F5 Networks Training

BIG-IP® LTM V11 Essentials

Web-Based Training Lab Guide

2015-02-12

BIG-IP LTM V11 Essentials

Lab Guide

Seventh Printing

This manual was written for BIG-IP® version 11.6.0.

Support and Contact Information

Obtaining Technical Support

Frequently Asked Questions	see FAQ in Lab email or \Shared directory
Email lab support	WBTsupport@f5.com
Email F5 University support	f5University@f5.com
Email Partner support	partners@f5.com
Email Professional Certification	F5Certification@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

3DNS; AAM; Access Policy Manager; Acopia; Acopia Networks; Advanced Client Authentication; Advanced Routing; AFM; APM; Application Acceleration Manager; Application Cloud Services; Application Security Manager; Application Services Controller; ARX; AskF5; ASM; BIG-IP; BIG-IP EDGE GATEWAY; BIG-IQ; COHESION; Cloud Extender; CloudFucious; Clustered Multiprocessing; CMP; Data Manager; DDoS Frontline; DDoS SWAT; Defence.net; DevCentral; DevCentral [DESIGN]; DSC; DNS Express; DSI; Edge Client; Edge Gateway; Edge Portal; ELEVATE; EM; Enterprise Manager; F5; F5 [DESIGN]; F5 Management Pack; F5 Networks; F5 Synthesis; Fast Application Proxy; Fast Cache; FirePass; Global Traffic Manager; GTM; GUARDIAN; iApps; IBR; iCall; iControl; Intelligent Browser Referencing; Intelligent Compression; IPv6 Gateway; iQuery; iRules; iRules OnDemand; iSession; L7 Rate Shaping; LC; LineRate Operating System; LineRate; Link Controller; Local Traffic Manager; LTM; LROS; Message Security Manager; MSM; NetCelera; OneConnect; Packet Velocity; PEM; Protocol Enforcement Manager; Protocol Security Manager; PSM; Real Traffic Policy Builder; SalesXchange; F5 Sales Exchange; ScaleN; SDAS; SDC; Signaling Delivery Controller; Solutions for an application world; SSL Acceleration; StrongBox; SuperVIP; SYN Check; TCP Express; TDR; TechXchange; TMOS; TotALL; Traffic Management Operating System; TrafficShield; Traffix; Transparent Data Reduction; UNITY; VAULT; vCMP; Versafe; VIPRION; Virtual Clustered Multiprocessing; WA; WAN Optimization Manager; WANJet; WebAccelerator; WOM; 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 U.S. Patents: 6,311,278; 6,327,242; 6,374,300; 6,405,219; 6,473,802; 6,505,230; 6,640,240; 6,772,203; 6,970,933; 6,889,249; 7,047,301; 7,051,126; 7,102,996; 7,113,962; 7,114,180; 7,126,955; 7,146,354; 7,197,661; 7,206,282; 7,286,476; 7,287,084; 7,296,145; 7,296,263; 7,308,475; 7,343,413; 7,346,695; 7,349,391; 7,355,977; 7,376,967; 7,383,288; 7,395,349; 7,409,440; 7,409,460; 7,430,755; 7,441,045; 7,461,290; 7,472,413; 7,487,253; 7,490,162; 7,493,383; 7,505,455; 7,509,322; 7,512,673; 7,552,191; 7,558,848; 7,562,110; 7,567,573; 7,580,353; 7,590,625;

7,606,912; 7,639,700; 7,640,347; 7,640,580; 7,650,392; 7,657,618; 7,676,828; 7,697,427; 7,702,809; 7,705,829; 7,707,182; 7,707,287; 7,707,289; 7,710,867; 7,752,400; 7,768,823; 7,774,484; 7,774,835; 7,783,781; 7,788,335; 7,822,839; 7,826,487; 7,831,712; 7,882,084; 7,916,728; 7,916,730; 7,921,282; 7,945,678; 7,953,838; 7,958,222; 7,958,347; 7,975,025 7,996,886; 8,004,971; 8,005,953; 8,010,668; 8,015,314; 8,024,443; 8,024,483; 8,103,746; 8,103,770; 8,103,809; 8,108,554; 8,112,491; 8,116,222; 8,117,244; 8,121,117; 8,145,768; 8,150,957; 8,159,940; 8,176,164; 8,180,747; 8,185,617; 8,189,476; 8,195,760; 8,195,769; 8,200,957; 8,203,949; 8,204,860; 8,204,930; 8.209,403; 8,239,354; 8,260,958; 8,261,351; 8,275,909; 8,284,657; 8,301,837; 8,306,036; 8,306,038; 8,326,923; 8,326,984; 8,341,296; 8,345,701; 8,346,993; 8,347,100; 8,352,597; 8,352,785; 8,375,421; 8,379,515; 8,380,854; 8,392,372; 8,392,563; 8,396,836; 8,396,895; 8,397,059; 8,400,919; 8,407,771; 8,412,582; 8,417,681; 8,417,746; 8,417,833; 8,418,233; 8,429,783; 8,432,791; 8,432,799; 8,433,735; 8,438,253; 8,447,871; 8,447,883; 8,447,884; 8,453,120; 8,463,850; 8,463,909; 8,477,609; 8,477,798; 8,484,361; 8,499,100; 8,516,113; 8,516,156; 8,533,254; 8,533,308; 8,533,662; 8,537,825; 8,539,062; 8,548,953; 8,549,582; 8,554,999; 8,559,313; 8,560,709; 8,565,088; 8,566,444; 8,566,452; 8,572,219; 8,611,222; 8,612,374; 8,613,045; 8,615,010; 8,621,078; 8,627,467; 8,630,174; 8,645,556; 8,650,389; 8,670,304; 8,676,955; 8,681,610; 8,682,916; 8,700,892; 8,711,689; 8,713,197; 8,738,700.

Other patents may be pending. This patent list is complete as of 1 Oct 2014.

Disclaimer

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.

Table of Contents

Chapter 0: Lab Introduction

What you Need to Know

Introduction

Welcome to the BIG-IP LTM Essentials Web-Based Training Course Lab Guide. The purpose of the BIG-IP LTM Essentials course is to introduce the basic information that you need to know to set up and operate the BIG-IP Local Traffic Manager (LTM). The purpose of this lab guide is to provide all of the information and exercises you need to work directly with a BIG-IP LTM system, and to solidify the concepts you have learned in the associated Web-based training modules.

The hands-on lab exercises included in this course are critically important to your learning. These exercises are especially helpful if you can do them as soon as possible after completing the associated training module. Therefore, we recommend the following approach: after completing the training module, do the lab exercises. Be sure to complete all of the exercises, including the review questions at the end.

There are eleven lecture modules in this course, each one taking approximately thirty minutes to complete. Nine of the lecture topics have labs. To complete the entire course, including modules and labs, will take you about fourteen hours.

In addition to the lab exercises, this guide has an appendix that shows you how to configure high availability in BIG-IP version 11.

We hope you enjoy learning with these lab exercises!

Connecting to the F5 Training Lab Environment

PLEASE NOTE: This lab is intended solely for instructional purposes and not as a test environment. It is strictly for use by students taking the BIG-IP LTM Essentials Web-based training (WBT) course. Each lab session is available for two hours. If you exceed the two hour time limit, the lab environment will stop responding. If this happens, log out of the lab environment and then create a new lab.

There are two methods of accessing the F5 Virtual Lab hosted on Skytap.

1. HTML5 Client < Preferred
2. Java SmartClient

Minimum Requirements

HTML5 Client Only (preferred for best user experience)

The HTML5 Client requires a modern web browser that supports Websocket technology. Supported browsers include:

- Google Chrome 31+
- Mozilla Firefox 31+
- Apple Safari 7+
- Microsoft Internet Explorer 10+

Internet Explorer 8 and Internet Explorer 9 users **will be unable to access** the HTML5 client.

*Skytap does not support Internet Explorer in Compatibility View. Compatibility View will operate like an older, unsupported browser. For more information about turning Compatibility View on and off, see http://windows.microsoft.com/en-us/internet-explorer/use-compatibility-view#ie=ie-11.

Java SmartClient Only

The Java SmartClient requires the latest version of Apple Java 1.6, Oracle Java 1.7, or Oracle Java 1.8.

- If you are unsure which version of Java you are running, simply click the following link and it will auto-detect your Java version: http://java.com/en/download/installed.jsp
- If you are running OS X, please see Running Java on Mac OS X.
- For information on installing Java on your local Linux machine, see Installing Java on a Local Linux Machine.

Operating Systems

You can access Skytap Cloud using any operating system that supports one or more of the browsers listed above. This includes most Microsoft Windows variants, Apple OS X, and most major Linux distributions.

For a complete list see: Skytap SmartClient Minimum Requirements

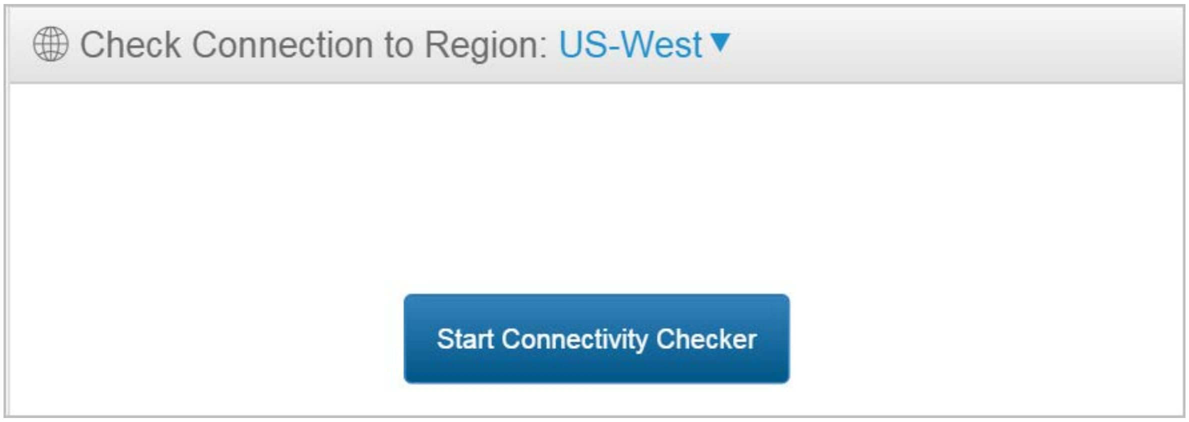
Run the Connectivity Checker

The Connectivity Checker will verify that you meet the browser and minimum connection speed requirements needed to access virtual machines using the HTML5 client. If you do not meet the requirements for the HTML5 Client, you can run the Connectivity Checker for the Java SmartClient.

The HTML 5 Connectivity Checker can be found here: https://cloud.skytap.com/connectivity.

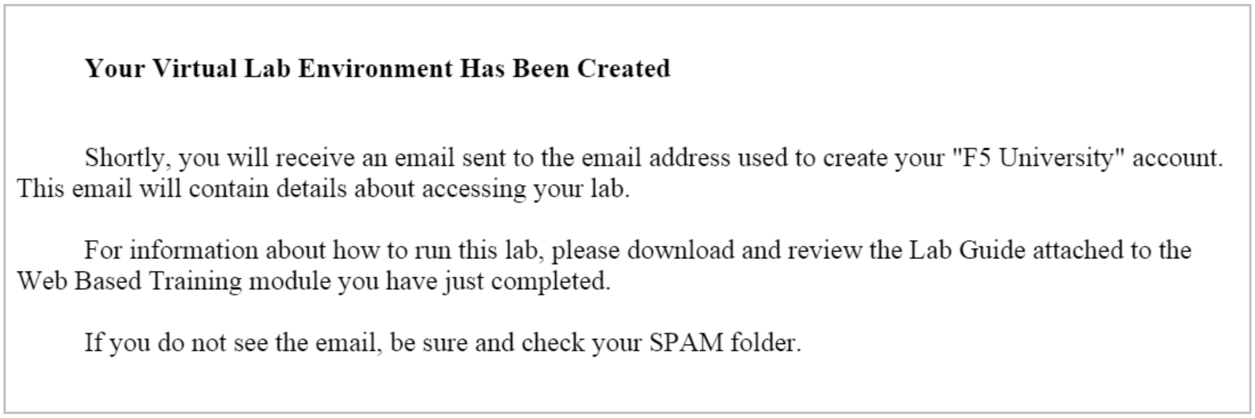
The Java Connectivity Checker can be found here: https://cloud.skytap.com/tools/connectivity

Click the drop down and select the US-West region. Please note, currently all F5 labs are ONLY hosted in the US-West region.


Check Connection to Region: US-West ▼
Start Connectivity Checker

How to Create a Lab Environment

1. Log in to F5 University.
2. Click the **F5 Training Lab** link on the top right.
3. On the F5 Training Lab screen, click the **BIG-IP v.11** tab.
4. Click the link to run the connectivity checker.
5. From the Check Connection to Region menu, select US-WEST.
6. Click **Start Connectivity Checker**.
7. Wait for the test to complete.
8. On the F5 Training Lab screen, click **Create a Lab Session. <=Click Only Once** and please wait patiently for 3 to 5 minutes.
9. After a short time, you should see the following message:



Your Virtual Lab Environment Has Been Created

Shortly, you will receive an email sent to the email address used to create your "F5 University" account. This email will contain details about accessing your lab.

For information about how to run this lab, please download and review the Lab Guide attached to the Web Based Training module you have just completed.

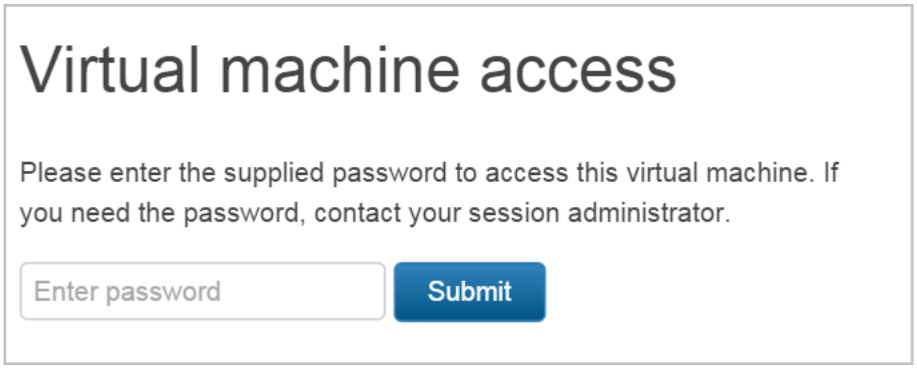
If you do not see the email, be sure and check your SPAM folder.

10. After a short time, you should receive an e-mail message from F5 Virtual Labs with the subject line “F5 University Lab is Available.”

    If you do not see the e-mail message in your Inbox, check your “Junk E-Mail” folder.

11. Copy the password from the e-mail message.
12. Click **Connect to your lab environment** in the e-mail message.

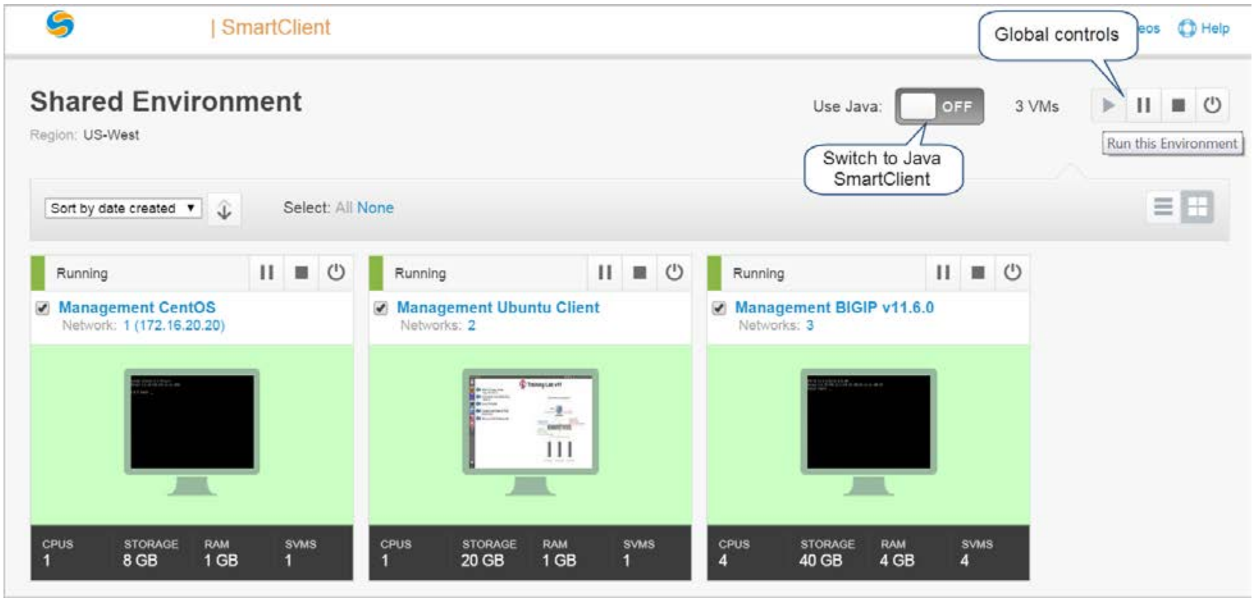
13. Paste your password into the page where indicated and then click **Submit**.



