Agility 2018 Hands-on Lab Guide

F5 201 Certification BIG-IP Administration

F5 Networks, Inc.
# Contents

1 Getting Started
   1.1 Lab Topology .................................................. 5
   1.2 Lab Basics and Prep ........................................... 6

2 Class - F5 201 Certification BIG-IP Administration ................................................. 9
   2.1 Module – Packet Processing and Virtual Servers .................................................. 9
   2.2 Module – Virtual Server and Pool Behavior and Status ........................................ 13
   2.3 Module – Troubleshooting the BIG-IP ................................................................. 19
   2.4 Module – Support and Analytics ......................................................................... 22
   2.5 Module – Managing the BIG-IP ......................................................................... 26
   2.6 Module – Modify and Manage Pools and Virtual Servers ..................................... 28
   2.7 Module – Appendix I - Answer Key ................................................................. 30
Getting Started

The purpose of this guide is to provide a sampling of hands-on exercises to better understand the subjects outlined in the 201-TMOS Administration Exam Blueprint.

The Ravello F5 vLab (virtual lab environment) is an F5-community supported tool. Please DO NOT contact F5 Support for assistance with the vlab. For help with the setup of the vLab or running a demonstration, you should contact your F5 Channel Account Manager (CAM).

To set up your own lab environment on your own platform. Please refer to vLab Setup and Configuration Guide for detailed instructions. This guide is included in the Partner_vLab_Package on https://downloads.f5.com.

Note: All work for this lab will be performed exclusively from the lab jumphost. No installation or interaction with your local system is required.

1.1 Lab Topology

Each student will have a BIG-IP VE environment with IP addressing as below:
1.2 Lab Basics and Prep

Accessing the lab environment.

1. Open a browser and go to `http://api.f5labs.io/<instructor_uri>/X` (where X is your student number)
2. Look for the xubuntu-jumpbox-vxx. You will use the xubuntu jumpbox for all the labs. (see below)
1. You can click on **RDP** to RDP to the Xubuntu jumpbox or you can select the **CONSOLE** link and access the jumpbox via your browser. **The CONSOLE link requires you turn off pop-up blockers.**
You are the administrator of a pair of BIG-IPs with a number of virtual servers pre-configured. In this lab you will determine how traffic is processed and take a look at various virtual server states and some reasons a virtual server may not be working.

Expected time to complete: **3 hours**

### 2.1 Module – Packet Processing and Virtual Servers

**Objective:**

- Objective 1.01
  - Given a connectivity-troubleshooting situation, consider the packet and virtual server processing order.
  
  Estimated completion time: 30 minutes

#### 2.1.1 Lab – Lab Preparation and Packet Processing

**Task – BIG-IP VE System Configuration**

Access your BIG-IP and verify it is configured properly.

1. Open a new Web browser and access [https://10.1.1.245](https://10.1.1.245). Log into the BIG-IP VE system using the following credentials: Username: `admin` Password: `admin`

2. Check the upper left-hand corner and ensure you are on the active device the status should be **ON-LINE (ACTIVE)**. Most deployments are active-standby and either device could be the active device.

3. On the **System >> Resource Provisioning** page ensure **Local Traffic (LTM)** and **Application Visibility and Reporting (AVR)** modules are provisioned.

4. Go to **Local Traffic >> Virtual Servers** and verify your virtual server states. They should match the graphic.
Task – Open BIG-IP TMSH and TCPDump session

In this task, you will open two SSH sessions to the BIG-IP. One for TMSH commands and the other for tcpdump of the client-side network.

1. Open command/terminal window (window1) from the shortcut bar at the bottom of the jumpbox.
   - `ssh root@10.1.1.245`  
     **Password:** default

2. Use tcpdump to monitor traffic from the client (10.1.10.51) destined to ftp_vs (10.1.10.100)
   - `tcpdump –nni client_vlan host 10.1.10.51 and 10.1.10.100`

3. Open command/terminal window (window2).
   - `ssh root@10.1.1.245`

4. Use tmsh to display connection table, at the Linux command prompt type:
   - `tmsh`

5. At the TMOS prompt (tmos)#
   - `show sys connection`

**Attention:**  
Q1. Do you see any connections from the jumpbox 10.1.1.51 to 10.1.1.245:22?  
Q2. Why are the ssh management sessions not displayed in connection table?

Task – Establish ftp connection

In this task you will open a third terminal window and establish an FTP session through the ftp_vs virtual server. With the connection remaining open you will view the results in window1 (tcpdump) and window2 (tmsh).

1. Open a third terminal window on the Xubuntu client (window3).
   - `ftp 10.1.10.100`

In window1 you should see something similar to the tcpdump captured below.
**Attention:** Q1. In the tcpdump above, what is client IP address and port and the server IP address port?

1. In window2 (tmsh) run the show sys conn again, but strain out the noise of other connections (mirrored and selfIP) by just looking at connections from your jumpbox.

   - `show sys conn cs-client-addr 10.1.10.51`

   The connection table on window2 will show the client-side and server-side connection similar to below

   ```
   !@
   show sys connection cs-client-addr 10.1.10.51
   
   sys::Connections
   10.1.10.51:57184 10.1.10.100:21 10.1.20.249:57184 10.1.20.11:21 tcp 217 (tm: 1) none
   Total records returned: 1
   ```

**Attention:** Q2. What is source ip and port as seen by ftp server in the example above?

Q3. What happened to the original client IP address and where did 10.1.20.249 come from?

