F5 Networks Training

Getting Started with BIG-IP

Part One: Administration

Lab Guide

July, 2017

Getting Started with BIG-IP Lab Guide

Part One: Administration

Lab Guide

Fourth Printing; July, 2017

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

Support and Contact Information

Obtaining Technical Support

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

Contacting F5 Networks

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

F5 Networks, Inc.
Corporate Office
401 Elliott Avenue West
Seattle, Washington 98119
T (888) 88BIG-IP
T (206) 272-5555
F (206) 272-5557
Training@f5.com

F5 Networks, Ltd.
United Kingdom
Chertsey Gate West
Chertsey Surrey KT16 8AP
United Kingdom
T (44) 0 1932 582-000
F (44) 0 1932 582-001
EMEATraining@f5.com

F5 Networks, Inc.
Asia Pacific
5 Temasek Boulevard
#08-01/02 Suntec Tower 5
Singapore, 038985
T (65) 6533-6103
F (65) 6533-6106
APACTraining@f5.com

F5 Networks, Inc.
Japan
Akasaka Garden City 19F
4-15-1 Akasaka, Minato-ku
Tokyo 107-0052 Japan
T (81) 3 5114-3200
F (81) 3 5114-3201
JapanTraining@f5.com

Legal Notices

Copyright

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

Trademarks

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

Materials

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

Patents

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

Table of Contents

Getting Started with BIG-IP Lab Guide

Lab 1: BIG-IP Administration

This lab corresponds with the activities presented in *Getting Started with BIG-IP: Part 1 – Administration*.

Estimated time for completion: 25 minutes

Lab Objectives

- Run the Setup utility and configure system access parameters
- Create a UCS archive of the BIG-IP system configuration.
- Create a qkview file, upload to BIG-IP iHealth for analysis, and review the diagnostics produced

Lab Requirements

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

Current BIG-IP Settings

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

Lab 1A: Set up the BIG-IP

Run the Setup utility

1. Click the **Firefox Web Browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at https://192.168.1.31.)
2. When prompted, log in with a username of **admin** and with a password of **admin**.
3. In the **Welcome** screen, click the **Next** link to access the Setup utility.
4. On the subsequent **Setup Utility** » **License** page, review the features that have been licensed and then click **Next**.

Verify Provisioning

5. On the **Resource Provisioning** page of the Setup utility, verify your provisioning settings match those listed in the table below. For these labs, the systems are already licensed and provisioned for Local Traffic Manager.

Setup Utility » **Resource Provisioning**		
Current Resource Allocation section		
	Management (MGMT)	**Small**
	Local Traffic (LTM)	**Nominal**
When complete, click…	**Next**	

Accept the BIG-IP Self-Signed Device Certificate

6. After provisioning is complete, the **Device Certificates** page in the Setup Utility is displayed. We will be using the BIG-IP system's self-signed certificate in this lab. Note the expiration date for the certificate. Click the **Next** button to continue.

Verify Platform General Properties

7. In the **General Properties** section of the next page, configure general properties and administrative access usernames/passwords. Some fields may already contain the correct values. Leave the default values for the fields not mentioned in the table below.

Setup Utility » Platform		
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: **default1** Confirm: **default1**
	Admin Account	Password: **admin1** Confirm: **admin1**
When complete, click	**Next**	

After clicking the Next button in the previous step, you will be logged out of BIG-IP. A message prompting you to log back in will be displayed. Click OK to proceed.

8. Log back in to BIG-IP as user **admin** with password **admin1**. You should be taken directly to the **Setup Utility** » **Network** page.

Configure the Network

9. Continue the Setup utility by performing a Standard Network Configuration. Click the **Next** button under the **Standard Network Configuration** heading.

Configure Redundant Device Wizard options

10. Accept these default settings to configure the **Redundant Device Wizard Options**, then click **Next**.

Configure Self IPs, VLANs, and High Availability

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

Setup Utility » VLANs		
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 Tag ID	**auto**
	Interfaces	VLAN Interfaces: Select **1.2** Tagging: Select **Untagged** Click the **Add** button
When complete, click…	**Next**	

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

Setup Utility » VLANs		
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**
	Floating IP	Address: **10.10.1.33** Port Lockdown: **Allow 443**
External VLAN Configuration section		
	VLAN Tag ID	**auto**
	Interfaces	Interfaces: Select **1.1** Tagging: Select **Untagged** Click the **Add** button
When complete, click…	**Next**	