Virtual machine access

Please enter the supplied password to access this virtual machine. If you need the password, contact your session administrator.

14. The SmartClient should open in the “Running” state. If it does not, be patient. Depending on system usage, the lab status can take from 2 to 5 minutes to change from “Busy” to “Running.” If your machines fail to start, use the global control in the top right corner of your screen to start them simultaneously.



Shared Environment

Region: US-West

Use Java: OFF

3 VMs

Sort by date created ▼

Select: All None

Running

☑ Management CentOS

Network: 1 (172.16.20.20)

CPUS	STORAGE	RAM	SVMS
1	8 GB	1 GB	1

Running

☑ Management Ubuntu Client

Networks: 2

CPUS	STORAGE	RAM	SVMS
1	20 GB	1 GB	1

Running

☑ Management BIGIP v11.6.0

Networks: 3

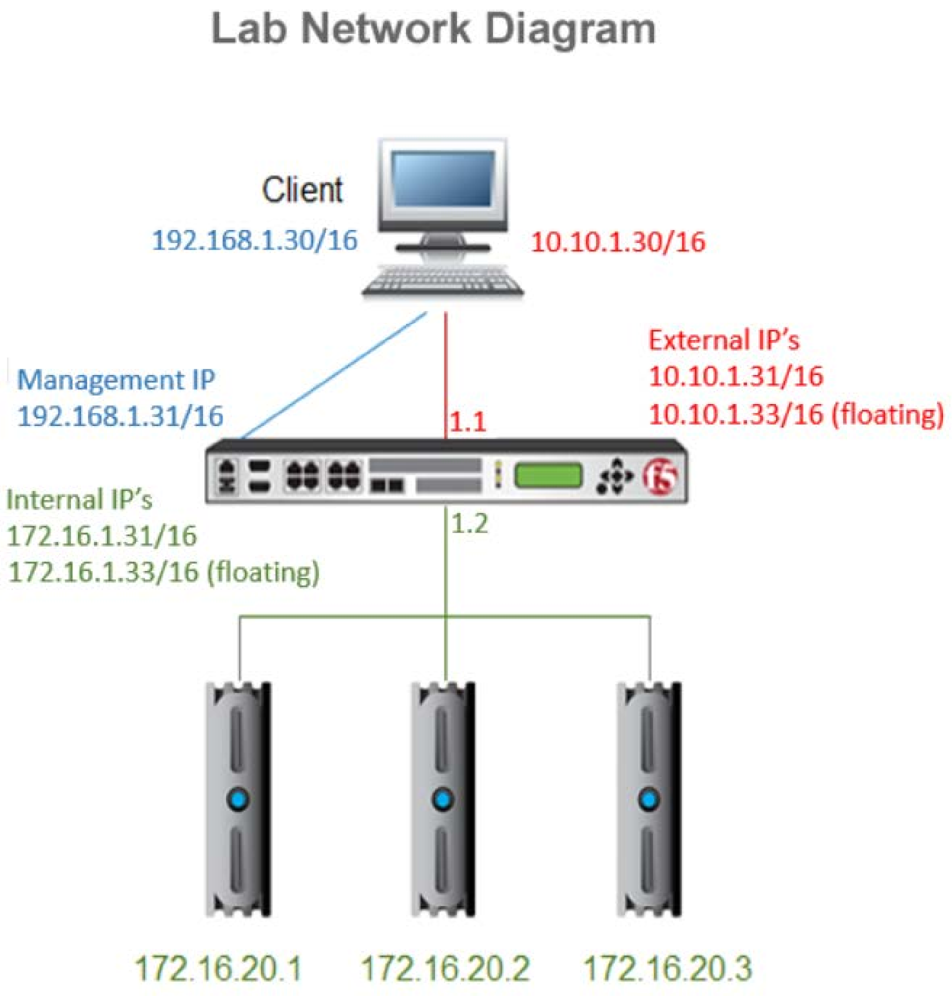
CPUS	STORAGE	RAM	SVMS
4	40 GB	4 GB	4

15. Click **Management Ubuntu Client** screen to begin your lab.

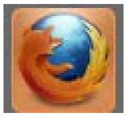
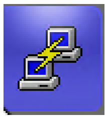
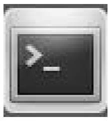
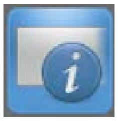
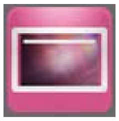
Lab Login and Password Information

Account	Login	Password
Linux “Ubuntu” operating system	student	student
BIG-IP Configuration Utility (GUI)	admin	admin
Command Line Interface (CLI)	root	default
Centos (back-end) server	student	student

Navigation Tips



Management Ubuntu Client Icon Legend

	To access the BIG-IP Management IP address, click the **Firefox** web browser icon. This launches the Configuration Utility (sometimes called the “GUI”), which is the main method that you will use to manage BIG-IP in this course.
	To access the BIG-IP command line interface (sometimes called the “CLI”), click the **PuTTY SSH Client** icon.
	To access the Ubuntu Client’s Linux terminal click the **Terminal** icon. If needed, use the terminal to ping the other devices in the network to ensure connectivity.
	To access this Lab Guide and the FAQ, click the **Manuals** icon.
	To return to the Desktop and see the Informational graphic click this **Show Desktop** icon. Clicking it again will return you to your application(s).

You can switch between applications like Firefox and PuTTy by clicking the icons for the applications.

Lab Session Time Limit

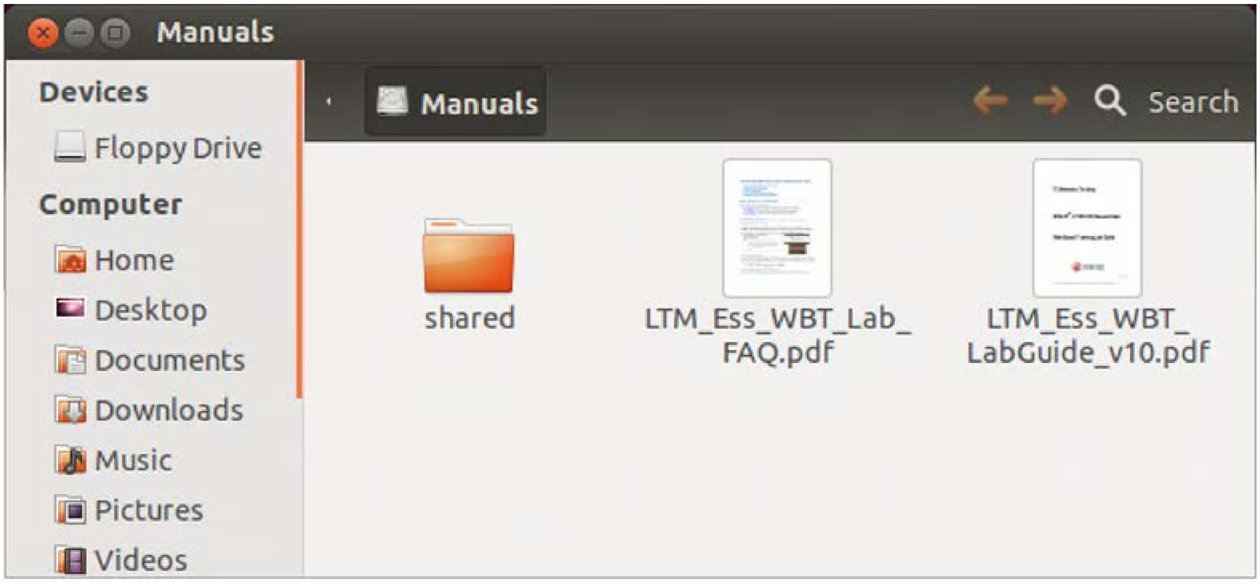
Important to note, your lab session will only be alive for 2-hours. At the end of the 2 hours, it will auto shutdown and auto-delete. To continue working you will have to create a new lab. Remember, each lab chapter can be started by loading the appropriate .ucs archive.

Getting the latest Lab Guide and FAQ

To get the latest version of this lab guide and the Frequently Asked Questions (FAQ) from the shared folder:

1. Click the **Manuals** icon.

   Here you will find the Lab FAQ and the Lab Guide.



How Lab Instructions Are Formatted

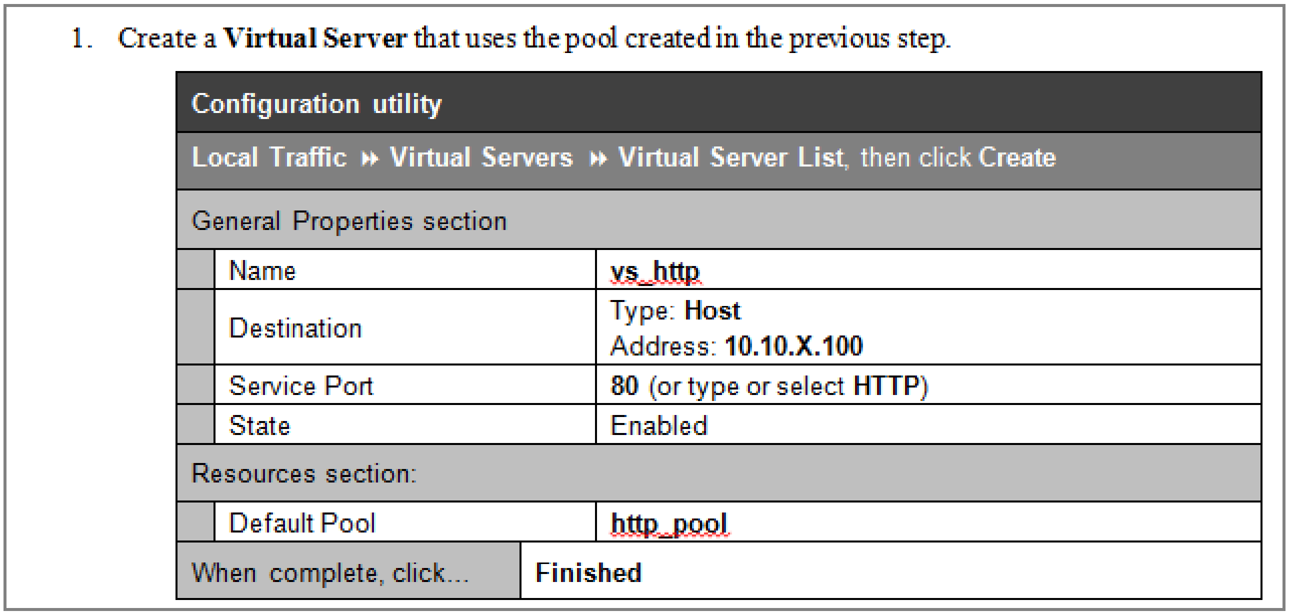
Detailed lab instructions for use at the beginning

Whenever browser-based tools are used, such as the Configuration utility, a tabular format is used to illustrate what tool is being used (e.g. **Configuration utility**, **Setup utility**), where to navigate within the tool (e.g. **Local Traffic** » **Virtual Servers** » **Virtual Server List**), and what information goes into what fields, what selection to make from a pull-down menu, or what button to click. The example below shows how instructions are formatted in this lab guide.

First, it shows how to navigate in and use the configuration utility (from **Local Traffic** to **Virtual Servers** to the **Virtual Server List**, and that you then click the **Create** button).

It also shows the fields that need to be filled in (for example, **Name**) and the value to enter in that field (**vs_http**).

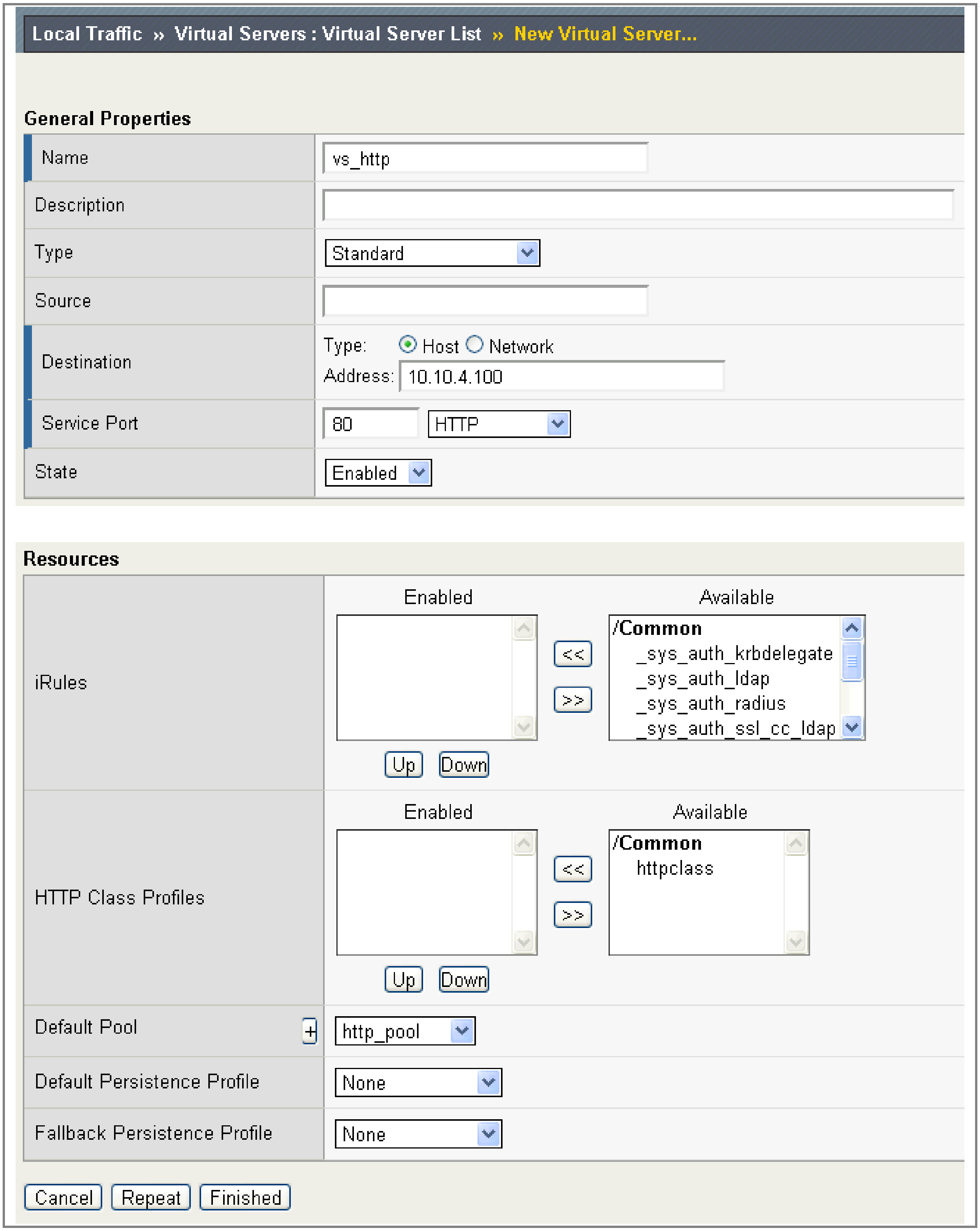
Finally, it tells you that when you have completed making the settings shown, you should click **Finish**.