**Hint:** You will have to review the configuration of ftp_vs to determine the answer to this question.

### 2.1.2 Lab – Packet Filters

**Task – Create a packet filter**

You are going to test how packet filters impact packet processing by creating a packet filter to block ftp connections to 10.1.10.100. Follow these steps to complete this task:

1. Go to **Network > Packet Filters > Rules** and Create a filter using the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Block_ftp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>First</td>
</tr>
<tr>
<td>Action</td>
<td>Discard</td>
</tr>
<tr>
<td>Destination Hosts</td>
<td>10.1.10.100</td>
</tr>
<tr>
<td>Destination Port</td>
<td>21 (FTP)</td>
</tr>
<tr>
<td>Logging</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

*Make sure you select Add after enter a host/network or a port.*

**Task – Test the FTP Packet Filter**

Ensure ftp connection is established. (See 2.1.3. Task – Establish ftp connection)
1. Go to Network > Packet Filters > General and select Enable and then Update.

Attention: Q1. Was the existing ftp connection in the connection table affected? Why?

2. Quit ftp and clear virtual server statistics by going to Local Traffic > Virtual Servers > Statistic, select the virtual server and hit Reset.

3. Attempt to establish an ftp connection to 10.1.10.100. Note tcpdump capture in Window1.

Attention: Q2. Was ftp connection successful? Why?
Q3. What did tcpdump reveal? Did the connection timeout or reset?
Q4. What did virtual server statistics for ftp_vs reveal? Why are counters not incrementing?
Q5. Prioritize the packet processing order below from 1-7:

Virtual Server___ SNAT___ AFM/Pkt Filter___ NAT___ Existing Connections___ Self IP___ Drop ___

4. Review the Packet Filter Logs and Packet Filter Statistics, then disable the Packet Filters.
   - Go to Network > Packet Filters > Statistics and review the information.
   - Go to System > Logs > Packet Filters and review the information.
   - Go to Network > Packet Filters > General and select Disable and then Update.

2.1.3 Lab – Virtual Server Packet Processing

Task 1 – Create additional Virtual Servers

Create a wildcard virtual server and pool, test and observe various traffic under different configurations to determine how virtual servers process new inbound connections. You will be using tcpdump from window1, virtual server statistics, as well as a browser to determine behavior.

1. Create wildcard_vs 10.1.10.100:* with TCP profile, Automap and wildcard_pool of 10.1.20.11:*  
   - To create the wildcard pool, go to Local Traffic > Pools > Pool List and select Create.

<table>
<thead>
<tr>
<th>Name</th>
<th>wildcard_pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>10.1.20.11</td>
</tr>
<tr>
<td>Port</td>
<td>*</td>
</tr>
</tbody>
</table>

Don’t forget to Add the pool member to the New Members box before you hit Finished.

2. To create the wildcard virtual server, go to Local Traffic > Virtual Server and select Create.

<table>
<thead>
<tr>
<th>Name</th>
<th>wildcard_vs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>10.1.10.100</td>
</tr>
<tr>
<td>Service Port</td>
<td>*</td>
</tr>
<tr>
<td>Source Address Translation</td>
<td>Automap</td>
</tr>
<tr>
<td>Default Pool*</td>
<td>wildcard_pool</td>
</tr>
</tbody>
</table>

Don’t forget to hit Finished.
**Task – Testing Virtual Server Packet Processing Behavior**

Many of your virtual servers have the same virtual address. You will now test various behaviors.

2. Observe connection statistics (VS stats) for each of the following
   - Browse to `http://10.1.10.100:8080`

   **Attention:** Q1. Which VS is used for web traffic over port 8080?
   - FTP to 10.1.10.100

   **Attention:** Q2. Which VS is used for FTP traffic?
   - Browse to `http://10.1.10.100`

   **Attention:** Q3. Which VS is used for this web traffic the default HTTP port? What port was used?

3. Clear virtual server stats.
4. Modify the `wildcard_vs` to only allow connections from a Source of 10.1.10.0/24
5. Browse to `http://10.1.10.100`
   - Observe connection statistics (VS stats)

   **Attention:** Q4. Which VS is used for web traffic?

7. Modify `wildcard_vs` to include the default Source of 0.0.0.0/0.

**2.2 Module – Virtual Server and Pool Behavior and Status**

**Objective:**

- Objective 1.02-1.06
  - Identify the reason a virtual server is not working as expected
  - Identify the reason a pool member has been marked down by health monitors
  - Identify a pool member not in the active priority group
  - Identify traffic diverted due to persistence record
– Identify the current configured state of the pool member
– Identify a persistence issue

Estimated completion time: 45 minutes

2.2.1 Lab – Virtual Server Status

Task – Test Disabled Virtual Servers

In this task, you will disable and enable various virtual servers and note the behavior.

1. Disable www_vs from the Virtual Server List or from within the www_vs GUI interface.
2. Open Local Traffic > Virtual Servers and hover over status icons.
3. From window2 (TMSH) type: show ltm virtual or show ltm virtual www_vs

Attention:
Q1. What is the Availability of www_vs? What is the State?
Q2. What symbol is used to represent www_vs status?
Q3. Would you expect browsing to http://10.1.10.100 to work?
Q4. Can you ping the virtual IP?

4. Clear virtual server stats and browse to http://10.1.10.100
5. Observe the tcpdump (window1) and connection statistics in the Virtual Server statics GUI interface.

Attention:
Q5. Did the site work? What did the tcpdump show?
Q6. Did statistics counters for any virtual increment?
Q7. Why do you think the wildcard_vs didn’t pick up the packets?

6. Disable wildcard_vs and note the State and Availability of the virtual servers.

Attention:
Q8. What symbol is used to represent wildcard_vs? Why is symbol a square?
Q9. What is the Reason given for current state?