13. Configure the high availability network to use the existing VLAN **internal**.

Setup Utility » VLANs		
High Availability Network Configuration section		
	High Availability VLAN	Click the **Select existing VLAN** radio button
	Select VLAN	**internal**
When complete, click…	**Next**	

Configure Network Time Protocol

14. Leave this page with its default settings, and click the **Next** button to continue.

Configure Domain Name Server

15. Leave this page with its default settings, and click the **Next** button to continue.

Configure ConfigSync

16. Accept the default settings for **ConfigSync** configuration, as shown below:

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

Configure Unicast and Multicast Failover settings

17. Accept the default settings for **Failover Unicast Configuration** and **Failover Multicast Configuration**, as shown below:

Setup Utility » **Failover**		
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. Accept the default primary and secondary local mirror address settings for **Mirroring Configuration**.

Setup Utility » **Mirroring**		
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

19. You have now configured the network interfaces required to support a standard BIG-IP configuration.
20. Click the **Finished** button under the **Advanced Device Management Configuration** heading. There should be a message at the top of the page indicating **Setup Utility Complete.**

Lab 1B: Create a UCS Archive of Your Configuration

1. Navigate to **System » Archives** to create a backup of your current configuration.

Configuration Utility	
System » **Archives** then click **Create**	
General Properties section	
File Name	**lab_base**
When complete, click…	**Finished**, then click **OK** when the archive is complete

2. Download your new UCS backup to your Ubuntu client.

Configuration Utility	
System » **Archives** then click **lab_base.ucs**	
General Properties section	
Archive File	Click **Download: lab_base.ucs**, then click **OK** to save when prompted.

Lab 1C: Generate a qkview File

If you do not have an iHealth account, please register for one at **iHealth.f5.com** before beginning this lab. You will need a valid email address to receive the registration confirmation email in order to finish creating your account. To register for an iHealth account, click on **Register for an Account** from iHealth.f5.com.

Generate a qkview file on your BIG-IP

1. Navigate to **System » Support**.
2. Click **New Support Snapshot**.
3. In the Support Snapshot section, click the pulldown menu next to Health Utility and select **Generate Qkview**.
4. Click **Start**.

The qkview process may take several minutes to complete. When it does, continue with the steps below.

Download the qkview file

3. Wait until the QKView displays "Complete."
4. Click the **Download** button.

A confirmation window will open, prompting you to either open the file or save it.

5. Select the **Save File** radio button and click **OK**.
6. Click the **Downloads** arrow icon in your Firefox browser to see a list of downloaded files.

7. Identify the downloaded qkview file in the list. The file should have a name similar to **support.qkview**.

   If you were to open a case with F5 Support, they may ask you to upload a qkview file to iHealth. If this were the case, you would re-name your qkview file to include the F5 Support case number.

Upload the qkview file to iHealth

8. Open a browser tab by clicking the plus icon from Firefox, and connect to **ihealth.f5.com**.
9. Sign in using your iHealth account credentials.
10. Click the **Upload** button.
11. Click the **Choose** button, navigate to the **Downloads** folder in your Ubuntu client, and double-click to select the qkview that you identified in step 7.
12. Click the **Upload QKView(s)** button to continue. The BIG-IP iHealth system may take several minutes to upload and extract the file.
13. After the analysis is complete, you will see your QKView listed in the **My QKViews** menu. You will be able to easily identify it by looking at the information in the **Generation Date** column.
14. Click on your QKView to view the results of your qkview file analysis.

Review diagnostic information

15. Do you have any high priority diagnostic results? What are the recommended actions?

Execute Commands against the qkview output

16. Click on the **Commands** menu in the iHealth window.
17. Click the **tmsh** folder.
18. Expand the **net** folder.
19. Run the following commands by clicking on them from the list:
    - list /net self all-properties
    - show running-config /net self
20. Explore iHealth's ability to display data graphically by going to **Graphs > Standard**. Explore how you can view the **Memory Used** and **System CPU Usage** over different time periods.

21. Add a comment to your qkview file. In the upper right area of the page, click the plus icon next to **Comments** and enter: **This is a test qkview**, then **Save**.

    Remember: Whatever comments you put here are visible by F5 Technical Support staff.

22. View and customize your iHealth settings at **Options > Settings** (upper right corner of the page).

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