1. Create a **Virtual Server** that uses the pool created in the previous step.

Configuration utility	
Local Traffic ⏩ **Virtual Servers** ⏩ **Virtual Server List**, then click **Create**	
General Properties section	
Name	**vs_http**
Destination	Type: **Host** Address: **10.10.X.100**
Service Port	**80** (or type or select **HTTP**)
State	Enabled
Resources section:	
Default Pool	**http_pool**
When complete, click…	**Finished**

Figure 1: Sample lab instructions



Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	vs_http
Description	
Type	Standard
Source	
Destination	Type: ● Host ○ Network Address: 10.10.4.100
Service Port	80 HTTP
State	Enabled

Resources

iRules	Enabled: (none) Available: /Common _sys_auth_krbdelegate, _sys_auth_ldap, _sys_auth_radius, _sys_auth_ssl_cc_ldap
HTTP Class Profiles	Enabled: (none) Available: /Common httpclass
Default Pool	http_pool
Default Persistence Profile	None
Fallback Persistence Profile	None

Figure 2: Lab steps executed on the Configuration utility page

Shorter lab instructions for use as you become more proficient

As you become proficient with BIG-IP, the level of detail provided in the lab instructions decreases.

For example, in the Configuration Lab Project, you'll be asked to create a monitor using the following information:

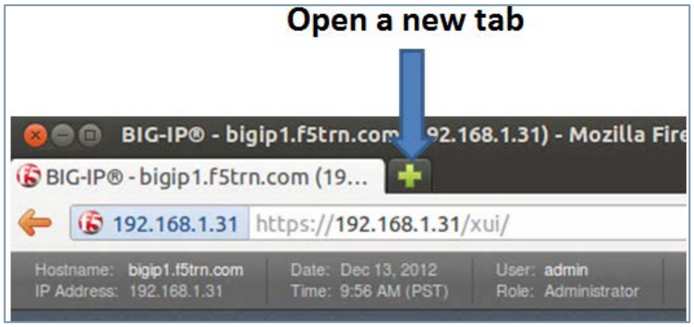
Name	Type	Settings	Associations
my_http	http	Interval – 5, Timeout – 16 Receive String – Server Others – leave at defaults	http_pool (After pool is created, below.)

The table here contains all the information you need to configure the objects needed for use during the lab. If you forget where to navigate to or what to do once you get there, please refer back to earlier labs for step-by-step instructions.

Accessing Backend Servers through a Virtual Server

In this lab guide, you will often be instructed to open a new browser session to access a particular virtual server (for example at http://10.10.1.100).

To do this, in the Firefox browser, click the **+** icon to open a new tab as indicated below:

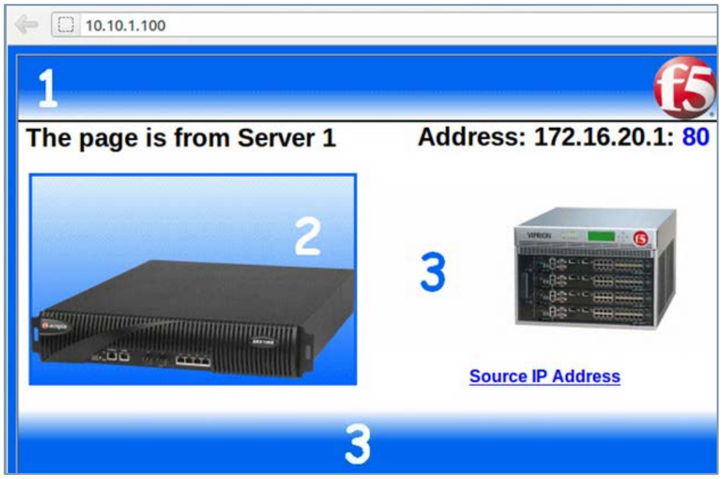


Open a new tab

BIG-IP® - bigip1.f5trn.com (192.168.1.31) - Mozilla Fire

Hostname: bigip1.f5trn.com
IP Address: 192.168.1.31
Date: Dec 13, 2012
Time: 9:56 AM (PST)
User: admin
Role: Administrator

In the browser, type **http://10.10.1.100** and enter. You should see a web page similar to:

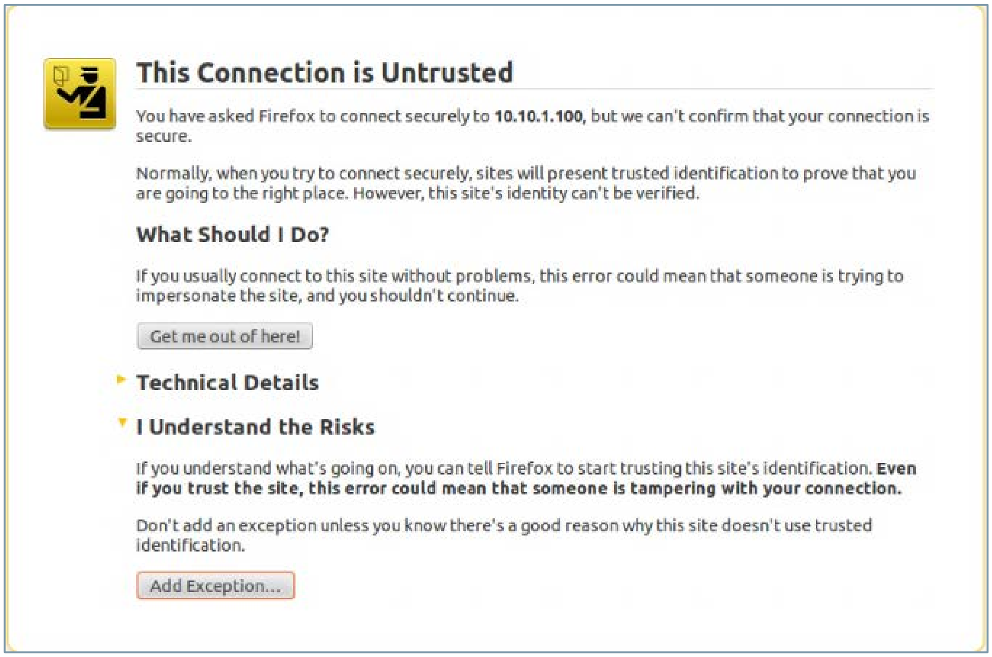


The page is from Server 1

Address: 172.16.20.1: 80

The blue theme indicates this content was accessed via HTTP versus HTTPS.

Additionally, you will access https://10.10.1.100. Because it is a secure connection, you will be prompted to accept a security exception:



This Connection is Untrusted

You have asked Firefox to connect securely to **10.10.1.100**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

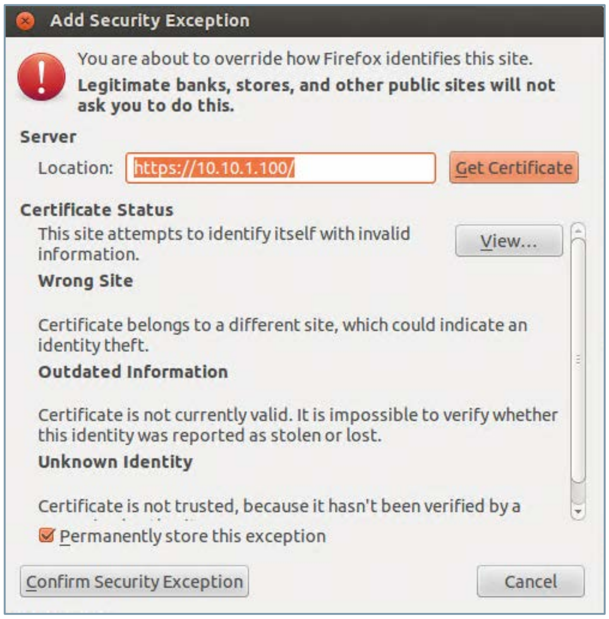
Technical Details

I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Next you will be prompted to confirm the security exception:



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.10.1.100/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

Outdated Information

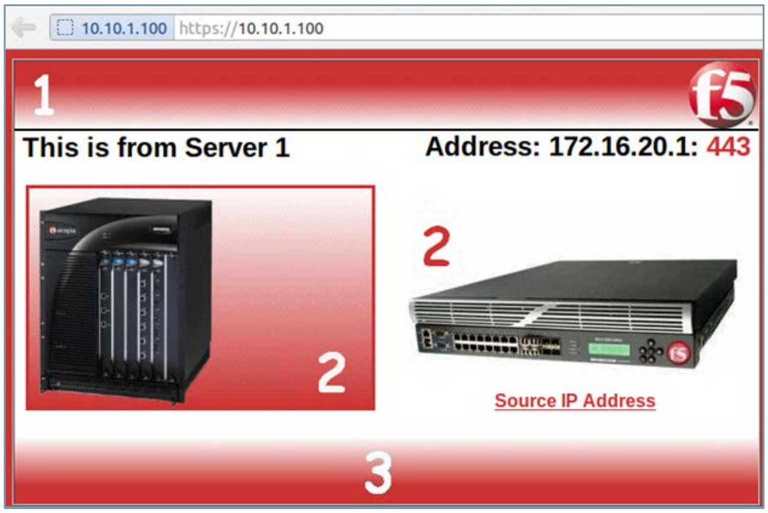
Certificate is not currently valid. It is impossible to verify whether this identity was reported as stolen or lost.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a

☑ Permanently store this exception

After confirming the security exception, you will see a Web page similar to:



10.10.1.100 https://10.10.1.100

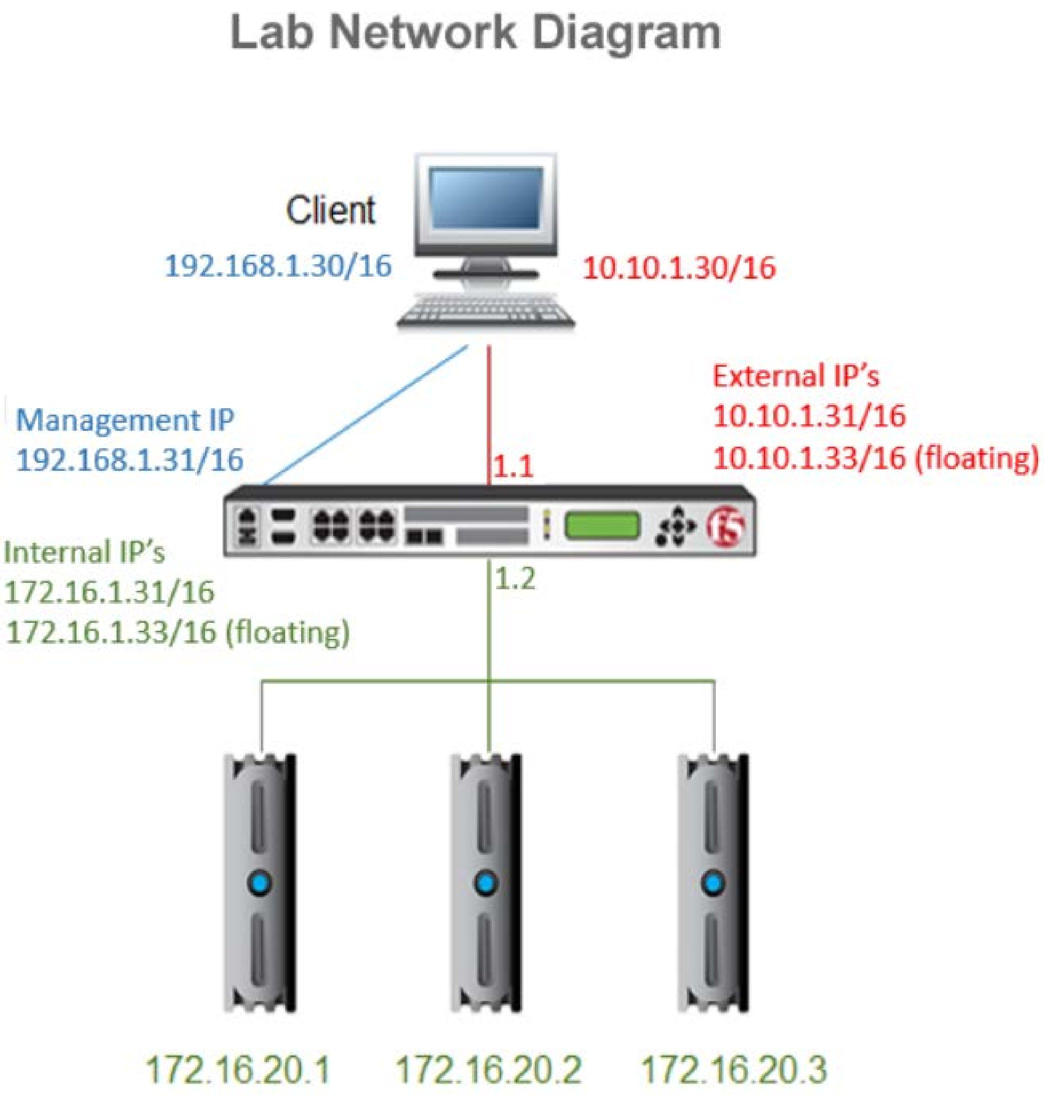
This is from Server 1

Address: 172.16.20.1: 443

The red theme indicates this is content is being accessed via secure HTTPS.

The F5 Training Lab Network

- You will be connected to a Linux Ubuntu client desktop that you can use to administer your BIG-IP LTM device and act as the client to drive traffic through your BIG-IP device.
- Your Ubuntu client has two IP addresses (192.168.1.30/16 and a 10.10.1.30/16) configured for the lab network shown below.
- The Management IP address of your BIG-IP device is already set to 192.168.1.31/16. You will set the other 10.10.0.0/16 External and 172.16.0.0/16 Internal IP addresses in Lab 1.
- There are also three origin Web servers configured at 172.16.20.1, 172.16.20.2 and 172.16.20.3. These are the servers to which we will load balance traffic starting in Lab 2. You cannot access these servers directly from your Ubuntu client. .



F5 Training Lab Limitations

- The F5 Training Lab is a virtual lab environment and therefore does not have all features of a hardware BIG-IP system available. For instance, you will not have a serial console connection to your BIG-IP.
- This lab environment supports only BIG-IP LTM. No other F5 products or BIG-IP modules (such as APM or ASM) are supported.
- This lab environment has only been tested with the lab steps in this lab guide. If you do not follow the steps in this lab guide, results will vary.

General Information

- Each lab starts with a BIG-IP device that has not been configured and instructs you to restore a UCS backup file that was captured at the end of the previous lab.
- You can only enter the F5 Training Lab environment from the links within F5 University.
- You can exit from the lab at any time by closing the browser page.
- The lab environment is available for two hours. After that the lab becomes inoperative and all of your configuration changes are lost. To continue after two hours you must create a new lab.

Chapter 1: Initial Setup

Module 1 – Introduction

Some information about the BIG-IP device in your lab environment.

This device is already installed, licensed, provisioned, and has a single management IP address applied to it so you can easily access the device via a web browser interface.

The objectives of this Initial Setup Lab is to walk you through all the other initial ‘setup utility’ configurations that have not been completed. You do **not** have to do this lab. Each lab can be initiated by first loading a pre-configured BIG-IP archive. The beginning of every lab has brief instructions on how to load the appropriate archive.

If you are new to the BIG-IP LTM you are encouraged to proceed through the labs sequentially.