7. Establish ftp connection to 10.1.10.100 and ensure successful login.
8. Disable ftp_vs.

Attention:
Q10. Does ftp session still work? Why?

9. Open another window and establish ftp connection to 10.1.10.100.

Attention: Q11. Did new ftp session establish connection? Why not?
**Important:** Make sure all virtual servers are Enabled before continuing.

---

**Task – Virtual Server Connection Limits and Status**

In this task, you will set the connection limit for the FTP virtual server to 1 and note the status and behavior of different connection scenarios.

1. Modify `ftp_vs` for connection limit of 1. The **Connection Limit** option can be found under the **Advanced** virtual server menus.
2. Establish ftp connection to **10.1.10.100** and hold the logon open.

<table>
<thead>
<tr>
<th>Attention:</th>
<th>Q1. Does FTP session work?</th>
<th>Q2. What is the virtual server symbol and status of <code>ftp_vs</code>?</th>
</tr>
</thead>
</table>

3. Open another window and establish a second ftp connection to 10.1.10.100.

| --- | --- | --- | --- |

---

**2.2.2 Lab – Pool Member and Virtual Servers**

**Task – Create a new monitor**

In this task, you will determine the effects of monitors on the status of pools members.

1. Create `mysql` monitor for testing.
   - Go to **Local Traffic > Monitors** and select **Create**.

<table>
<thead>
<tr>
<th>Name</th>
<th>mysql_monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Monitor</td>
<td>mysql</td>
</tr>
<tr>
<td>Interval</td>
<td>15</td>
</tr>
<tr>
<td>Timeout</td>
<td>46</td>
</tr>
</tbody>
</table>

**Task – Effects of Monitors on Members, Pools and Virtual Servers**

1. Go to **Local Traffic -> Pools -> www_pool** and assign `mysql_monitor` to the pool.
2. Observe Availability Status of **www_pool**. The pool status momentarily changes to **Unknown**.

<table>
<thead>
<tr>
<th>Attention:</th>
<th>Q1. Since the <code>mysql_monitor</code> will fail, how long will it take to mark the pool offline?</th>
</tr>
</thead>
</table>

3. Go to **Local Traffic > Pool > www_pool** and then **Member** from the top bar and open member **10.1.20.13:80** and note the status of the monitors.
4. Open Local Traffic -> Network Map -> Show Map

Attention: Q2. What is the icon and status of www_vs?
Q3. What is the icon and status of www_pool?
Q4. What is the icon and status of the www_pool members?
Q5. How does the status of the pool configuration effect the virtual server status?

5. Clear the virtual server statistics.
7. Disable www_vs and clear the statistics and ping the virtual server.

Attention: Q6. What is the icon and status of www_vs?

8. Browse to http://10.1.10.100 and note the browser results, statistics and tcpdump.

Attention: Q7. Did traffic counters increment for www_vs?
Q8. What is the difference in the tcpdumps between Offline (Disabled) vs Offline (Enabled)?

Make sure all virtual servers are Enabled before continuing.

Task – More on status and member specific monitors

1. Go to Local Traffic > Pool > www_pool and then Member from the top bar and open member 10.1.20.13:80. Enable the Configuration: Advanced menus.

Attention: Q1. What is the status of the Pool Member and the monitors assigned to it?

2. In Health Monitors select Member Specific and assign the http monitor and Update.
3. Go to the Network Map.

Attention: Q2. What is the status of www_vs, www_pool and the pool members? Why?


Attention: Q3. Did the site work?
Q4. Which www_pool members was traffic sent to?

Important: After completion of this task remove mysql_monitor from the www_pool health monitors.
2.2.3 Lab – Load Balancing

Task – Load Balancing

In the task, you will look and the various effects of different load balancing configurations.

1. Open the **www_pool Members** tab.

2. Note the load balancing method on the pool and the **Ratio** and **Priority** settings on the members. Select each member and update them to the following:

<table>
<thead>
<tr>
<th>Member</th>
<th>Ratio</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.20.11</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>10.1.20.12</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>10.1.20.11</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

3. Go to Local **Traffic > Pools > Statistics** and clear the **www_pool** statistics.

4. Browse to **http://10.1.10.100** and refresh or <ctrl> F5 several times.

**Attention:**

Q1. Which **www_pool** members was traffic sent to?

Q2. Did member **10.1.20.11** receive the most traffic? Why not?

5. Under the **Members** tab change **Load Balancing Method** to **Ratio (member)** then **Update**.

6. Clear stats for **www_pool** and browse **http://10.1.10.100** several times.

**Attention:**

Q3. Which **www_pool** members was traffic sent to?

Q4. Did member **10.1.20.11** receive the most traffic?

Task – Priority Group Activation

1. Change **Priority Group Activation** to less than 2 and **Update**.

2. Clear stats for **www_pool** and browse to **http://10.1.10.100**.

**Attention:**

Q1. Which **www_pool** members was traffic sent to?

3. On the pool statistics page, select member **10.1.20.11:80** and change the **State** to **Disable**.

4. Clear the statistics for the **www_pool** and browse to **http://10.1.10.100** several times.

**Attention:**

Q2. Which **www_pool** members was traffic sent to? Why?

Q3. Would the results have been different if 10.1.20.11:80 had been marked offline or marked with a yellow triangle?
Important: Once you have complete the lab, change the Load Balancing Method to Round Robin, Priority Group to Disabled, and Enable pool member 10.1.20.11:80

Task – The Effects of Persistence on Load Balancing

In this task, you will enable persistence on the www_vs and see the effects of persistence on load balancing. You will also see where to view persistence records that are maintain by the BIG-IP.

