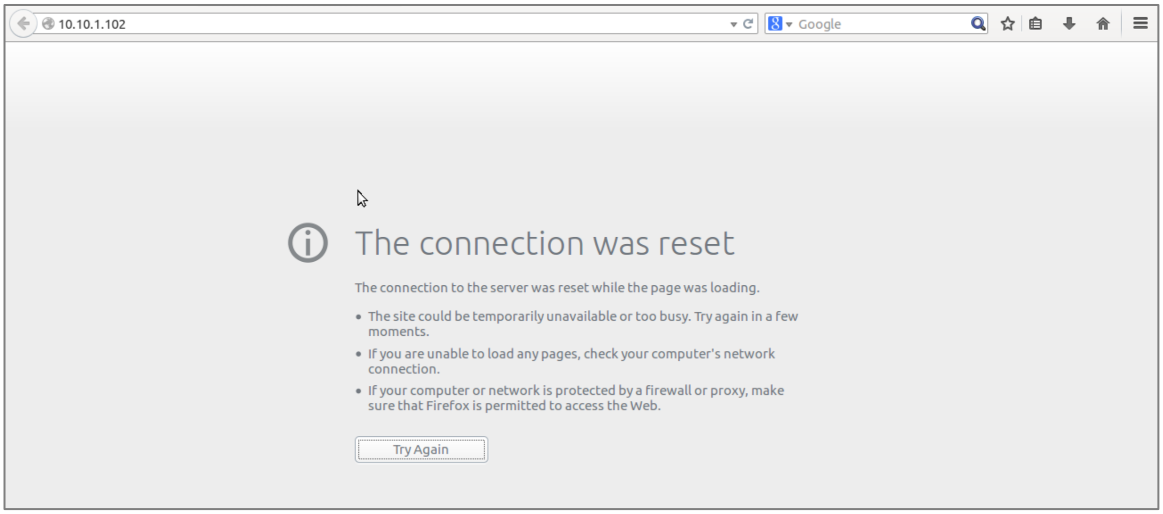
Create a virtual server

2. Create a virtual server at the destination IP address 10.10.1.102 that load balances to http_pool2.

Configuration utility		
Local Traffic » **Virtual Servers** » **Virtual Server List**, then click **Create**		
General Properties section		
	Name	**http_vs2**
	Destination	Address: **10.10.1.102**
	Service Port	**80** (or type or select **HTTP**)
Resources section:		
	Default Pool	**http_pool2**
When complete, click…		**Finished**

Access the virtual server to test application delivery

3. Open a new tab on your Firefox browser, and connect to the virtual server at **http://10.10.1.102**. Your request should fail, and Firefox should produce an error message indicating the connection was reset, similar to below:



The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

4. View statistics and validate that traffic is flowing to the back end servers, but no response is coming back to BIG-IP.

Configuration utility		
Statistics ⏩ Module Statistics ⏩ Local Traffic		
Display Options section		
	Statistics Type	**Virtual Servers**
	Did traffic go into the virtual server?	
	Statistics Type	Change to **Pools**
	Did traffic go into each pool member?	
	Did traffic go out of each pool member?	

Expected Results

- Traffic is coming in to the virtual server, but virtually no traffic is going out, except for the packets required to complete the client-side connection.
- More importantly, traffic is sent to the pool members, but nothing is returned. The server-side TCP connection never completes.

Modify Virtual Server http_vs2

5. Configure Source Address Translation with Auto Map. This setting changes the source address from the client's IP address to the floating self IP on VLAN internal (the egress VLAN). This will cause the server response to go back through the BIG-IP system, rather than through the server's default gateway.

Configuration utility		
Local Traffic » **Virtual Servers**, then click **http_vs2**		
Configuration section		
	Source Address Translation	Select **Auto Map**
When complete, click…	**Update**	

Test Connectivity with SNAT Auto Map

6. Try connecting to **http://10.10.1.102** again. Refresh the screen 5-10 times using Ctrl + F5.
   - What is the client IP address as seen by the pool member?
   - Is traffic going in and out of the pool members?

Expected Results

- You should see traffic going to **and** coming from the pool members

You may continue with Lab 3, or end your lab session now.

Lab 3: Monitoring Application Health

This lab corresponds with the activities presented in **Lesson 3** of *Getting Started with BIG-IP: Part 2 – Application Delivery*.

Estimated time for completion: 20 minutes

Lab Objectives

- Monitor the health of an HTTP web application

Lab Requirements

You must have successfully completed the instructions entitled "Starting up the Lab Environment" in the *Getting Started Lab Introduction* document.