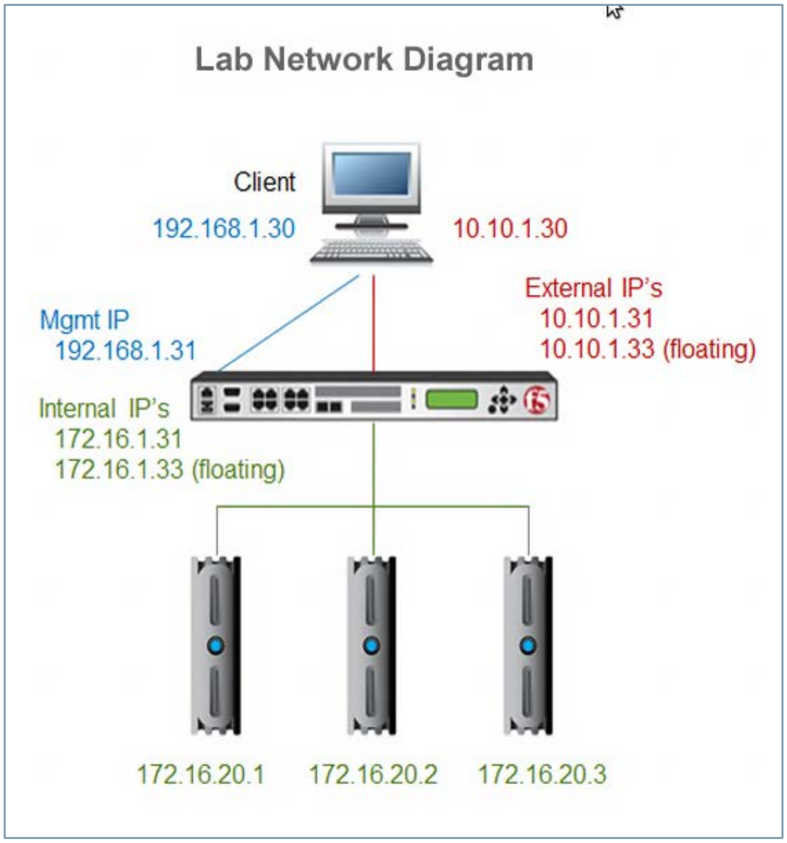
Module 1 Lab – Initial Setup and Access

Initial Setup Labs

Objective:

- Perform initial setup of the BIG-IP LTM System
- Explore the Web Configuration Utility
- Make a backup of the BIG-IP System

Estimated Time: 30 minutes



LAB CONFIGURATION

Setup Utility Lab

Objective:

- Run the Setup utility and configure system access parameters
- Estimated time for completion: 20 minutes

Lab Requirements:

- Valid IP address on the management port of the BIG-IP LTM device
- Valid license for the BIG-IP LTM systems
- Administration system with an IP address on the network of the BIG-IP LTM device

Current BIG-IP Settings

At this point, your BIG-IP system is licensed and the management address is already set to **192.168.1.31/16**.

Computer Configuration

Your virtual computer (Linux Ubuntu client) is configured with two IP addresses so that it can reach both the Management and client (External) networks.

IP address on Management network	**192.168.1.30 / 16**
IP address on External network	**10.10.1.30 / 16**

Access the BIG-IP LTM System

1. On the Skytap Cloud SmartClient Web page click **Ubuntu Client**.
2. Click the **Firefox Web Browser** icon. When prompted, log in with a username of **admin** and with a password of **admin.**

Run the Setup utility

1. For these labs, the systems should already be licensed and provisioned for Local Traffic Manager. (Normally, you would need to license and provision a new BIG-IP System.)
2. Typically, the Setup utility would run automatically on a new BIG-IP system.

   In our lab environment, click the F5 red logo in the upper left corner: .
3. Scroll down to the **Setup utility** section, then click **Run the Setup Utility**.
4. Review the features that have been licensed. Click **Next**.

Verify Provisioning

5. On the next screen, verify that provisioning for **Local Traffic (LTM)** is set to **Nominal**. All other products are set to **None, Disabled,** or **Small**. Click **Next**.

Accept the BIG-IP Self-Signed Device Certificate

6. On the next page, note the certificate properties, including the Expires date, and click the **Next** button to continue.

Verify Setup

7. In the **General Properties** section of the next page, verify host name, time zone, and administrative access usernames and passwords settings. Click **Next**. NOTE: You will be logged out and have to log back in at this point.

Setup utility		
General Properties section		
	Management Port Configuration	**Manual**
	Host Name	**bigip1.f5trn.com**
	Host IP address	Use Management Port IP address
	Time Zone	America/Los Angeles
User Administration section		
	Root Account	Password: **default** Confirm: **default**
	Admin Account	Password: **admin** Confirm: **admin**
	SSH Access	Enabled
	SSH IP Allow	* All Addresses
When complete, click	**Next**	

8. In the **Standard Network Configuration** section, click **Next**.

Next the configuration wizard guides you through the steps required to create two VLANs (named Internal and External) and to configure their IP addresses and interfaces.

Most steps below take the default Redundant Device Options, and therefore, settings like Mirroring and Floating Self IP addresses are configured. These concepts are discussed later in the course in the Redundant Pair Setup and High Availability modules.

10. Under **Redundant Device Wizard Options**, verify that:
    - **Display configuration synchronization options** is selected (checkbox is checked).
    - **Display failover and mirroring options** is selected (checkbox is checked).
    - **Failover Method** is set to **Network.**

    Click **Next**.

Configure Self IPs, VLANs, and High Availability

11. Configure the internal network and VLAN by making the following settings:

Setup utility		
Internal Network Configuration section		
	Self IP	Address: **172.16.1.31** Netmask: **255.255.0.0** Port Lockdown: **Allow Default**
	Floating IP	Address: **172.16.1.33** Port Lockdown: **Allow Default**
Internal VLAN Configuration section		
	VLAN Name	internal
	VLAN Tag ID	**auto**
	VLAN Interfaces	Select VLAN interface **1.2** and add it **Untagged** to the Interfaces list.
When complete, click…	**Next**	

12. Next, configure the external network and VLAN by making the following settings:

Setup utility		
External Network Configuration section		
	External VLAN	**Create VLAN external** radio button selected
	Self IP	Address: **10.10.1.31** Netmask: **255.255.0.0** Port Lockdown: **Allow 443** Default Gateway**: Leave blank**
	Default Gateway	Leave Blank
	Floating IP	Address: **10.10.1.33** Port Lockdown: **Allow 443**
External VLAN Configuration section		
	VLAN Name	external
	VLAN Tag ID	**auto**
	VLAN Interfaces	Select VLAN interface **1.1** and add it **Untagged** to the Interfaces list.
When complete, click…	**Next**	

13. Configure the high availability network to use the existing VLAN, **internal**, by making the following settings:

Setup utility		
High Availability Network Configuration section		
	High Availability VLAN	Click the **Select existing VLAN** radio button
	Select VLAN	**internal**
	Self IP	Address: **172.16.1.31** Netmask: **255.255.0.0**
High Availability VLAN Configuration section		
	VLAN Name	internal
	VLAN Tag ID	**auto**
	VLAN Interfaces	**1.2** (untagged)
When complete, click…	**Next**	

Configure Network Time Protocol

14. Leave this blank and click **Next**

Configure Domain Name Server

15. Leave this blank and click **Next**

Configure ConfigSync

16. Configure ConfigSync on the non-floating self IP for internal VLAN by making the following settings:

Setup utility		
ConfigSync Configuration section		
	Local Address	**172.16.1.31 (internal)**
When complete, click…	**Next**	

Configure Unicast and Multicast Failover settings

17. Configure the failover settings by making the following settings:

Setup utility		
Failover Unicast Configuration section		
	Local Address | Port | VLAN	172.16.1.31 | 1026 | internal 192.168.1.31 | 1026 | Management Address
Failover Multicast Configuration section		
	Use Failover Multicast Address	Unchecked (Disabled)
When complete, click…	**Next**	

Configure Mirroring

18. Use the default primary and secondary local mirror address settings for **Mirroring Configuration**.

Setup utility		
Mirroring Configuration section		
	Primary Local Mirror Address	172.16.1.31 (internal)
	Secondary Local Mirror Address	None
When complete, click…	**Next**	

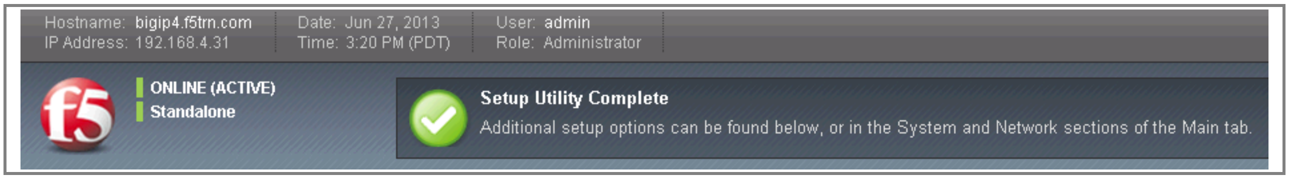
Complete the Setup utility

You have now configured the network interfaces. We will not be configuring a standard Active/Standby pair in this course.

19. Click **Finished**.

The message, **Setup Utility Complete** appears.

You should now be at the Welcome page and there should be a message at the top of the page indicating the Setup utility has completed, as shown below.



Hostname: bigip4.f5trn.com
IP Address: 192.168.4.31
Date: Jun 27, 2013
Time: 3:20 PM (PDT)
User: admin
Role: Administrator

ONLINE (ACTIVE)
Standalone

Setup Utility Complete
Additional setup options can be found below, or in the System and Network sections of the Main tab.

Configuration Utility Lab

Objective:

- Get familiar with managing BIG-IP from the command line and with the Web Configuration utility.
- Estimated time for completion: 5 minutes

Lab Requirements:

To log on to the system, you must know the following information, which is provided below:

- Management IP address of the BIG-IP LTM system
- User ID and password of the BIG-IP LTM system's Web Configuration utility
- User ID and password of the BIG-IP LTM system's command line interface

Computer Configuration

The virtual computer you are using is configured with two IP addresses: one in order to reach both the management and client networks once they are configured on your BIG-IP device.

Management IP address	**192.168.1.30/16**
Client IP address	**10.10.1.31/16.**

The Web Configuration Utility

1. In the Firefox Web browser, enter the address **https://10.10.1.31** to connect to the Web Configuration utility (which is often called "the GUI"). If questions appear regarding SSL Certificates, answer "Yes."
2. Enter the user ID and password of **admin** and **admin** that you entered during setup.
3. Note the setup and support options available on the Welcome page.
4. In the navigation pane on the left side of the Configuration Utility, click **Network**.

   A dropdown appears displaying the various network configuration options.
5. Click **Interfaces**, **Self IPs**, and **VLANs** and note the settings for each.

Command Line access (SSH)

6. Open an **SSH** session by clicking on the Putty icon.
7. Attempt to connect the external IP address of your BIG-IP system (**10.10.1.31**).
8. You **cannot** access BIG-IP LTM at this address because during setup you enabled **Port Lockdown** for the external self-IP addresses with only port 443 open. Therefore, you cannot access the device at port 22.

9. Reconfigure the self IP address **10.10.1.31** to also allow access via port 22 using the following settings:

Configuration utility		
Network » **Self IPs** » **10.10.1.31**		
Configuration section		
	Port Lockdown	Select **Allow Custom**
	Custom List	Select **TCP** and **Port** Type **22** in the field to the right of **Port** Click **Add**
When finished:		Click **Update**

10. Now try to open another SSH session to **10.10.1.31**, using **root** as the user ID and **default** as the password. You should have success this time. If not, review the Port Lockdown settings for this self IP and make sure port 22 was successfully added in the previous step. If you are prompted to accept the SSH key, do so.

Note: In the next section, you will start using some Traffic Management Shell (tmsh) commands to become familiar with the command line interface.

The "| less" command used in the instructions below allows scrolling when output from a tmsh command is more than the console can display on one screen. Use the arrow keys and the space bar to scroll through the output. Press <q> to quit scrolling mode and return to the Linux bash prompt.

11. Use the Traffic Management Shell (tmsh) command to view various configuration settings.

   a. At the command line in PuTTY, type:

   ```
   tmsh list /net vlan |less
   ```

   Compare the results with what you see in the Web Configuration utility (the "GUI") at **Network » VLANs**.

   b. Type the following command:

   ```
   tmsh list /net self |less
   ```

   Compare the results with what you see in the Configuration utility at **Network » Self IPs**.

   c. Type the following command:

   ```
   tmsh list /net interface |less
   ```

   Compare the results with what you see in the Configuration utility at **Network » Interfaces**.

   d. Type the following command:

   ```
   tmsh show /sys license |less
   ```

   Compare the results with what you see in the Configuration utility (GUI) at **System » License**.

   What is the **registration key** for your BIG-IP system?

What is the software **version** number this license was first activated for?

What is the **service check date** for your BIG-IP system?

e. Close the PuTTY window and terminate the session.

Configure command line access for the admin user

12. Open an SSH session to **10.10.1.31** or to **192.168.1.31** and attempt to log in as the **admin** user with password **admin**. Were you successful?

Your attempt to log in to the command line interface in the previous step as the **admin** user should fail because by default, the admin user does **not** have access to the command line.

13. Update the **admin** user settings to permit access to the command line interface but only to tmsh (i.e., not full Linux administrative privileges).

Configuration utility		
System » **Users** then click on user **admin**		
Account Properties section		
	Terminal Access	**tmsh**
When finished, click:	**Update**	

14. Open an SSH session to **10.10.1.31** or to **192.168.1.31** and try to log in with the **admin** user credentials again. Were you able to connect this time?
15. How is your access different from the **root** user? (**Hint:** Check the prompt after you log in as each user. Close your "admin" PuTTY session and open a new PuTTY session and log in with the **root** user credentials.) What do you have access to as the **root** user that you do not have access to as the **admin** user?
16. Close the PuTTY windows and terminate the sessions.

Check root user access to the GUI

17. Open a browser window to **https://10.10.1.31** or **https://192.168.1.31** and attempt to log in as the **root** user. Were you successful?

Note: User "root" has access to BIG-IP only with the command line, and not with the Web Configuration utility.

Configuration Backup Lab

Objective:

- Create a backup of the BIG-IP System on both the BIG-IP and your desktop.
- Estimated time for completion: 5 minutes

Lab Requirements:

- External IP address of the BIG-IP LTM system

Create a UCS Archive of Your Configuration

1. Open a browser window to **https://10.10.1.31** or **https://192.168.1.31** and create a backup of your current configuration

Configuration utility		
System » **Archives** then click **Create**		
General Properties section		
	File Name	**train1_base.ucs**
	Encryption	**Disabled**
	Private Keys	**Include**
When complete, click…	**Finished**, then click **OK** when the archive is complete	

2. Download your new UCS backup to your workstation hard drive for use possible in a later lab.

Configuration utility		
System » **Archives** then click **train1_base.ucs**		
train1_base.ucs section		
	Archive File	Click **Download: train1_base.ucs**, then save to download folder.

View the backup UCS file using the command line interface

3. Open an SSH session to BIG-IP system.
4. At the config# prompt, make a new directory:

```
mkdir /var/tmp/test
```

5. Change to the new directory:

```
cd /var/tmp/test
```

6. Copy the backup previously downloaded to the new directory (and replace, if necessary).

```
cp /var/local/ucs/train1_base.ucs train1_base.ucs
```

7. Decompress and extract the file contents:

   ```
   tar –xvzf train1_base.ucs
   ```

   The resulting files show the directory structure and all files stored within the UCS backup. Individual files can be viewed with `cat`, `tail`, `more`, `less`, and other command line tools.

8. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the “Creating an HTTP Pool and Virtual Server Lab.”

Chapter 2: Traffic Processing

Module 2 Lab – Processing Traffic

Objectives:

- Configure pools for servers
- Configure virtual servers and associate them with a pool
- Verify functionality

Estimated time for completion: 20 minutes

Lab Requirements:

- IP address/port combinations for BIG-IP LTM that can be reached by the client systems
- Servers configured with appropriate routes to return traffic through each BIG-IP LTM system

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module2_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33.

Creating an HTTP Pool and Virtual Server Lab

Create a Pool

1. Create a **Pool** using the information in the following table.

Configuration utility		
Local Traffic ⏩ Pools ⏩ Pool List, then click **Create**		
Configuration section		
	Configuration	**Basic**
	Name	**http_pool**
	Description	**HTTP pool**
Resource section:		
	Load Balancing Method	**Round Robin**
	Priority Group Activation	**Disabled**
	Node Name	(Leave blank)
	New Members	Address:Port **172.16.20.1**:**80** Click **Add** Address:Port **172.16.20.2**:**80** Click **Add** Address:Port **172.16.20.3**:**80** Click **Add**
When complete, click…	**Finished**	

Create a Virtual Server

2. Create a **Virtual Server** that uses the pool created in the previous step.

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

Test Your Configurations

Examining Virtual Server Statistics Verification through Statistics

3. Open a new browser session on your PC and point it to the virtual server at **http://10.10.1.100**. Note the results and refresh the screen 5-10 times. You may need to refresh using **Ctrl** + **F5** to force the browser not to use its cache.
4. View statistics and configuration information.

Configuration utility		
Statistics ⏩ Module Statistics ⏩ Local Traffic		
Display Options section		
	Statistics Type	**Virtual Servers**
	Did traffic go to the virtual server?	
	Statistics Type	Change to **Pools**
	Did traffic go to each pool member?	
	Did each pool member manage the same number of connections?	
	Did each pool member manage the same number of bytes?	
	How many TCP connections are opened each time you refresh the browser page?	