1. Enable a Persistence Profile on www_vs by opening the virtual server and selecting the Resources tab.

2. Assign the following persistence profiles:

<table>
<thead>
<tr>
<th>Default Persistence Profile</th>
<th>cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fallback Persistence_Profile</td>
<td>source_addr</td>
</tr>
</tbody>
</table>

If you see an error requiring an HTTP profile, go to Properties and assign the default HTTP profile.

Attention: Q1. Why was a http profile required?


Attention: Q2. Was traffic evenly distributed to all www_pool members? Why not?

4. In the web page under HTTP Request and Response Information is Display Cookie link.
   • Select Display Cookie to view the cookie created by the BIG-IP.
   • Open Statistic > Module Statistics > Local Traffic > Persistence Records.
   • Click on pool member displayed on persistence record and Disable the pool member.
   • Browse to http://10.1.10.100.

Attention: Q3. Did you persist to the Disabled member? Why?

5. Change status of persisted pool member to Forced Offline.


Attention: Q4. Does traffic continue to persist to the member Forced Offline?

Q5. If cookies were disable on your browser would persistence still work? Why?

Alternate method to display persistence is: tmsh show ltm persistence persist-records.
2.3 Module – Troubleshooting the BIG-IP

Objective:

- Objectives 2.01-2.05
  - Perform an End User Diagnostic per F5 documentation and collect the output
  - Interpret the LCD Warning Messages
  - Identify a possible hardware issue within the log files
  - Force an active unit to standby under the appropriate circumstances
  - Understand the relationship between interfaces, trunks, VLANs and their status/statistics
- Objectives 3.01-3.02
  - Perform a packet capture within the context of a performance issue
  - Use BIG-IP tools in order to identify potential performance issues
- Objectives 4.01-4.03
  - Verify remote connectivity to the box in order to determine the cause of a management connectivity issue
  - Check and interpret port lockdown settings and packet filters in order to determine the cause of a management connectivity issue
  - Given the use of a remote authentication server, verify proper DNS and NTP settings in order to diagnose a connectivity issue

Estimated completion time: 20 minutes

2.3.1 Lab – Trouble-shooting Hardware

Review what you have learned about troubleshooting hardware.

Note:  SKIP THIS LAB 2.3.1 - This section does not require the lab environment so can be completed later.

Task – End User Diagnostics

**Attention:**  Q1. What three methods are available for running EUD on F5 Hardware?

Q2. How do you determine EUD version?

Q3. What is the filename and location of the EUD output?

Task – LCD Panel
Attention: Q1. How do you halt the unit via the LCD panel?
Q2. Holding the X for 4 seconds does what?
Q3. Holding the Check button for 4 seconds does what?

Task – Hardware Log Files

Attention: Q1. What is the filename and location of the logs for LTM?
Q2. Where will power supply, fan and hard disk related issues be logged?

Task – HA and Failover

Attention: Q1. Is failover sometimes used to determine issues related to hardware or software?
Q2. How do you initiate failover to standby unit?
Q3. What persistence profile cannot be mirrored?
Q4. What two connections types are re-mirrored after failback?
Q5. When would you recommend using connection mirroring?
Q6. Where is connection mirroring configured?
Q7. Where is persistence mirroring configured?
Q8. What tmsh command is used to view mirrored connections?
Q9. What tmsh command is used to view mirrored persistence?
Q10. What can be the cause of primary unit returning to active state after initiating failover to standby?

2.3.2 Lab – tcpdump Packet Capture

In this exercise are going to perform tcpdump packet captures and review the results.

Task 1 – Packet Captures of multiple interfaces simultaneously

1. Open SSH session window1, and enter on one line to perform capture in background:
   • tcpdump –ni client_vlan –eXs 0 –w /var/tmp/dump.cap & tcpdump –ni server_vlan –eXs 0 –w /var/tmp/dump2.cap &
2. Browse to http://10.1.10.100
3. Enter the following commands to stop captures:
   • Type fg then <crtl> c
   • Repeat, type fg then <crtl> c
4. Enter the following command to read packet captures
   • tcpdump –r /var/tmp/dump.cap & tcpdump –r /var/tmp/dump2.cap
Attention: Q1. What is the alternate method for capturing two interfaces simultaneously?
Q2. What interface does 0.0 represent?
Q3. What interface typically represents the management interface?
Q4. What is recommended method for packet captures on high load system?
Q5. Will tcpdump capture PVA accelerated traffic?

2.3.3 Lab – Performance Statistics

Task 1 – Observing performance statistics

1. Open Statistics >> Performance page

Note: Stats are available for System, Connections, Throughput and Cache

Attention: Q1. What is the longest time interval available for performance statistics?

2.3.4 Lab – Connectivity Troubleshooting

Task 1 – Connectivity troubleshooting tools

1. Disable all virtual servers with the 10.1.10.100 virtual address and clear stats. Ping 10.1.10.100.

Attention: Q1. Was echo response received?
Q2. What is the status of the virtual servers?

2. The purple_vs is currently Offline (Enabled). Ping the virtual at 10.1.10.105.

Attention: Q3. Was echo response received?

2.3.5 Lab – Self IP Port Lockdown and more

Task 1 – Effects of Port Lockdown

1. Ping 10.1.10.245

Attention: Q1. Was echo response received?