Access the BIG-IP System

- Click the **Firefox Web Browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at https://192.168.1.31.)
- Log in to your BIG-IP system as the **admin** user and with password **admin.**

If you completed all of the previous labs in this guide within this same lab session, please skip forward to Step 1 on the next page. Otherwise, please complete the items below to restore the BIG-IP configuration.

Restore the BIG-IP Configuration

1. On your BIG-IP system, navigate to **System** » **Archives**.
2. Click the **BIGIP2_Lab3_Monitors.ucs** file from the list, and then click the **Restore** button.
3. The restore process will take about a minute or two. Please wait until the **Operation Status** message indicates **Saving active configuration…**
4. Then click the **OK** button.

Continue with Step 1 on the next page.

Create an HTTP Monitor

1. Create a monitor called **My_HTTP** with all defaults as follows:

Configuration utility		
Local Traffic » Monitors » Create		
General Properties section		
	Name	**My_HTTP**
	Type	Select **HTTP**
When complete, click…	**Finished**	

2. Assign **My_HTTP** to **http_pool** using the information in the following table:

Configuration utility		
Local Traffic » Pools : **Pool List**, then select **http_pool**		
Configuration section		
	Health Monitors	Move **My_HTTP** from the **Available** column to the **Active** column.
When complete, click…	**Update**	

3. Notice that the availability of the pool is now **Available (Enabled)**, as indicated by a green circle icon.
4. Click the **Members** tab and verify that the status of each member is Available as indicated by the green circle icon.

Modify My_HTTP Monitor

5. Customize My_HTTP with a Receive string “Server 2”. The receive string “Server 2” only appears on the index page if it’s served from pool member 172.16.20.2:80.

Configuration utility		
Local Traffic » Monitors » My_HTTP		
Configuration section		
	Send String	**GET /index.php\r\n**
	Receive String	**Server 2**
When complete, click…	**Update**	

6. Navigate to **Local Traffic » Pools: Pool List** and click **http_pool**.
7. Click on **Members** tab.
8. Notice that the status changes, and pool members 172.16.20.1 and 172.16.20.3 display a red diamond to indicate they are **Offline (Enabled) –Pool member has been marked down by a monitor**. The pool member 172.16.20.2 displays a green circle to indicate it is **Available (Enabled) – Pool member is available**. If the pool members are all green still, wait 16 seconds and click the **Members** tab again.
9. Navigate to **Local Traffic » Virtual Servers: Virtual Server List** and click **http_vs**. It displays a green circle because all it needs is one pool with one pool member available.
10. Connect to the virtual server at **http://10.10.1.100**. What pool member is serving all the page contents?

Fix the Monitor

Configuration utility		
Local Traffic » Monitors » My_HTTP		
Configuration section		
	Send String	**GET /index.php\r\n**
	Receive String	**Server [1-3]**
When complete, click…	**Update**	

11. Navigate to **Local Traffic » Pools** and click **http_pool**. Click the **Members** tab. What are the pool members’ status now?

Expected Results

- When the receive string was set to “Server 2,” only the pool member 172.16.20.2:80 returned a value that matched. The other two pool members 172.16.20.1:80 and 172.16.20.3:80 returned “Server 1” and “Server 3” respectively. Therefore, they were marked by the monitor as “unavailable” to process traffic after the default timeout value expired.
- After changing the receive string to “Server [1-3], all pool members returned a value that matched. Therefore, you should see all pool members are “Available (Enabled) – Pool member is available” as indicated by the green circle.

You may continue with Lab 4, or end your lab session now.

Lab 4: Modifying Traffic Behavior with Profiles

This lab corresponds with the activities presented in **Lesson 4** of *Getting Started with BIG-IP: Part 2 – Application Delivery*.

Lab Objectives

- Create a Client SSL profile, assign the profile to a virtual server, and observe the change in traffic behavior between the BIG-IP system and the pool member.

Estimated time for completion: 20 minutes

Lab Requirements

You must have successfully completed the instructions entitled "Starting up the Lab Environment" in the *Getting Started Lab Introduction* document.

Access the BIG-IP System

- Click the **Firefox Web Browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at https://192.168.1.31.)
- Log in to your BIG-IP system as the **admin** user and with password **admin.**

If you completed all of the previous labs in this guide within this same lab session, please skip forward to Step 1 on the next page. Otherwise, please complete the items below to restore the BIG-IP configuration.

Restore the BIG-IP Configuration

1. On your BIG-IP system, navigate to **System** » **Archives**.
2. Click the **BIGIP2_Lab4_Profiles.ucs** file from the list, and then click the **Restore** button.
3. The restore process will take about a minute or two. Please wait until the **Operation Status** message indicates **Saving active configuration…**
4. Then click the **OK** button.