Expected Results and Troubleshooting

- Expected result: Five connections per refresh, distributed evenly among the pool members. The Web page consists of index.html and four objects. The Web servers have keep-alives disabled.
- If not, verify the following:
  - Is traffic getting to the virtual server?
    - Does 10.10.1.100 appear in your workstation's ARP table?

      Type `arp -a` at the workstation's terminal (command prompt).
    - Does the Statistics page show traffic received by vs_http?

      Verify that the address and port are correctly configured
- Is traffic getting to the pool members?
  - If no traffic is going to the pool members:
    - Verify http_pool has been assigned to vs_http
    - Verify that members' addresses and ports are correct
  - If traffic goes to pool member, but does not return:
    - Verify that self IP address 172.16.1.33 is configured on port 1.2. (This address is the pool members' default route.)

Create a Second Pool and Virtual Server

Next, you will create a second virtual server that has the same IP address as the virtual server you created previously (10.10.1.100). The port, however, will be different (443 instead of 80). This time, you will “forget” to create a pool first, and you will learn how to create a pool during the virtual server configuration.

5. Create another virtual server and pool.

Configuration utility	
Local Traffic ⏩ Virtual Servers : Virtual Server List, then click **Create**	
General Properties section	
Name	**vs_https**
Destination	Type: **Standard** Address: **10.10.1.100**
Service Port	**443** (or type or select **HTTPS**)
State	Enabled
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)	
Load Balancing Method	Round Robin
Node Name	(Leave blank)
New Members	Click **Node List** and use the resulting pull-down to select the nodes to add to the member list: 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**

Test Your Configuration

Note: When sending traffic to your virtual servers during testing, make sure that you are connected to the correct one: **http**://10.10.1.100 for virtual server 10.10.1.100:80, and **https**://10.10.1.100 for virtual server 10.10.1.100:443.

Examining Virtual Server Statistics

6. Open a new browser session on your Linux Ubuntu virtual computer and enter the address of the virtual server at **https://10.10.1.100**. Note the results, then press **Ctrl +F5** to refresh the screen 5-10 times.
7. View statistics and configuration information.

Configuration utility	
Statistics ⏩ Module Statistics ⏩ Local Traffic	
Display Options section	
Statistics Type	**Virtual Servers**
Did traffic go to the virtual server?	
Statistics Type	Change to **Pools**
Did traffic go to each pool member?	
Did each pool member manage the same number of connections?	
Did each pool member manage the same number of bytes?	
How many TCP connections are opened each time you refresh the browser page?	

Examining Statistics Using the Command Line

8. Using PuTTY, open an SSH session to your BIG-IP device at either the management IP address (192.168.1.31) or the self-IP address (10.10.1.31).
9. At the login prompt, enter the **root** user credentials you set up in the first lab.
10. Back on your browser window connected to **https://10.10.1.100**, refresh the page once using **Ctrl+F5**.
11. In your SSH client window, view pool statistics and virtual server statistics by entering the following commands at the config# prompt:

```
tmsh show /ltm pool https_pool |more
tmsh show /ltm virtual vs_https |more
```

Expected Results and Troubleshooting

- Expected result: You might see six connections the first time you request the page, (because of the SSL key exchange), but you should see only five connections each time you refresh the screen thereafter. The requests should be evenly distributed among the pool members.
- If you do not get the expected result, verify the following:

- Confirm that the virtual server was created. (Did you forget to click **Finish** for the virtual server after clicking **Finish** for the pool?)
- Is traffic getting to the virtual server?
    - ♦ Does 10.10.1.100 appear in your workstation’s ARP table? (You may need to clear your ARP table before testing to remove the entry from the vs_http virtual server.)
    - ♦ Does the Statistics page show traffic received by vs_https?

      Verify that the address and port are correctly configured.
- Is traffic getting to the pool members? Check Pool statistics:
    - ♦ If no traffic is going to the pool members:

      Verify https_pool has been assigned to vs_https
      Verify the correct members address and port
- If traffic goes to pool member but does not return:
    - ♦ Verify that the self IP address 172.16.1.33 is configured on port 1.2. (This address is the pool members’ default route).

Continue to the next lab.

Network Map Lab

View Configuration and Status from Network Map

1. If you have not done so, in your web browser, type the address **https://10.10.1.31**.
2. In the Navigation menu, click **Local Traffic » Network Map**, then click **Update Map**.
3. In **Local Traffic Network Map**, place your cursor over both virtual server and pool objects and notice what information is displayed about each object.
4. Select a pool member and disable it. You can do this by clicking the pool member in the Network Map, clicking **Disabled**, and then clicking **Update**.
5. Return to the **Local Traffic Network Map** and notice that status changed to disabled, indicated by a black square.
6. Re-enable the disabled pool member so that it will be used in later lab exercises.
7. Type **20.1** in the search field and then click **Update Map**. Notice that all members are still listed, but matches are highlighted.
8. Click **System » Preferences** and change the **Start Screen** from **Welcome** to **Network Map.** Click **Update**.
9. Click **Log out** and then log back in to **https://10.10.1.31** and notice that your default screen is now **Network Map**.
10. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the “Review Round Robin Load Balancing Statistics Lab.”

Chapter 3: Load Balancing

Module 3 Lab – Load Balancing

Objectives:

- Choose differing load balancing methods and view the resulting behavior
- Choose differing member priority and ratio values and view the resulting behavior

Estimated time for completion: 10 minutes

Lab Requirements:

- Access to a BIG-IP LTM with at least one pool that has two or more working members

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module3_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33. Click on **Local Traffic** >> **Network Map** and you should see **vs_http** configured with the **http_pool** and the **vs_https** configured with **https_pool**.

Review Round Robin Load Balancing Statistics

Reset the Statistics for http_pool

1. From the Navigation pane, click **Statistics » Module Statistics : Local Traffic**.
2. In the **Statistics Type** menu, select **Pools**.
3. Select (check) the checkbox next to **http_pool,** and then click **Reset**.

View Results using Round Robin Load Balancing

4. Open a browser session and access http://10.10.1.100 (**not** https://10.10.1.100).
5. Refresh the screen three times by pressing **Ctrl+F5**.
6. Return to the pools statistics on the **Local Traffic** page and click **Refresh**.
7. What are the results? Were the connection requests distributed evenly?
8. Reset the statistics for **http_pool** again.

Ratio (member) Load Balancing Lab

Configure Ratio (member) Load Balancing and test.

9. In the Navigation pane, expand the **Local Traffic** section.
10. Click **Pools**.
11. Click **http_pool**.
12. Click the **Members** tab.
13. In the **Load Balancing** section, change **Load Balancing Method** to **Ratio (member)** and then click **Update.**
14. In the **Current Members** section, click each member, set **Ratio** to the value in the table and then click **Update**. Click the **Members** tab to return to the **Current Members** list.

Member	Ratio
172.16.20.1:80	**1**
172.16.20.2:80	**2**
172.16.20.3:80	**3**

15. Open a new browser session and connect to **http://10.10.1.100**.
16. Refresh the browser 5-10 times by pressing **Ctrl+F5**.
17. In the Configuration Utility, view the pool statistics. You may need to refresh the view. What are the results? Traffic should be distributed to the members with a 1:2:3 ratio.

Priority Group Activation Lab

Configure Priority Group Activation

1. Reset the statistics for **http_pool**.
2. From the Navigation pane, expand the **Local Traffic** section and select **Pools**.
3. Select **http_pool**.
4. Select the **Members** tab.
5. In the **Load Balancing** section, change the **Priority Group Activation** setting to **Less than …**, the number of Available Members to **2**, and click **Update**.
6. Within the **Configuration** section of each member, set the **Priority** values as follows:

Member	Ratio	Priority Group
172.16.20.1:80	**1**	**0**
172.16.20.2:80	**2**	**4**
172.16.20.3:80	**3**	**4**

Remember to click **Update** after each entry.

7. Open a new browser session and connect to **http://10.10.1.100**.
8. Refresh the screen 5-10 times by pressing **Ctrl+F5**.
9. View the pool statistics. What are the results?
10. Reset the statistics for **http_pool**.
11. Disable pool member **172.16.20.2:80** in **http_pool**.
12. In the browser session connected to **http://10.10.1.100**, refresh the screen 5-10 times by pressing **Ctrl+F5**.
13. **Refresh** and view the pool statistics. What are the results?
14. Enable pool member **172.16.20.2:80** in **http_pool**.

Expected Results and Troubleshooting

- With Priority Group Activation set to less than 2 members and all pool members enabled, 172.16.20.1:80 should receive no traffic. Traffic is distributed to members 172.16.20.2 and 172.16.20.3 in a 2:3 ratio.
- With Priority Group Activation set to less than 2 members and pool member 172.16.20.2:80 disabled, 172.16.20.2:80 is not eligible to receive traffic. The next lower priority group (0) is activated as the number of available members in the pool has now fallen below the minimum 2. Traffic is distributed to members 172.16.20.1 and 172.16.20.3 in a 1:3 ratio

Reset Configuration

Reset **http_pool** and members to the following settings:

- Load Balancing: **Round Robin**
- Priority Group Activation: **Disabled**

If you want to continue to the next lab exercise, skip the "Lab Instructions" on the next page and go directly to the "Monitor for Nodes Lab."

Chapter 4: Monitors

Module 4 Lab – Monitors

Objective:

- Associate nodes, pools and pool members with monitors
- Create custom monitors
- Estimated time for completion: 30 minutes

Lab Requirements:

- Access to a BIG-IP LTM with at least one pool with two working members
- Some knowledge of the traffic sent by the members

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module4_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33. Click on **Local Traffic** >> **Network Map** and you should see **vs_http** configured with the **http_pool** and the **vs_https** configured with **https_pool**.

Monitor for Nodes Lab

Configure Monitors for Nodes

Check current nodes status

1. Observe the node status indicators and answer the questions in the spaces provided.

Configuration utility		
Local Traffic ⏩ Nodes ⏩ Node List		
Node List section		
	What are the nodes' statuses?	
	Will BIG-IP load-balance traffic to nodes with status ***Unknown?***	

Assign a default monitor to all nodes

2. Click **Default Monitor** tab in the menu bar.
3. Add **icmp** as the default monitor for all three nodes.

Configuration section		
	Health Monitors	Select **icmp** Press **<<** button
When complete, click…	**Update**	

Each time you click the Node List tab, the screen is refreshed.

4. Click **Node List** in the menu bar.
5. Recheck node status indicators.

	What are the nodes' statuses?	
	Was the change immediate?	

Create a Custom ICMP Monitor

6. Create a new ICMP monitor called **my_icmp.**

Configuration utility	
Local Traffic ⏩ Monitors ⏩ Create	
General Properties section	
Name	**my_icmp**
Type	ICMP
Configuration section	
Interval	**10** seconds
Timeout	**31** seconds
Transparent	**No**
When complete, click…	**Finished**

Assign the custom monitor to selected node

7. Add **my_icmp** as the default monitor for node 172.16.20.1.

Configuration utility	
Local Traffic ⏩ Nodes: Node List ⏩ 172.16.20.1	
Configuration section	
Health Monitors	**Node Specific**
Select Monitors	Select **my_icmp** Press **<<** button
When complete, click…	**Update**

8. Recheck node status indicators.

What are the nodes' statuses?	

Disassociate all monitors from selected node

9. Remove the monitor from node 172.16.20.2. Leave monitor my_icmp on 172.16.20.1.

Configuration utility		
Local Traffic ⏩ Nodes: Node List ⏩ 172.16.20.2		
Configuration section		
	Health Monitors	None
When complete, click…	**Update**	

10. Check the nodes’ statuses.

	What is the node status of Node 172.16.20.1?	
	What is the node status of Node 172.16.20.2?	
	What is the node status of Node 172.16.20.3?	
	Was the change immediate?	

Conclusion

Now each node is being tested differently:

- Node 172.16.20.1 has a specific assignment, **my_icmp**.
- Node 172.16.20.2 has no monitor assigned.
- Node 172.16.20.3 is using the **Node Default** monitor, which is currently icmp.

This is not a recommended configuration; rather it is used to demonstrate the three ways monitors can be associated with nodes.

Monitors for Pools and Pool Members Lab #1

Objective:

- Associate pool members with monitors
- Create custom monitors
- Estimated time for completion: 10 minutes

Check Current Member State

1. From the Navigation pane, click **Local Traffic » Pools** and then click **http_pool**.
2. Click the **Members** tab.
3. Check the status of the members.

	What are the members' statuses?	
	*Will BIG-IP load-balance traffic to nodes with status **Unknown?***	

Assign a Standard Monitor to a Pool

4. Assign the default http monitor to the http_pool.

Configuration utility		
Local Traffic ›› Pools : Pool List ›› http_pool		
Properties tab		
Configuration section		
	Health Monitors	Click **http** Press the **<<** button
When complete, click…	**Update**	

5. Recheck the member statuses.

Each time you press the Members tab, the screen is refreshed.

Create a New HTTP Monitor

6. Create a customized monitor based on the HTTP Monitor.

Configuration utility	
Local Traffic ⏩ Monitors ⏩ New Monitor	
General Properties	
Name	**my_http**
Type	**HTTP**
Parent Monitor	**http**
Configuration section	
Send String	**GET /index.html\r\n**
Receive String	**Server**
When complete, click…	**Finished**

Assign the Custom Monitor to a Pool Member

7. From the Navigation pane, click **Local Traffic » Pools** and then click **http_pool**.
8. Click the **Members** tab.
9. Click the member 172.16.20.2:80.

Configuration utility	
Local Traffic ›› Pools : Pool List ›› http_pool	
Configuration section	Select **Advanced** from the dropdown list.
Health Monitors	**Member Specific**
Select Monitors	Select **my_http** Press **<<** button
When complete, click…	**Update**

10. Check the members' statuses.

What are the members' statuses?	

Disassociate all Monitors for Selected Member

11. From the Navigation pane, click **Local Traffic » Pools** and click **http_pool**.
12. Click the **Members** tab.
13. Click the member 172.16.20.3:80.

Configuration utility	
Local Traffic ›› Pools : Pool List ›› http_pool	
Configuration section	Select **Advanced** from the dropdown list.
Health Monitors	**None**
When complete, click…	**Update**

14. Check the status.

What are the members' statuses?	
Was the change immediate?	

Conclusion

Now each member is being tested differently:

- Member 172.16.20.1:80 has its health monitor set to **inherit from pool**, so it inherits an http health monitor.
- Member 172.16.20.2:80 has a specific monitor assigned: **my_http**.
- Member 172.16.20.3:80 does not have an assigned monitor.

This configuration is not recommended; rather it is used to demonstrate the three ways monitors can be associated with pool members.

Monitors for Pools and Pool Members Lab #2

Objective:

- Associate members with monitors
- Create custom monitors
- Estimated time for completion: 10 minutes

Check Current Member State

1. From the Navigation pane, select **Local Traffic » Pools** and select **https_pool**.
2. Click **Members** tab.
3. Check the members' statuses.

	What are the members' statuses?	

Create a New HTTPS-based Monitor

4. Create a custom monitor based on the HTTPS Monitor.

Configuration utility		
Local Traffic ⏩ Monitors ⏩ New Monitor		
General Properties		
	Name	**my_https**
	Type	**HTTPS**
	Parent Monitor	**https**
Configuration section		
	Send String	**GET /index.html\r\n**
	Receive String	**Server 2**
When complete, click…	**Finished**	

Assign the Custom Monitor to Pool Members

5. From the Navigation pane, click **Local Traffic » Pools** and then click **https_pool**.

Configuration utility		
Local Traffic ›› Pools : Pool List ›› https_pool		
Configuration section		
	Health Monitors	Click **my_https** Press **<<** button
When complete, click…	**Update**	

6. Check the members' statuses.

	What are the members' statuses?	
	Was the change immediate?	
	What is the status of the virtual server vs_https?	

Check Status of Nodes and Members from Network Map

7. From the Navigation pane, expand the **Local Traffic** section, and then click the **Network Map**.
8. Move the cursor over the pool members. Notice that the status of a node state can be different from the status of a pool member.

	What are the members' statuses?	

Recall that you have assigned different monitors to nodes and pool members.