2. SSH to 10.1.10.245
3. Open Network > Self IPs > 10.1.10.245 and change Port Lockdown to Allow Defaults
4. SSH to 10.1.10.245
5. Browse to https://10.1.10.245

   **Attention:** Q2. Was ssh successful? Why not?

3. Open Network > Self IPs > 10.1.10.245 and change Port Lockdown to Allow Defaults
4. SSH to 10.1.10.245
5. Browse to https://10.1.10.245

   **Attention:** Q1. Did SSH work? Did browsing work?
   Q2. What other ports are opened when you select Allow Defaults.

6. Open Network > Self IPs > 10.1.10.245 and change Port Lockdown to Allow Custom and add Port 22
7. SSH to 10.1.10.245
8. Browse to https://10.1.10.245

   **Attention:** Q3. Did SSH work? Did browsing work?

**Task 2 – Effects of Port Lockdown**

1. Open System >> Platform
2. On SSH IP Allow > Specify Range of 10.1.1.10-20

   **Attention:** Q4. Does existing SSH window still work?

3. Open new SSH session to 10.1.1.245

   **Attention:** Q5. Was new ssh session established?

**Task 3 – Check DNS and NTP are configured properly**

1. Verify the DNS and NTP configuration and test DNS.
   - Go to System >> Configuration >> Device >> General and review the DNS and NTP setting
2. In BIG-IP command line terminal window (window 2) test DNS from the CLI or TMSH enter:
   - dig pool.ntp.org

**2.4 Module – Support and Analytics**

**Objective:**
- Objective 5.01
Identify the appropriate supporting components and severity levels for an F5 support ticket

- Objective 6.01-6.04
  - Review the network map in order to determine the status of objects
  - Use the dashboard to gauge the current running status of the system
  - Review log files and identify possible events
  - Use iApps Analytics to gauge the current running status of application services

Estimated completion time: 45 minutes

2.4.1 Lab – Support, Status and Logs

Task – Qkview and iHealth

1. Open System->Support page.
2. Ensure QKView is selected then click Start.
3. Download snapshot file and upload ihealth.f5.com (login is required).

<table>
<thead>
<tr>
<th>Attention:</th>
<th>Q1. Are logs associated with qkview?</th>
</tr>
</thead>
</table>

4. From ssh window run qkview

<table>
<thead>
<tr>
<th>Attention:</th>
<th>Q2. Where is default filename and location of qkview output?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q3. Where is the default filename and location of core dump?</td>
<td></td>
</tr>
<tr>
<td>Q4. What is Severity and Condition for unit failure in active/standby pair?</td>
<td></td>
</tr>
<tr>
<td>Q5. If support case was opened online with Severity 4 and no call has been received in a week. What should you do?</td>
<td></td>
</tr>
<tr>
<td>Q6. What is the procedure to escalate support case?</td>
<td></td>
</tr>
</tbody>
</table>

Task – Network Map

1. Explain status icons of objects on network map.
   - Open Local Traffic > Network Map and hover over icons and observe status info.
   - Ensure all icons are green. If not, then troubleshoot.

   *Note the top-down status relationship between VS, pools, pool members and nodes.*

<table>
<thead>
<tr>
<th>Attention:</th>
<th>Q1. What is a node?</th>
</tr>
</thead>
</table>

2. Open Local Traffic > Nodes and disable node 10.1.20.11.
3. Attach irule to virtual server via Network Map.
   - Select www_vs from Network Map.
   - Select Resources > Manage irules.
   - Enable _sys_https_redirect irule and click Finished.

   **Attention:** Q4. Where is irule reflected on Network Map?

**Task - Dashboard**

1. Observe Dashboard statistics
   - Log on to the BIG-IP GUI using Firefox and go to Statistics >> Dashboard

   **Attention:**
   Q1. What is longest duration available for reporting?
   Q2. How can report be exported?

**Task 4 – Log files**

1. Interpret the LTM log file
   - Open ssh window1 and enter the following command:
     - `tail -f /var/log/ltm`

2. Disable ftp_vs

   **Attention:** Q1. Was alert logged?

3. Go to System > Logs > Local Traffic

   **Attention:** Q2. Was the alert logged here?

4. From ssh window 1 enter <CTRL> C and at the CLI prompt enter:
   - `grep alert /var/log/ltm`
   - `grep www_pool /var/log/ltm`

   **Attention:** Q3. What command is needed to find all instances of err in /var/log/ltm
2.4.2 Lab – iApps and Analytics

Task 1 – Create and iApps and add Analytics

As you saw in the first lab, Application Visibility and Reporting has already been provisioned. You are going to create an analytics profile and attach it to an HTTP iApp application you will create.

1. Open Local Traffic >> Profiles >> Analytics page.
2. Create an analytics profile using the following information, and then click Finished.

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>custom_analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collected Metrics</td>
<td>Max TPS and Throughput Page Load Time</td>
</tr>
<tr>
<td>Collected Entities</td>
<td>URLs, Countries, Client IP Addresses, Client Subnets, Response Codes, User Agents, Methods</td>
</tr>
</tbody>
</table>

1. Go to iApps >> Application Services and select Create.
2. Select the f5.http template, name it iapp_lab and review the Basic selections in the Template Options section set the configuration mode to Advanced – Configure advanced options
3. Build the iApp using the following information:

<table>
<thead>
<tr>
<th>Virtual Server IP</th>
<th>10.1.101.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server Port</td>
<td>80</td>
</tr>
<tr>
<td>FQDN</td>
<td>iapp.f5demo.com</td>
</tr>
<tr>
<td>Pool member 1</td>
<td>10.1.20.14:80</td>
</tr>
<tr>
<td>Pool member 2</td>
<td>10.1.20.15:80</td>
</tr>
<tr>
<td>Analytics Profile</td>
<td>custom_analytics</td>
</tr>
</tbody>
</table>

1. Review the status and components built by the iApp.
2. From both the Chromium and Firefox browsers go to http://10.1.10.110 and refresh the page several times and the select the following links from the page on each browser.
   - Request and Response Headers Allowed (review the request and response headers)
   - HTTP Compress Example
   - Multiple Stream Example

   It may take up to 10 minutes for Analytic statistics to be available.