Continue with Step 1 on the next page.

Create a Virtual Server and Pool

1. Create a virtual server at the destination address 10.10.1.100 that load balances to a new Round Robin load balancing pool.

Configuration utility	
Local Traffic ▸▸ Virtual Servers : Virtual Server List, then click **Create**	
General Properties section	
Name	**ssl_vs**
Destination	Address: **10.10.1.100**
Service Port	**443** (or type or select **HTTPS**)
Resources section:	
Default Pool	Click + (This opens the **New Pool** screen)
Local Traffic ▸▸ Pools : Pool List ▸▸ New Pool	
New Pool screen Configuration section	
Name	**https_pool**
Resources section (on **New Pool** screen)	
New Members	Address: **172.16.20.1** Service Port: **443** Click **Add** Address: **172.16.20.2** Service Port: **443** Click **Add** Address: **172.16.20.3** Service Port: **443** Click **Add**
When complete, click…	**Finished** (This will return you to the **New Virtual Server** screen)
Local Traffic ▸▸ Virtual Servers: Virtual Server List ▸▸ New Virtual Server…	
Resources section (back on the **New Virtual Server** screen)	
Default Pool	**https_pool**
When complete, click…	**Finished**

2. Test connection to the virtual server by opening a web browser session to **https://10.10.1.100.**
3. If using Firefox, click **I Understand the Risks**. Click **Add Exception**. Click to deselect the check next to **Permanently store this exception**. Click **Confirm Security Exception**.
4. You should see a Web page similar to those in the previous labs, with the exception of a red background. The red background indicates that the content is encrypted, given that it is served from port 443.

Generate a Certificate

In a production BIG-IP environment, you would almost certainly import and install a certificate from a trusted Certificate Authority to use in conjunction with your Client SSL profile. In our lab environment, we'll mimic this behavior but create and test with a self-signed certificate instead.

5. Create a new self-signed certificate called **TestCertificate**.

Configuration utility		
System » **Certificate Management: Traffic Certificate Management**: **SSL Certificate List** and click **Create**		
General Properties section		
	Name	**TestCertificate**
Certificate Properties section		
	Issuer	**Self**
	Common Name	**www.testsite.com**
	Division	**Training**
	Organization	**F5 Networks**
	Locality	**Seattle**
	State or Province	**Washington**
	Country	**United States**
Key Properties section		
	Size	**2048** bits
When complete, click…	**Finished**	

Create an SSL Client Profile

6. Create a Client SSL profile called **Pr_Client_SSL** with **clientssl** as its parent.

Configuration Utility		
Local Traffic » **Profiles** » **SSL** » **Client** and click **Create**		
General Properties section		
	Name	**Pr_Client_SSL**
	Parent Profile	**clientssl**
Configuration section		
	Certificate Key Chain	**Check** the **Custom** check box to the far right. Click **Add** Certificate: **TestCertificate** Key: **TestCertificate** Click **Add** button
When complete, click…	**Finished**	

Assign a Client SSL profile to ssl_vs

7. Assign the **Pr_Client_SSL** profile to virtual server **ssl_vs**.

Configuration utility		
Local Traffic » **Virtual Servers** : **Virtual Server List**, then select **ssl_vs**		
Configuration section		
	SSL Profile (Client)	**Pr_Client_SSL**
When complete, click…	**Update**	

This will cause BIG-IP to terminate SSL encryption inside BIG-IP and send traffic over the server side connection unencrypted.

8. Connect by opening a browser session to **https://10.10.1.100**. Refresh the screen using **Ctrl + F5** to force the browser not to use its cache.
9. If using Firefox, click **I Understand the Risks**. Click **Add Exception**. Click to **deselect** the check next to **Permanently store this exception**. Click **Confirm Security Exception**.

Expected Results

A **Bad Request** response is displayed. The reason is BIG-IP negotiates the cert and key exchange, but our app breaks because we're load balancing to a pool that is expecting encrypted traffic.

Fix Load Balancing Pool

10. Change default pool on **ssl_vs** to use pool **http_pool,** which uses port 80. Navigate to **Local Traffic » Virtual Servers: Virtual Server List: ssl_vs**. Click the **Resources** tab. Change the **Default Pool** to **http_pool** and click **Update**.

Since we’re sending unencrypted traffic across server side connection, we can load balance to a pool of servers that is not expecting encrypted traffic.

11. Connect again to **https://10.10.1.100** and you will see a blue background.

Expected Results

After changing the default pool to **http_pool**, you should see the output being served from **port 80** even though you connected to a **port 443** virtual server.

STOP

You have completed the labs associated with this WBT. Please terminate your lab session now.