Change the Definition of the Custom Monitor

9. From the Navigation pane, expand the **Local Traffic** section.
10. Click **Monitors**.
11. Click **my_https**.
12. In the **Configuration** section, change the Receive String to **Server [1-3]**

[1-3] is a regular expression that matches any single character in the range from 1 to 3.

13. When complete, click **Update**.
14. Check the status of members in **https_pool**.

	What are the members' statuses?	
	Was the change immediate?	

Reset Configuration

15. Make sure all **pool members** for both **http_pool** and **https_pool** are in one of the following states:

    - **Available** or **Green**
    - **Unknown** or **Blue**

16. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the “Source Address Persistence Lab.”

Chapter 5: Profiles

Module 5 Lab – Profiles

There is no lab for Module 5 Profiles. There are labs using Profiles in both Modules 6: Persistence and Module 7: SSL Termination.

Chapter 6: Persistence

Module 6 Labs – Persistence

Objective:

- Configure persistence profiles and associate them with virtual servers
- Verify functionality
- Estimated time for completion: 30 minutes

Lab Requirements:

- Two or more working members in https_pool
- A virtual server at https://10.10.1.100 that is associated with https_pool

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module6_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named "external" and "internal"), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33. Click on **Local Traffic** >> **Network Map** and you should see **vs_http** configured with the **http_pool** and the **vs_https** configured with **https_pool**.

Source Address Persistence Lab

Objective:

- Configure a Source Address Persistence profile and associate it with virtual servers
- Verify functionality
- Estimated time for completion: 10 minutes

Configure Source Address Affinity

Confirm traffic behavior before persistence

1. Ensure that the load balancing method for **https_pool** is **Round Robin** and that **Priority Group Activation** is disabled. Although this step is not required to enable persistence, it ensures that the recurring direction of a connection to a pool member is due to persistence and not due to a load balancing choice.
2. Access and reset the statistics for the pool **https_pool**.
3. Open a new browser session and connect to **https://10.10.1.100**.
4. Refresh the browser 5-10 times by clicking **Ctrl+F5**.
5. Refresh and view pool statistics.

Q. What are the results?

Expected results and troubleshooting

You should see BIG-IP load-balance the traffic from each refresh request across all pool members, and each pool member should receive approximately the same amount of traffic. If you do not see these results, make sure you reset the statistics properly in step 1, and then repeat the steps through step 4 again.

Configure a Source Address Affinity persistence profile and assign it to a virtual server

6. Create a Persistence Profile based on the following:

Configuration utility	
Local Traffic ⏩ Profiles ⏩ Persistence ⏩ Create	
General Properties section	
Name	**Pr_Src_Persist**
Persistence Type	**Source Address Affinity**
Configuration section	
Timeout	Select (check) the **Custom** checkbox for **Timeout** and then set **Timeout** to **15 seconds.**
Mask	Click on the **Custom** checkbox for **Mask** and specify a network mask of **255.255.255.0.**
When complete, click…	**Finished**

7. Assign **Pr_Src_Persist** to **vs_https**

Configuration utility	
Local Traffic ⏩ Virtual Servers ⏩ vs_https ⏩ Resources	
Load Balancing section	
Default Pool	**https_pool**
Default Persistence Profile	**Pr_Src_Persist**
When complete, click…	**Update**

Confirm traffic behavior after persistence

8. Access and reset the statistics for **https_pool**.
9. Open a new browser session and connect to **https://10.10.1.100.**
10. Press **Ctrl+F5 to** refresh the screen five to ten times.
11. View the pool statistics.

Q. What are the results?

12. Wait for at least 30 seconds, and then refresh again the https://10.10.1.100 website again. Now the web traffic should be load-balanced to another pool member. Confirm this by refreshing and viewing the pool member statistics.
13. View persistence records statistics.

Configuration utility		
Statistics ▸▸ Module Statistics ▸▸ Local Traffic		
Display Options section		
	Statistics Type	**Persistence Records**
	Data Format	**Normalized**
When complete, click…	**Refresh**	

14. If persistence records do not appear, go back to the browser connected to **https://10.10.1.100** and refresh by clicking **Ctrl+F5** the screen three times. Check for persistence records statistics again.

Q. Why might persistence records statistics not appear the first time?

Expected results and troubleshooting

While the persistence entry is active for the chosen client IP address, all of the traffic generated each time you refresh the display is directed to the same pool member. Because the persistence profile is configured with a timeout value of 15 seconds, your persistence entry may time out before you are able to view the persistence statistics in the Configuration utility.

Continue to the next lab.

Cookie Persistence Lab

Objectives:

- Configure a cookie persistence profile, assign it to a virtual server, verify functionality, and observe changes in traffic behavior.
- Estimated time for completion: 10 minutes

Lab Requirements:

- Two or more working pool members in http_pool
- A virtual server at http://10.10.1.100 associated with http_pool

Configure Cookie Persistence

Confirm traffic behavior before persistence

1. Set the load balancing method for http_pool to **Round Robin** and make sure that **Priority Group Activation** is disabled. (Although this step is not required to enable persistence, it ensures that the recurring direction of a connection to a pool member is determined by persistence settings and not by the load balancing choice.)
2. Access and reset the statistics for pool **http_pool**.
3. Open a new browser session and connect to **http://10.10.1.100**.
4. Refresh the screen 5-10 times by clicking **Ctrl+F5**.
5. Refresh and view pool statistics.

Q. What are the results?

Expected results and troubleshooting

The BIG-IP device should load-balance the traffic resulting from each refresh request across all pool members, with each pool member receiving approximately the same amount of traffic. If you do not see these results, make sure that you changed the load balancing method to Round Robin and that you reset the statistics, and then repeat the preceding lab steps.

Create a cookie persistence profile and assign it to a virtual server

6. Create a custom cookie persistence profile named **Pr_Cookie_Persist**. When you select **Cookie** as the **Persistence Type**, the **Configuration Section** appears. Leave all of the settings in the **Configuration** section in their default state for now.

Configuration utility		
Local Traffic ▸▸ Profiles ▸▸ Persistence ▸▸ Create		
General Properties section		
	Name	**Pr_Cookie_Persist**
	Persistence Type	**Cookie**
When complete, click…	**Finished**	

7. Assign **Pr_Cookie_Persist** to **vs_http**.

Configuration utility		
Local Traffic ▸▸ Virtual Servers ▸▸ vs_http ▸▸ Resources		
Load Balancing section		
	Default Pool	**http_pool**
	Default Persistence Profile	**Pr_Cookie_Persist**
When complete, click…	**Update**	

Hint: If you received an error message in the preceding section, think about profile dependencies. Modify **vs_http** to include an HTTP Profile and repeat the step above.

Confirm traffic behavior after persistence

8. Access and reset the statistics for **http_pool**.
9. On the browser connected to **http://10.10.1.100**, refresh the screen 5 to 10 times.
10. View the pool statistics.

Q. What are the results?

11. Click the **Display Cookie** link in the web page to view the cookie.

Expected Results and Troubleshooting

All traffic is directed to one member. If not, ensure that the browser allows cookies to be saved and disable persistence on the virtual server.

12. Set the default persistence profile on the virtual server **vs_http** to **None**.

Configuration utility		
Local Traffic ▸▸ Virtual Servers ▸▸ vs_http ▸▸ Resources		
Load Balancing section		
	Default Pool	**http_pool**
	Default Persistence Profile	**None**
When complete, click…	**Update**	

Continue to the next lab.

Disabled Members Lab

Objective:

- Observe the interaction between persistence and the disabled status
- Estimated time for completion: 15 minutes

Lab Requirements:

- Virtual server **vs_https** configured with the pool **https_pool** and the persistence profile **Pr_Src_Persist**

Persistence and Disabled Pool Members

Preconfiguration steps

1. Update the timeout value in the Pr_Src_Persist profile.

Configuration utility		
Local Traffic ⏩ Profiles ⏩ Persistence ⏩ Pr_Src_Persist		
Configuration section		
	Timeout	**800** seconds
When complete, click…	**Update**	

Establish a persistent session and disable a member

2. Open a Web browser to **https://10.10.1.100**. Refresh the page several times to verify that there is a persistent connection to the same pool member.

Q. What is the IP address of the pool member to which there is a persistent connection?

3. Disable the pool member to which there is a persistent connection (as noted in Step 2).

Configuration utility	
Local Traffic ⏩ Pools ⏩ https_pool ⏩ Members	
Current Members section	
	Click the checkbox on the left side of the pool member that you identified in previous step.
When complete, click…	**Disable**

4. In the browser connected to **https://10.10.1.100,** refresh the page by clicking **Ctrl+F5** several times.

Q. Is the persistent connection still to the same pool member?

5. Force offline the pool member to which there is a persistent connection.

Configuration utility		
Local Traffic ⏩ Pools ⏩ https_pool ⏩ Members		
Current Members section		
	In the **Member** column, click the IP address:port link of the pool member that you identified in previous step.	
Member Properties section		
	State	Click the **Forced Offline (Only active connections allowed)** radio button
When complete, click…	**Update**	

6. In the browser connected to **https://10.10.1.100**, refresh the page several times.

Q. Is the persistent connection still to the same pool member?

Disable the parent node and test the results

7. Disable the parent node of the pool member to which there is a persistent connection.

Configuration utility	
Local Traffic ⏩ Nodes ⏩ Node List	
Node List section	
	Click the checkbox to the left of the parent node of the pool member to which there is a persistent connection. In this class, the name of the parent node is the IP address part of the pool member.
When complete, click…	**Disable**

8. Refresh the page at **https://10.10.1.100** several times.

Q. Is the persistent connection still to the same node?

View object status from the Network Map

9. View the status of all your configuration objects in the Network Map. Hover your cursor over the entry for the pool member with the persistent connection and note the status of the pool member.

10. Enable the node and the pool member that you disabled earlier in this lab.

Clean up at end of lab

11. Remove the **Pr_Src_Persist** profile from **vs_https**.
12. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the “Client SSL Lab.”

Chapter 7: SSL Termination

Module 7 Lab – SSL Termination

Objective:

- Create a self-signed certificates
- Create a clientssl profile
- Create a virtual server that uses the clientssl profile and load-balances traffic

Lab Requirements:

- A pool of members at port 80 (http_pool)
- A Web browser

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module7_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33. Click on **Local Traffic** >> **Network Map** and you should see **vs_http** configured with the **http_pool** and the **vs_https** configured with **https_pool**.

Client SSL Lab

Behavior before configuration: SSL traffic is encrypted from client.

1. Open a Web browser and connect to **https://10.10.1.100.**
2. Depending on the browser, you may see a lock in the lower right corner of the window; it indicates the session is encrypted and secure. Alternately, find the certificate that is being used for the session. Right click on the web page, choose "**View Page Info**" and click the **Security** tab.
3. On the Web page, note the pool member address and port in the body of the Web page (for example: 172.16.20.1:443).

Generate a Certificate

Create an SSL Certificate

4. Create a custom SSL Certificate.

Configuration utility	
System ›› File Management : SSL Certificate List ›› click Create...	
General Properties section	
Name	**StudentCertificate**
Certificate Properties section	
Issuer	**Self**
Common Name	**www.student.com**
Division	**Training**
Organization	**F5 Networks**
Locality	**Seattle**
State or Province	**Washington**
Country	**US**
E-mail Address	**Leave blank**
Lifetime	**365**
Key Properties section	
Size	**2048**
When complete, click…	**Finished**

Create an SSL Profile

5. 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**
When complete, click…	**Finished**

Create a New Virtual Server

6. Create a new virtual server called **vs_ssl** with an IP address of **10.10.1.101:443** and assign pool **https_pool** as its default pool.

Configuration utility	
Local Traffic ⏩ Virtual Servers ⏩ Virtual Server List, then click Create	
General Properties section	
Name	**vs_ssl**
Destination	Type: **Standard** Address: **10.10.1.101**
Service Port	**443** (or type or select **HTTPS**)
State	Enabled
Configuration section	
SSL Profile (Client)	**Pr_Client_SSL**
Resources section:	
Default Pool	**http_pool**
When complete, click…	**Finished**

7. In your Web browser, go to **https://10.10.1.101**. If prompted, accept the SSL certificate.

The browser session is encrypted on the client side, but not on the server side.

8. Note the Pool Member address:port combination in the body of the web page (172.16.20.1:80).

Expected Results

Unless otherwise configured, traffic is encrypted from client to the BIG-IP system, but unencrypted between the BIG-IP and the pool members. In other words, the pool member should be using port 80, which is unencrypted.

9. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the “Configuring a NAT Lab.”

Chapter 8: NATs and SNATs

Module 8 Labs – NATs and SNATs

Lab Objectives:

- Configure a NAT to pass traffic between an external device and an internal node
- Configure SNAT Auto Map and a SNAT Pool and test address translation

Lab Requirements:

- One or more servers on the internal side of the BIG-IP system
- An available IP address to use for the NAT

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module8_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33. Click on **Local Traffic** >> **Network Map** and you should see **vs_http** configured with the **http_pool** and the **vs_https** configured with **https_pool**.

Configuring a NAT Lab

The Network Address Translation screen displays the NAT address and the associated node address for each NAT.

Configure a NAT

1. In the Navigation pane, expand **Local Traffic**.

Configuration utility	
Local Traffic » **Address Translation** » **NAT List**, then click **Create**	
Configuration section	
Name	**Nat_200_to_2**
NAT Address	**10.10.1.200**
Origin Address	**172.16.20.2**
State	**Enabled**
When complete, click…	**Finished**

Testing the NAT - Inbound

2. Open a browser session to **http://10.10.1.200**.
3. Note what is on the page.
4. Using PuTTY, open an SSH session to 10.10.1.200 port 22.
5. If prompted, accept the certificate and log in with a user ID of **student** and password of **student**.

   Note that you can connect to multiple services through the NAT (in this example, using both a Web browser and PuTTY) and that the connection always connects to 172.16.20.2.

NOTE: Although the NAT that you configured could provide outbound connections as well, the routing tables on the server do not allow that in the lab environment.

Delete the NAT

6. In the Navigation pane, expand **Local Traffic**.
7. Click **Address Translation** and then the **NAT List** tab.
8. Check the box next to the NAT you just created, **10.10.1.200**, and then click the **Delete** button.
9. Click **Delete** to confirm the deletion

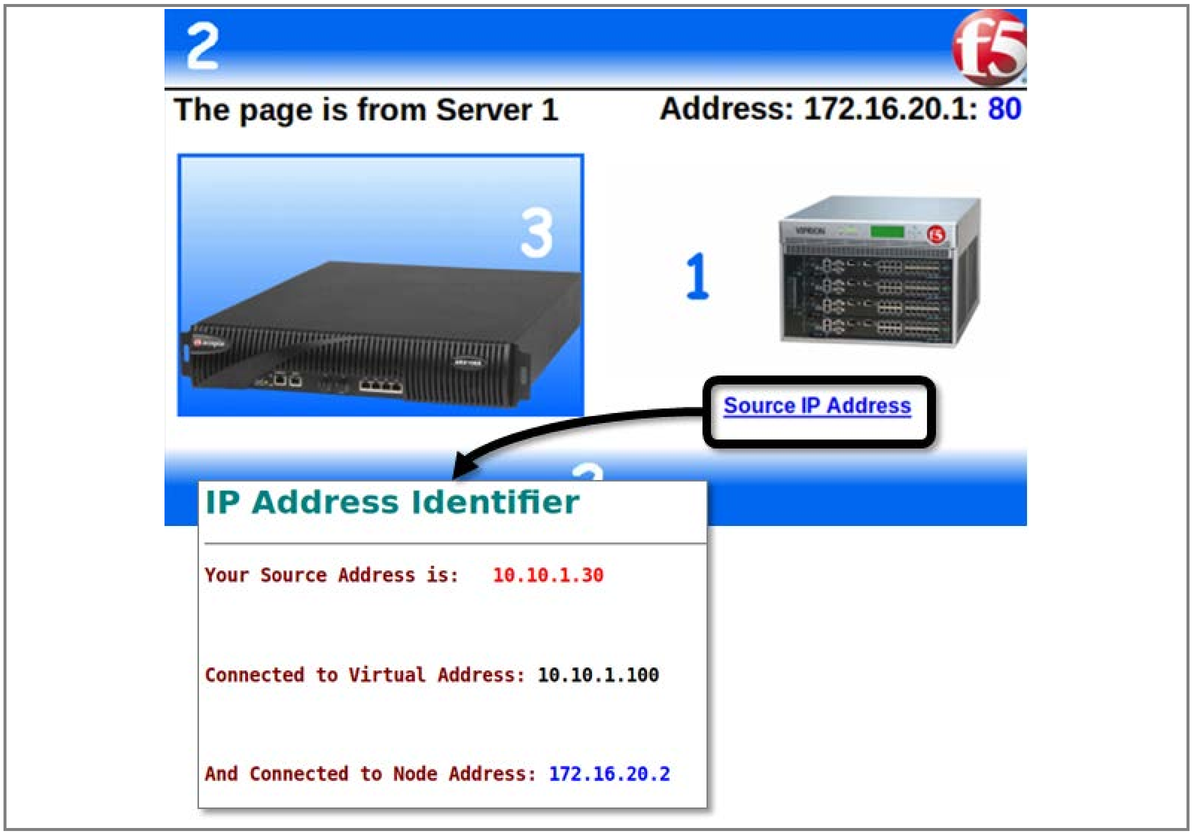
SNAT Labs

Lab Requirements:

- Access to a BIG-IP LTM System
- An available IP address to use for the SNAT

Test Behavior Without a SNAT

1. Open two browser sessions: one to **http://10.10.1.100** and the other to **https://10.10.1.100**.
2. On both of the resulting Web pages, click the link that says **Source IP Address** (as shown in the image below) and note the source IP addresses as passed from BIG-IP to the internal application server.