**Attention:** Q1. Did both pool members respond? Why?

3. Go to Statistics >> Analytics >> HTTP and review the information.
Attention: Q2. Can you determine which page took the longest to load?

4. Go to Local Traffic >> Pools and attempt to add 10.1.20.13:80 to the iapp_lab_pool.

Attention: Q3. Could you add the pool member? Why?

Q4. Can you add the custom_analytics profile to the ftp_vs? Why?

2.5 Module – Managing the BIG-IP

Objective:

• Objective 7.01-7.08
  – Create and restore a UCS archive under the appropriate circumstances
  – Identify which high-level tasks can be automated using BIG-IQ
  – Manage software images
  – Given an HA pair, describe the appropriate strategy for deploying a new software image
  – Understand the processes of licensing, license reactivation, license modification and add-ons
  – Identify which modules are licensed and/or provisioned
  – Explain how to create a user
  – Explain how to modify user properties

Estimated completion time: X minutes

2.5.1 Lab – UCS, BIG-IP Archive

Task – Create UCS Archive Files

1. Open System > Archives page.
2. Create new archive backup_labs_1_to_4

Attention: Q1. What extension must Archive have?
Q2. What is the default location for ucs files?
Q3. What is command for loading ucs file?
Q4. What issues will occur by restoring ucs file on RMA device?
2.5.2 Lab – Upgrading a BIG-IP Device Service Clusters (DSC)

Task – Upgrading software

Prior to any upgrade, you would want to backup your device and then synchronize your changes. In the upper left corner, you should see Changes Pending due to the changes you have made to bigip01.f5demo.com.

#. Click on Changes Pending or go to Device Management >> Overview and select bigip01.
#. The Sync Device to Group button should already be selected. Hit the Sync button at the bottom.

1. Sometime sync get slightly off, if your sync fails select Overwrite Configuration and try again.

Attention: Q1. You are about to start your upgrade to 12.1, which device will you upgrade first?

2. On the appropriate device go to System >> Software Management
3. Select the v12.1.2 image and hit Install.
4. In the Volume set name selection enter upgrade.
   You could also have picked a volume, but for the lab you are creating a new one.

Attention: Q2. True or false? Once the install is complete, the BIG-IP will automatically reboot to the new volume.
Q3. What steps would be required to complete the upgrade?

2.5.3 Lab – BIG-IQ

Task – Peruse BIG-IQ

In this lab you will talk a short walk through the BIG-IQ interface and perform a few tasks.

1. Logon to the BIG-IQ at https://10.1.1.235 Username: admin Password: admin

Attention: Q1. What BIG-IPs are being managed?

2. Select the Backups pane, select “+” and the Add Backup
4. Go to BIG-IQ >> ADC and review the information in the panels.

Attention: Q2. Where are configurations currently being display from?
Q3. What is the difference between displaying from BIG-IQ and displaying from BIG-IP?

5. Select bigip02 and the hover the mouse over the Nodes title.
6. Now select the BIG-IQ radio button from above, select bigip02, and then hover over the Nodes title.
Task – Make a modification via the BIG-IQ

1. With, **BIG-IQ** and **bigip02** selected hover over **Nodes** and hit the plus sign (+) and add a new node to **bigip02** named **new_node** with an IP address of **10.1.20.252**.

   **Attention:** Q1. Was new_node added to bigip02?

2. Let's have BIG-IQ deploy the change. Select **Deployment** next to **ADC** on the top bar.
3. Next to **Deployments**, select the plus sign (+) and **Deploy Configuration Changes**. Select the **review Pending Changes** link.

   **Attention:** Q2. What is being added? What is in the **New Version** window?

4. Name deployment **deploy_new_node**, select the **bigip02** device and click on **Deploy** in the upper left.

   **Attention:** Q3. Check **bigip02**, was **new_node** created?

2.6 Module – Modify and Manage Pools and Virtual Servers

**Objective:**
- Objective 8.01-8.02
  - Modify and manage virtual servers
  - Modify and manage pool images

Estimated completion time: A lot of minutes

2.6.1 Lab – Modify and Troubleshoot Virtual Servers

**Task – Troubleshooting virtual servers**

By now, I am sure you are dying to know what's up with the **purple_vs**. Here's a chance to find out. You are going to some troubleshooting with a little guidance.

1. Go to **Network Maps** and take a look at the status of the **purple_vs** and its components.

   It is obvious that all pool members are offline which could be anything, a network issue, a server issue, a **BIG-IP configuration issue**.

   **Attention:** Q1. Where would you start?
2. SSH to **bigip01** at 10.1.1.245.

| **Attention:** | Q2. Attempt to ping the pool members. Does it work? What does this tell you? |
|               | Q3. Attempt a `curl -i` against the pool members. Does it work? What does this tell you? |
|               | Q4. Since the problem affects all pool members, what would you suspect as a possible issue? |

3. Find the issue with the pool members and correct the issue.

| **Hint:** | You may want to read [https://support.f5.com/csp/article/K2167](https://support.f5.com/csp/article/K2167) |

| **Attention:** | Q5. Did you correct the issue? (If not go to **Appendix 1 – Answer Key** and see how the issue was fixed) |
|               | Q6. Now the pool is working and purple_vs is available can you access the page through the virtual? |
|               | Q7. What is your next step in debugging? Is the virtual server processing traffic? |

4. You need to watch traffic from your PC to the BIG-IP virtual server and from the BIG-IP to the pool.

| **Attention:** | Q8. What command(s) could you use to watch traffic hit the virtual server and leave toward the pool? |

*(Try to figure it out, if you need help go to Appendix 1 – Answer Key and my version of the commands)*

| **Attention:** | Q9. Did you see traffic hit the virtual server? Did you see BIG-IP send traffic to a pool member? |
|               | Q10. Did you see the return traffic? If there was no response, what is your step? |

5. The server’s default gateway is 10.1.20.240, which is an **unused** IP address on the 10.1.20.0/24 network. There were two ways to resolve the virtual server issue. Your **purple_vs** should now be **available**.

*(If you need help go to **Appendix 1 – Answer Key** and my version of the commands)*

**Task – Working with profiles**

1. Create new virtual server **secure_vs 10.1.10.100:443** with TCP profile, Automap and **www_pool**.

2. Browse to [https://10.1.10.100](https://10.1.10.100) and observe tcpdump.

| **Attention:** | Q1. Did site work? Why not? |

3. Change SSL Profile to include clientssl then update
4. Browse to https://10.1.10.100 and observe tcpdump

   **Attention:** Q2. Did site work?

5. Enable cookies Default Persistence Profile and update? Note error and troubleshoot to fix.

   **Attention:** Q3. What was needed to add cookie persistence?


   **Attention:** Q4. What is the name of the cookie inserted begin with?

7. Create new pool **secure_pool** with members of 10.1.20.11:443, 10.1.20.12:443 and 10.1.20.13:443 and assign to **sure_vs**.

8. Browse to https://10.1.10.100

   **Attention:** Q5. Did site work?

9. Troubleshoot and fix.

   **Attention:** Q6. What profile was needed to correct the error?

### 2.7 Module – Appendix I - Answer Key

The answers to all of your questions. Literally.

**Note:** In this appendix the third digit in the section (ie. 2.7.**X**) represents the module number and the fourth digit (ie. 2.7.X.**Y**) the task/lab number.

#### 2.7.1 Module 1 - Packet Processing and Virtual Servers

**Lab Preparation and Packet Processing**

**Open BIG-IP TMSH and TCPDump session**

**Q1. Why are ssh sessions not displayed in connection table?**

**tmsh show sys connections** displays connections on the TMOS data plane. SSH connections are established to out-of-band management interface and thus not seen.
Establish ftp connection

Q1. In the tcpdump above, what is client IP address and port and the server IP address port?
10.1.10.1:60603 and 10.1.10.20:21 (FTP)

Note: 60603 is an ephemeral port and BIG-IP will attempt to use the same client port on the server-side connection

Q2. What is source ip and port as seen by ftp server in the example above?
Source IP: 10.1.20.249 Source IP: 61236

Q3. What happened to the original client IP address and where did 10.1.20.249 come from?
The virtual server was configured to do source address translation using the SNAT Pool, SNAT249_pool. Reviewing the configuration of SNAT249_pool shows it was configured with IP address 10.1.20.249.

Packet Filters

Test the FTP packet filter

Q1. Was the existing ftp connection in the connection table affected? Why?
The FTP connection is not affected because adding packet filter does not impact established connections.
Q2. Was ftp connection successful? If yes, why?
The attempt to establish a new FTP connection was blocked, because the packet filter rule applies to all new connection attempts
Q3. What did tcpdump reveal? Connection timeout or reset?
Tcpdump revealed multiple S (syn) attempts without receiving ack. This is indicating a connection timeout.
Q4. What did virtual server statistics for ftp20_vs reveal? Why are counters not incrementing?
VS stats shows no new connection attempts because Filter is applied before VS in order of processing
Q5. Prioritize the packet processing order:
Virtual Server 3 SNAT 4 AFM/Pkt Filter 2 NAT 5 Existing Connections 1 Self IP 6 Drop 7

Virtual Server Packet Processing

Testing Virtual Server Packet Processing Behavior

Q1. Which VS is used for web traffic over port 8080?
 wildcard_vs
Q2. Which VS is used for ftp traffic?
 ftp_vs
Q3. Which VS is used for web traffic over the default HTTP port? Which port was used?
 www_vs port 80
Q4. Which VS is used for web traffic?
2.7.2 Module 2 - Virtual Server and Pool Behavior and Status

Virtual Server Status

Test Disabled Virtual Server

Q1. What is the Availability of www_vs? What is the State?
Availability: available, State: disabled
Q2. What symbol is used to represent www_vs status?
Black Circle
Q3. Would you expect browsing to http://10.1.10.100 to work?
No
Q4. Can you ping the virtual IP?
Yes, the virtual address still responds to pings
Q5. Did the site work? What did the tcpdump show?
No, the tcpdump showed the virtual server 10.1.10.100:80 responding to SYNs with Resets
Q6. Did statistics counters for any virtual increment?
No
Q7. Why do you think the wildcard_vs didn’t pick up the packets?
www_vs was the most specific virtual server so it responded. Because the www_vs was disabled the response was to reset the connection. This make sense if you think about it. What good would it do to disable a virtual server just to have another virtual server pick up the traffic either process incorrectly or send it to servers you just tried to prevent traffic from going too.
Q8. What symbol is used to represent wildcard_vs? Why is symbol a square?
The status symbol is a black square. Black because the virtual server was administratively disabled and square because there is no monitor and the state is Unknown
Q9. What is the reason given for current state?
The children pool member(s) either don’t have service checking enabled, or service check results are not available yet. Availability: unknown State: disabled
Q10. Does ftp session still work? Why?
Disabling a configuration item (node, pool or virtual server) does not affect existing connections.
Q11. Did new ftp session establish connection? Why not?
No, a disabled virtual server will not process new connections.