The page is from Server 1 Address: 172.16.20.1: 80

Source IP Address

IP Address Identifier

Your Source Address is: 10.10.1.30

Connected to Virtual Address: 10.10.1.100

And Connected to Node Address: 172.16.20.2

3. The three Web servers have IP addresses of 172.16.20.1, 172.16.20.2, and 172.16.20.3. The servers can return response traffic to your computer at 10.10.1.30 through the BIG-IP device because each contains the following server route:

Destination	Gateway
10.10.1/24	**172.16.1.33**

Configure SNAT Auto Map

Add SNAT Auto Map to the virtual server

1. Refresh (Ctrl+F5) the browser window that is connected to **https://10.10.1.100**.
2. View your source IP address again by clicking the **Source IP Address** link on the page. Your source IP address should still be 10.10.1.30.
3. Now add SNAT Auto Map to **vs_https**:

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

Test connectivity with the SNAT

4. Refresh (Ctrl+F5) the browser that is connected to **https://10.10.1.100** and view your source IP address there. It should have changed to 172.16.1.33, which is the floating IP address of VLAN internal, the egress VLAN for traffic flowing from the BIG-IP system to the pool members.

Continue to the next lab.

Configure SNAT Pool

Configure a SNAT pool

SNAT pools were not discussed during the lecture portion of the LTM Essentials WBT, but are another common method to accomplish SNAT'ing so lab steps are included here.

5. Follow the instructions in the table below to create a new SNAT pool called **MySnatPool**.

Configuration utility		
Local Traffic » Address Translation » SNAT Pool List, then click **Create**		
Configuration section		
	Name	**MySnatPool**
	Member List	**IP Address: 10.10.1.150, then click Add** **IP Address: 172.16.1.150, then click Add**
When complete, click…	**Finished**	

Change the virtual server to use a SNAT pool

6. Refresh (Ctrl+F5) the browser window that is connected to **http://10.10.1.100**.
7. View your source IP address again by clicking on the **Source IP Address** link on the page. Your source IP address should still be 10.10.1.30.
8. Change the source address translation method on **vs_http** to SNAT pool.

Configuration utility		
Local Traffic » Virtual Servers, then click **vs_http**		
Configuration section		
	Source Address Translation	Select **SNAT**
	SNAT Pool	Select **MySnatPool**
When complete, click…	**Update**	

Test connectivity with the SNAT Pool

9. Refresh (Ctrl+F5) the browser that is connected to **http://10.10.1.100** and view your source IP address there. It should have changed to 172.16.1.150, the translation IP address in the SNAT pool that is on VLAN internal, which is the egress VLAN for traffic flowing from the BIG-IP system to the pool members.

Clean up and Delete the SNATs

10. Remove the SNAT option from virtual server **vs_http** and **vs_https** by setting **Source Address Translation** to **None**.
11. In the Configuration utility, navigate to **Local Traffic » Address Translation : SNAT Pool List** and delete **MySnatPool**.

12. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the “iRules Lab #1.”

Chapter 9: iRules

Module 9 Labs – iRules

Objective:

- Configure a series of iRules, pools, and virtual servers to demonstrate a variety of rule features and functions.
- Estimated time for completion: 30 minutes.

Lab Requirements:

- External IP address of the virtual server
- IP address(es) of internal node(s)

Lab Instructions

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module9_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33. Click on **Local Traffic** >> **Network Map** and you should see **vs_http** configured with the **http_pool** and the **vs_https** configured with **https_pool**.

iRules Lab

Create and use an iRule that processes requests based on the TCP port.

iRules Lab Steps

Create pools for application services deployment

1. In **Local Traffic** » **Pools**, create three new pools.
2. Create **pool1** that contains one member, **172.16.20.1:*** (Port is "All services")
3. Create **pool2** that contains one member, **172.16.20.2:*** (Port is "All services")
4. Create **pool3** that contains one member, **172.16.20.3:*** (Port is "All services")

Create an iRule for TCP port checking

5. Navigate to **Local Traffic** and create an **iRule** as follows:

Configuration Utility		
Local Traffic ›› iRules : iRule List then click **Create**		
General Properties section		
	Name	**Rule_tcp_port**

	Definition	`when CLIENT_ACCEPTED {`
		`   if {[TCP::local_port] == 80} {`
		`      pool pool1`
		`   }`
		`   elseif {[TCP::local_port] == 443} {`
		`      pool pool2`
		`   }`
		`}`

When complete, click…		**Finished**

6. Create a virtual server that uses this iRule:

Configuration Utility	
Local Traffic ›› Virtual Servers : Virtual Server List then click **Create**	
General Properties section	
Name	**vs_tcpport**
Destination	**10.10.1.103**
Service Port	***All Ports**
Resources section	
iRules	**rule_tcp_port**
Default Pool	**pool3**
When complete, click…	**Finished**

Verify behavior through statistics

7. Open a new browser session on your computer and direct it to your Virtual Server address and files:
    - http://10.10.1.103
    - https://10.10.1.103
    - Using Putty, open an **SSH** session to **10.10.1.103** port **22**

NOTE: You can verify that your SSH session went to Pool3 using Statistics.

8. View statistics and configuration information by navigating to **Statistics » Module Statistics : Local Traffic**

9. In the **Statistics Type** menu, select **Virtual Servers**
10. In the **Statistics Type** menu, select **Pools**
11. To which node is traffic being directed for each client request above and why?
12. If you want to continue to the next lab exercise, skip the “Lab Instructions” on the next page and go directly to the

Chapter 10: Redundant Pair Setup

The online lab environment does not support setting up a redundant pair.

If you would like to get hands-on training with redundant systems, please enroll in the *Configuring BIG-IP Local Traffic Manager (LTM) v11* instructor-led course. For current course offerings and schedules, visit the Training page at F5.com.

The steps to set up a redundant pair in BIG-IP Version 10 can be found in Appendix A.

Chapter 11: High Availability

The Online Lab Environment does not support High Availability.

If you would like to get hands-on training with high availability, please enroll in the *Configuring BIG-IP Local Traffic Manager (LTM) v11* instructor-led course. For current course offerings and schedules, visit the Training page at F5.com.

The steps to set up High Availability in BIG-IP Version 10 can be found in Appendix A.

Configuration Lab Project

Configuration Lab Project

Lab Objectives:

In this lab, you will work with many of the concepts that you learned in Modules 1 to 8. In those modules, the lab steps were very specific and told you exactly what to do. One of the objectives of this lab configuration project is to see if you remember how to configure each feature. Therefore, the lab steps in this configuration project are not specific but rather given at a much higher level. Another objective of this configuration project is to give you an opportunity to configure all features together rather than individually. Upon completion, you will have configured a BIG-IP system with working virtual servers, profiles, monitors, and pools.

There are two stages to this lab:

1. Create new pools, profiles, monitors, and virtual servers.
2. Verify that the configuration works as expected.

Lab Instructions – Loading a Base Configuration

1. After connecting to the F5 Training Lab, click the **Ubuntu Client** icon**.**
2. Click the **Firefox Web browser** icon in the left panel. When prompted, log in as **admin** with a password of **admin.**
3. In the Navigation pane, expand the **System** section, and then click **Archives**.
4. Click the **Module2_Lab_begin.ucs** archive and then click **Restore**. It will take a minute to restore the .ucs archive. A status message appears telling you how the configuration process is proceeding. Disregard any error messages (which are an artifact of the training environment) and click **OK**.
5. Reconfiguring from the .ucs archive installs a known, good configuration at the beginning of the lab. As you can see, after reconfiguring, your system is licensed, has two VLANs (named “external” and “internal”), and four self IPs: 10.10.1.31, 10.10.1.33, 172.16.1.31 and 172.16.1.33.

Reconfigure the BIG-IP LTM System

A. Create monitors according to the following table

Name	Type	Settings	Associations
my_http	http	Interval – 5, Timeout – 16 Receive String – Server Others – leave at defaults	http_pool (Once pool is created, below.)

B. Assign monitors according to the following table

Name	Type	Settings	Associations
icmp (Default Monitor)	icmp	Use all default settings	Node Default

C. Create pools according to the following table

Name	Load Balance	Members	Port	Ratio	Priortity	Monitors
ssh_pool	Round Robin	172.16.20.1 172.16.20.2 172.16.20.3	22 22 22	1 1 1	1 1 1	
http_pool	Ratio Member Priority Group Activation Less than 2	172.16.20.1 172.16.20.2 172.16.20.3	80 80 80	2 2 1	1 4 4	my_http
https_pool	Round Robin	172.16.20.1 172.16.20.2 172.16.20.3	443 443 443	1 1 1	1 1 1	

D. Create profiles as listed in the following table

Name	Profile	Type	Parent Profile	Settings
Pr_Src_Persist	Persistence	Source Address	source_addr	Timeout of 30 seconds and mask of 255.255.255.0
Pr_SSL_term	SSL	Client	clientssl	Create a self-signed certificate: “TestCertificate.” Assign it to this profile. Refer to Lab 7 for example.

E. Create virtual servers according to the following table

NOTE: Remember that persistence profiles are configured on the **Resources** tab of the virtual server configuration page and that all other profile types on the **Properties** tab.

Name	**IP Address**	**Port**	**Resources**	**Profiles & SNAT**
vs_ssh	**10.10.1.100**	**22**	**ssh_pool**	**Defaults only**
vs_http	**10.10.1.100**	**80**	**http_pool**	**SNAT Automap**
vs_https	**10.10.1.100**	**443**	**https_pool**	**Pr_Src_Persist**
vs_ssl	**10.10.1.102**	**443**	**http_pool**	**Pr_SSL_term**

F. Save your new configuration

Back up your new configuration as **Lab_Project.ucs**.

Verification

Activity	Questions	Working?
Open a browser and connect to http://10.10.1.100 Refresh the screen 5-10 times	Is the system performing load balancing? Why or why not?	
Open a browser and connect to https://10.10.1.100 Refresh the screen 5-10 times View the node statistics	Is the system performing load balancing? Why or why not?	
Open a PuTTY SSH session to: 10.10.1.100:22 After connecting, log in User ID: student and password: student View the node statistics.	Were you able to connect? Which node did you connect to? Do you have an open connection?	
Open a browser and connect (again) to https://10.10.1.100 Refresh the screen 5-10 times View the node statistics.	Is the system performing load balancing? Why or why not? Are you connecting to the same node as when tested above?	
Open a browser and connect to both https://10.10.1.100 and http://10.10.1.100 Click the link to show the source address.	What is the source address for http and https? Why are they different?	
Open a browser and connect to https://10.10.1.102	Is the session secure? Is the data from BIG-IP LTM to the server encrypted?	

Review Questions

1. Which admin users' passwords are changed by the BIG-IP setup utility, and what type access do those users get by default (Web GUI or Command Line or both)?

2. What is a node? What are a pool and pool member? What is a profile? What is a virtual server?

3. Name the load-balancing modes.

4. How are monitors created, and to what can they be assigned?

5. If a particular node is in a node-disabled condition, will any types of client requests still be directed to that pool member?

6. What is the difference between the client SSL and the server SSL Profiles?

7. Why would you use SNATs?

This completes the BIG-IP LTM Essentials Web-Based Training Lab Guide.

Thank you for taking the time to complete the exercises.

Answers to Configuration Project Questions

Activity	Questions	Answers
Refresh http://10.10.1.100	**Are you load balancing? Why or why not?**	**Yes, but should only be using Nodes 20.2 & 20.3 because they have higher priorities for Priority Group Activation**
Refresh https://10.10.1.100	**Are you load balancing? Why or why not?**	**Actually this is a trick question. The first request is load balanced but subsequent requests within the 30 second timeout window should persist to same Node.**
SSH to: 10.10.1.100:22 Login with user ID and password of student View the node statistics	**Did you connect? Which node did you connect to? Do you have an open connection?**	**Should have connected ok. You have to go to statistics to figure out which node and your SSH connection remains open until you exit putty or logoff.**
Refresh (again) https://10.10.1.100	**Are you load balancing? Why or why not? Are you connecting to the same node as 2 steps above?**	**Your previous 30 second persistence record should have timed out by now. The first request should go to a different member than previous session and then should persist for another 30 seconds.**
For both https and http Click link source address	**What is source address for http and https? Why are they different?**	**http should have a source IP of 172.16.1.33 because of SNAT Automap, and https should have a source IP of 10.10.1.30.**
Browser session to https://10.10.1.102	**Is the session secure? Is the data encrypted from the Server to the BIG-IP LTM?**	**The session should be secure (using https) from client PC to BIG-IP, then unencrypted (http) from BIG-IP to Server.**

Answers to Review Questions

1. **Which admin users passwords are changed by the BIG-IP setup utility, and what access do they have (Web GUI or Command Line)?**
    - **root** – and it should have access only to command line not the web GUI.
    - **admin** – and it should initially have access only to the web GUI, but command line access can be added
2. **What is a node? A pool and pool member? A virtual server?**
    - Node is IP Address only of a server where Pool Member typically contains both IP Address and Port
    - A Pool is a group of Pool Members, and the Virtual Server is the client representation of the application. Clients seldom know there are multiple Pool Members behind a Virtual.
3. **List the load balancing modes.**
    - Round Robin is the default load balancing mode but we can also use Ratio, Least Connections, Fastest, Observed and Predictive.
    - F5 Networks continues to add new features to BIG-IP LTM including new load balancing modes, so you might see more depending on what version you are running.
4. **How are monitors created, and what can they be assigned to?**
    - Just like other objects, they are created by selecting Monitors and clicking the create button or the ⊕ sign from the flyout menu.
    - Monitors also need to be assigned before they will be used. Monitors can be assigned to all Nodes or an individual Node, or at the Pool level or to an individual Pool Member
5. **If a particular node is in a node disabled condition, will any types of client requests still be directed to that pool member?**
    - Yes, client requests can still be directed to a disabled Node if there is still a persistent session (i.e. within the timeout window)
    - On the other hand, if the Node is administratively “Forced Offline” rather than Disabled then no more client requests will be sent until the Node is Enabled again.
6. **What is the difference between the client SSL and server SSL Profiles?**
    - The Client SSL Profile encrypts (https) network traffic between the client and BIG-IP.
    - The Server SSL Profile encrypts (https) network traffic between BIG-IP and the servers.
7. **Why would you use SNATs?**
    - SNATs are used to fix or assist with routing issues. There are MANY ways a SNAT can be used to resolve the many different types of routing issues, two are listed below.
        - RFC1918 (non-routable) client traffic outbound to internet
        - Pool Members default route cannot be pointed at BIG-IP. But remember--if BIG-IP changes an IP Address then response packet must return through BIG-IP.

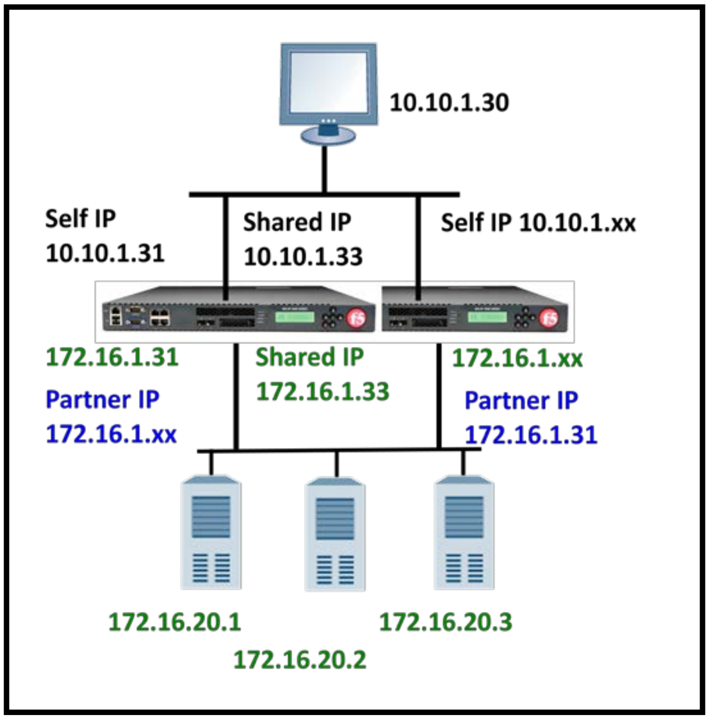
Appendix A

Setting up a Redundant Pair and High Availability in BIG-IP Version 10

Setting up a Redundant Pair

Configuration of BIG-IP #1 and BIG-IP #2

BIG-IP #1 should now be configured like the diagram shown below and also have Virtual Servers, Pools, Monitors and Profiles. On the next page we will configure BIG-IP #2 from a clean system.



BIG-IP Redundant Pair Configuration

Setup of BIG-IP #2 Lab

NOTE: The second system in your lab pair is licensed but not currently configured. Connect to **https://192.168.1.246** and run the Setup Utility using the configuration options below.

Step	**System Y**
Management Port IP address	**192.168.1.246**
Management Port Netmask	**255.255.255.0**
Hostname	**bigip2.f5trn.com**
High Availability	**Redundant Pair**
Unit ID	**2**
root password	**default**
admin password	**admin**
SSH Access	*** All Addresses**
VLAN Name on 1.2	**Internal**
Self IP Address	**172.16.1.32**
Netmask	**255.255.0.0**
Port Lockdown	**Allow Default**
Floating IP	**172.16.1.33**
Failover Peer IP	**172.16.1.31**
Port Association	**1.2 Untagged**
VLAN Name on 1.1	**External**
Self IP Address	**10.10.1.32**
Netmask	**255.255.0.0**
Port Lockdown	**Allow Default**
Default Gateway	**Leave Blank**
Floating IP	**10.10.1.33**
Port Association	**1.1 Untagged**

Status of BIG-IP #1 and BIG-IP #2

Note: You may notice that both BIG-IP #1 and #2 are in an Active state. This is not a desired state, but we will wait to resolve this in the next Module 11 Lab when we setup Network Failover.

Synchronization Lab

Synchronization should always be from the system's whose configuration is desired. In our case, we wish to Synchronize the BIG-IP #1 configuration to BIG-IP #2 since it has no configuration.

BIG-IP #2 configuration before Synchronization

At this point, the BIG-IP #2 should have a base configuration set with passwords, VLANs and Self IPs. Verify the Self IPs (Network / Self IPs) for BIG-IP #2 are set to 10.10.1.xx, 10.10.1.33, 172.16.1.xx and 172.16.1.33.

Synchronizing Configuration from BIG-IP #1 to #2

1. Open a browser to **https://192.168.1.245. (BIG-IP #1)**
2. From the Navigation pane of the active system, expand the **System** section.
3. Either select **High Availability** and then the **ConfigSync** tab or use the flyout menus to expand **High Availability → ConfigSync** and click **ConfigSync**.
4. Click the **Synchronize TO Peer** button for a push operation to BIG-IP #2.
5. At the **Synchronize this BIG-IP LTM to its failover partner** prompt, click **OK.**
   The synchronization process takes 15-60 seconds.
6. Verify your configuration was copied to the second System.

Expected Results and Troubleshooting

- At this point, the BIG-IP #1 and #2 system configurations should be similar. Verify that BIG-IP #2 has the same Virtual Servers, Pools, Profiles, Monitors and iRules as BIG-IP #1. The License, Hostname and Self IPs (Network / Self IPs) should be different.
- If the Self IPs are the same for both systems, verify the following:
  - The hostnames (System / Platform) should be different (bigip1… and bigip2)
- If BIG-IP #2 does not have Virtual Servers from BIG-IP #1, verify the following:
  - Were there errors during Synchronization? (System / Logs / System)
  - Did you Synchronize the wrong way? (from BIG-IP #2 to #1)

High Availability

Lesson Objective:

During this lesson, you will failover features of a redundant pair of BIG-IP systems.

Restoring BIG-IP #1 from previous Lab

1. After connecting to F5 Training Lab, open a browser to **https://192.168.1.245.**
2. When prompted, login as **admin** with a password of **admin.**
3. If you have an existing lab environment, skip to step 10 below.
4. If starting with a new lab environment, on the **Welcome / Setup Utility** screen click **Next**.
5. On both the **License** and **Resource Provisioning** screens click **Next**.
6. On the Setup Utility / Platform screen enter a **Host Name** of **bigip1.f5trn.com** and change **High Availability** setting to **Redundant Pair**.
7. Enter a **Root Account** password of **default** twice and an **Admin Account** password of **admin** twice and then click **Next**.
8. You will be prompted to login again because of changing the Admin password.
9. After logging in, click the **Finished** button under **Advanced Network Configuration**.
10. From the Navigation pane, expand the **System** section, then select **Archives**.
11. Click the **Module11_Lab_BIGIP1.ucs** archive and then click the **Restore** button. An **Ok** button appears to acknowledge the restore has started. It will take a minute, but watch this screen and you should see messages that your restore completed successfully. You might receive one error message but that is ok and is due to the F5 Training Lab environment only.
12. Because of the state of BIG-IP, we need to reboot so that our Licensing and Provisioning takes effect. Select **System / Configuration** and click the **Reboot** box under **Operations**.
13. Your configuration should be as if you had just finished all Module 10 labs. Please verify this is the case. BIG-IP #1 should be licensed and include five Pools, two iRules, five Virtual Servers, and Monitors assigned to some but not all Pool Members. No Pool Members should be marked Offline (red) or Disabled (black). It should have a hostname of **bigip1.f5trn.com** and Self IPs (Network / Self IPs) of **10.10.1.31, 10.10.1.33**, **172.16.1.31** and **172.16.1.33**.

Restoring BIG-IP #2 from previous Lab

1. After connecting to F5 Training Lab, open a browser to **https://192.168.1.246.**
2. When prompted, login as **admin** with a password of **admin.**
3. If you have an existing lab environment, skip to step 10 below.
4. If starting with a new lab environment, on the **Welcome / Setup Utility** screen click **Next**.
5. On both the **License** and **Resource Provisioning** screens click **Next**.
6. On the Setup Utility / Platform screen enter a **Host Name** of **bigip2.f5trn.com** and change **High Availability** setting to **Redundant Pair**.
7. Enter a **Root Account** password of **default** twice and an **Admin Account** password of **admin** twice and then click **Next**.
8. You will be prompted to login again because of changing the Admin password.
9. After logging in, click the **Finished** button under **Advanced Network Configuration**.
10. From the Navigation pane, expand the **System** section, then select **Archives**.
11. Click the **Module11_Lab_BIGIP2.ucs** archive and then click the **Restore** button. An **Ok** button appears to acknowledge the restore has started. It will take a minute, but watch this screen and you should see messages that your restore completed successfully. You might receive one error message but that is ok and is due to the F5 Training Lab environment only.
12. Because of the state of BIG-IP, we need to reboot so that our Licensing and Provisioning takes effect. Select **System / Configuration** and click the **Reboot** box under **Operations**.
13. Your configuration should be as if you had just finished all Module10 Labs. Please verify this is the case. BIG-IP #2 should be licensed and include five Pools, two iRules, five Virtual Servers, and Monitors assigned to some but not all Pool Members. No Pool Members should be marked Offline (red) or Disabled (black). It should have a hostname of **bigip2.f5trn.com** and Self IPs (Network / Self IPs) of **10.10.1.32, 10.10.1.33**, **172.16.1.32** and **172.16.1.33**.

Network Failover Lab

Objectives:

During this lab, you will configure network failover.

Determining State Prior to Configuration

1. Open an SSH session to each system, 10.10.1.31 and 10.10.1.32. Press **Enter** to update the prompt repeatedly. Note that both systems are in Active state because we haven't configured Network Failover yet.

Note: The F5 virtual environment does not support the use of hardware failover cables.

Network Failover Configuration and Testing

1. This feature is not synchronized, so you must configure **each system separately**.
2. Navigate to **System** / **High Availability** / **Network Failover**.
3. On BIG-IP #1, Enter the following in the **Configuration** section:

Network Failover	Check the box
Peer Management Address	192.168.1.246
Unicast	Configuration Identifier: peer_bigip2 Local Address: Self IP address 172.16.1.31 Remote Address: 172.16.1.32 Port: Blank (defaults to 1026)
Multicast	Leave Blank

4. When complete, click **Update**.

5. On BIG-IP #2, Enter the following in the **Configuration** section:

Network Failover	Check the box
Peer Management Address	192.168.1.245
Unicast	Configuration Identifier: peer_bigip1 Local Address: Self IP address 172.16.1.32 Remote Address: 172.16.1.31 Port: Blank (defaults to 1026)
Multicast	Leave Blank

6. When complete, click **Update**.
7. When both systems have been set, note that the systems change to active-standby mode. BIG-IP #2 should be the one to fallback to standby state because it is unit 2.

8. Normally you would remove the Ethernet cable but for remote labs we will disable “Network Failover” on unit #2.
9. How quickly did the standby system change to the active role also?
10. If disabling “Network Failover” on unit #2 does not cause it to go active then you may need to disable Network Failover on unit #1 also.
11. Note that when both systems are in active mode; both are trying to service all virtual servers, NATs and SNATs.
12. Again, normally we would now replace the Ethernet cable but for remote labs we will enable “Network Failover” again on both units.
13. Unit #2 should now fall back to standby state.

Force to Standby and Failover

1. On both BIG-IPs, navigate to **System** / **High Availability** / **Redundancy**.
2. Currently, BIG-IP #1 should be Active and BIG-IP #2 should be Standby.
3. On BIG-IP #1, click the **Force to Standby** button: Notice that BIG-IP #1 falls back to **Standby** state, and BIG-IP #2 takes over the **Active** roll.

Connection Mirroring Lab

Objective:

During this lesson, you will learn how to configure connection mirroring.

Lab Requirements:

A working Active / Standby redundant pair of BIG-IP's.

Create an ssh Pool

1. Create a Pool with the following characteristics, Configuration section:

Configuration Level	**Basic**
Name	**ssh_pool**
Health Monitors	**Leave Blank**

2. In the **Resources s**ection, enter the following:

Load Balancing Method	**Round Robin**
Priority Group Activation	**Disabled**
New Members **For each, enter Address and Service Port and press Add**	**172.16.20.1 port 22** **172.16.20.2 port 22** **172.16.20.3 port 22**

3. When complete, click **Finished.**

Create a Virtual Server that uses this pool

4. Create a Virtual Server with the following characteristics, **General Properties** section:

Name	**vs_ssh**
Destination	**10.10.1.100**
Service Port	**22 (or SSH)**
State	**Enabled**

5. In the **Configuration** section, accept all defaults.
6. In the **Resources** section, accept all defaults except the following:

Default Pool	**ssh_pool**

1. When complete, click **Finished.**

Synchronize the configuration

1. Synchronize from the same system (**System / High Availability / ConfigSync)** and click the **Synchronize TO Peer** button.

2. Click **OK** when prompted.

Testing before Mirroring

1. Using an SSH client, such as Putty, open an SSH session to: **10.10.1.100:22**.
2. Login as **student** / **student**.
3. Test your connection by typing `ls` <enter> or similar command.

Perform Failover

1. Force the Active system to standby (System / High Availability / Force to Standby).
2. Notice that the SSH connection has been lost.

Testing with Connection Mirroring enabled

1. From the same system's Navigation Pane, click **Local Traffic / Virtual Servers** and select the SSH virtual server.
2. Select **Advanced** from the **Configuration** menu.
3. Check the **Connection Mirroring** checkbox.
4. Click **Update** to set changes.
5. Synchronize from the same system (**System** / **High Availability** / **ConfigSync)** and click the **Synchronize TO Peer** button.
6. Click **OK** when prompted.

Establish a new SSH connection and Failover again

1. Using an SSH client such as Putty open an SSH session to: **10.10.1.100:22**.
2. Login as **student** / **student**.
3. Test your connection by typing `ls` <enter> or similar command.
4. Force the Active system to standby. (**System / High Availability / Force to Standby**).
5. Test your connection by typing `ls` <enter> or similar command. Note the connection is maintained.

Persistence Mirroring Lab

Objective:

During this lesson, you will learn how to activate persistence mirroring for a pool where simple persistence in enabled.

Lab Requirements:

You must have a virtual server and pool appropriate for persistence other than cookie persistence.

Behavior Prior to Configuring Persistence Mirroring

Configure Persistence, Establish an https session

1. From the Navigation Pane, expand the **Local Traffic** section.
2. Select **Virtual Servers** and the virtual server **vs_https.**
3. Select the **Resources** tab, and ensure that **Pr_Src_Persist** is still listed as the Default Persistence Profile.
4. Select **Local Traffic / Profiles / Persistence** and the **Pr_Src_Persist** profile. Set the **Timeout** value to **30** seconds and click **Update.**
5. Synchronize from the same system (**System** / **High Availability** / **ConfigSync / Synchronize TO Peer**).
6. Open a browser session to: **https://10.10.1.100**.
7. Ensure your session persists by hitting the <Ctrl>-F5 key combination several times.

View the Persistence Record

1. View the persistence records on both systems.
   a. From the Configuration Utility, Navigate to Overview / Statistics. In the Display Options section, choose Persistence Records.
   b. From the Command Line, enter: `b persist all show all`
2. On the active system, you should see a record. On the standby, you should not.
3. Re-enter this command several times and notice the **Age** of the record changes.
4. Let the **Age** count up to **30** seconds and then re-enter the command again. What happened to the persistence record?
5. Refresh **the https://10.10.1.100** browser session again and then re-enter the command again. Did the Age count start over?

Perform Failover

1. Force the Active system to standby. (**System** / **High Availability** / **Redundancy** / **Force to Standby**).
2. Refresh the session to **https://10.10.1.100**. While there is some chance the same node may be chosen, the https session does not persist to the same server. If it does seem to persist to the same node, failover again and test. You may need to refresh by pressing Ctrl-F5 to ensure the browser does not simply display its cache.

Configuring Persistence Mirroring and Testing Subsequent Behavior

1. From the Navigation Pane, select **Local Traffic** menu, **Profiles** option, **Persistence** tab, and then click the **Pr_Src_Persist** profile.
2. Check the **Custom** box for **Mirror Persistence**, check **Enabled**, and then click **Update**.
3. Synchronize from the same system (**System** / **High Availability** / **ConfigSync / Synchronize to Peer**).
4. Make sure to check that the **Mirror Persistence** option was set on the other System for the **Pr_Src_Persist** profile.

Re-establish the https session, failover and retest

1. Open a browser session to **https://10.10.1.100**.
2. Ensure your session persists by pressing the CTL-F5 several times.
3. Force the Active system to standby. (**System / High Availability / Redundancy / Force to Standby**).
4. Refresh the browser session to **https://10.10.1.100**. Notice that the https session does persist to the same server.
5. View the persistence records on both systems.
   a. From the Configuration Utility, Navigate to Overview / Statistics. In the Display Options section, choose Persistence Records.
   b. From the Command Line, enter: `b persist all show all`
6. You should see a persistence record on both systems.
7. Re-enter this command several times and notice the **Age** of the record for each system. Does the **Age** remain the same on both Systems?
8. Refresh the https://10.10.1.100 browser session again and then re-enter the command again. Explain the **Age** count on each system?