Virtual Server Connection Limits and Status

Q1. Does ftp session work?
Yes
Q2. What is the virtual server status of ftp_vs?
Yellow Triangle - Availability: unavailable - State: enabled

Q3. Did new ftp session establish connection? Why not?
No, the virtual server’s connection limit has been reached.

Q4. Did tcpdump capture show a connection reset?
Yes, tcpdump revealed R TCP reset the connection.

Pool Member and Virtual Servers

Effects of Monitors on Members, Pools and Virtual Servers

Q1. Since the mysql_monitor will fail, how long will it take to mark the pool offline?
60 seconds, the monitor will have to fail 4 times at 15 second intervals before it exceeds the 46 second timeout value.

Q2. What is the icon and status of www_vs?
Red Diamond - Availability: offline - State: enabled - The children pool member(s) are down

Q3. What is the icon and status of www_pool?
Red Diamond - Availability: offline - State: enabled - The children pool member(s) are down

Q4. What is the icon and status of the www_pool members?
Red Diamond - Availability: offline - State: enabled - Pool member has been marked down by a monitor

Q5. Does pool configuration have an effect on virtual server status?
Yes, the status of the pool members can affect the status of the virtual server.

Q6. What is the icon and status of www_vs?
Black Diamond - Availability: offline - State: disabled - The children pool member(s) are down

Q7. Did traffic counters increment for www_vs?
No

Q8. What is the difference in the tcpdumps between Offline (Disabled) vs Offline (Enabled)?
Offline (Disabled) - immediate connection reset, you will see no virtual server statistics.
Offline (Enabled) - initial connection accepted then reset, the virtual server stats are incremented

More on status and member specific monitors

Q1. What is the status of the Pool Member and the monitors assigned to it?
Red Diamond - Red Diamond - Availability: offline - State: enabled - Pool member has been marked down by a monitor
http - Green Circle, mysql_monitor - Red Diamond

Q2. What is the status of www_vs, www_pool and the pool members? Why?
Green, Green, Red, Red, Green. One pool member available, marks the pool available and since the pool is available, the virtual server is available
Q3. Did the site work?
Yes
Q4. Which www_pool members was traffic sent to?
Traffic was distributed to available pool members.

Load Balancing

Q1. Which www_pool members was traffic sent to?
Traffic was distributed to 10.1.20.12 and 10.1.20.13
Q2. Did member 10.1.20.12 receive the most traffic? Why not?
No, because LB method is Round Robin, Ratio and Priority Group configurations on pool members do not apply.
Q3. Which www_pool members was traffic sent to?
Traffic was distributed to 10.1.20.12 and 10.1.20.13
Q4. Did member 10.1.20.12 receive the most traffic?
10.1.20.12 received 5x more traffic than 10.1.20.12

Priority Group Activation

Q1. Which www_pool members was traffic sent to?
Traffic was distributed to 10.1.20.11 and 10.1.20.12
Q2. Which www_pool members was traffic sent to? Why?
Traffic was distributed to 10.1.20.12 and 10.1.20.13. Pool member availability dropped below 2 available members in the highest priority group and the next lowest priority group was activated.
Q3. Would the results have been different if 10.1.20.11:80 had been marked offline or marked with a yellow triangle?
No, both mark the member as Unavailable, dropping the Available members below 2.

The Effects of Persistence on Load Balancing

Q1. Why was a http profile required?
The http profile was required to tell the BIG-IP to parse the http request/response sequence for the virtual server so it could insert and read cookies in the http headers.
Q2. Was traffic evenly distributed to all www_pool members? Why not?
Traffic went to only on pool member because of persistence,
Q3. Did you persist to the Disabled member? Why?
Yes, a Disable pool member will still receive new connections if a persistence record points to it.
Q4. Does traffic continue to persist to the member Forced Offline?
No, another available member was selected and a new persistence record was created

Q5. If cookies were disable on your browser would persistence still work? Why?
Yes, source address persistence would be used to persist to a pool member

2.7.3 Module 3 - Trouble-shooting the BIG-IP

Trouble-shooting Hardware

End User Diagnostics

Q1. What three methods are available for running EUD on F5 Hardware?
USB CDROM, USB Bootable Drive, Hardware Boot Menu

Q2. How do you determine EUD version?
EUD image downloaded or eud_info

Q3. What is the filename and location of the EUD output?
/shared/log/eud.log

LCD Panel

Q1. How do you halt the unit via the LCD panel?
Press X, select system menu, press check, select halt, press check to confirm

Q2. Holding the X for 4 seconds does what?
Powers down unit

Q3. Holding the Check button for 4 seconds does what?
Reboots the unit

Hardware Log Files

Q1. What is the filename and location of the logs for LTM?
/var/log/ltm

Q2. Where will power supply, fan and hard disk related issues be logged?
/var/log/ltm

HA and Failover

Q1. Is failover sometimes used to determine issues related to hardware or software?
hardware

Q2. How do you initiate failover to standby unit?
From Active unit select Network > Traffic Groups, select traffic group, select Force to Standby

Q3. What persistence profile cannot be mirrored?
Cookie persistence is not mirrored

Q4. **What two connection types are re-mirrored after failback?**
Only FastL4 and SNAT connections are re-mirrored after failback

Q5. **When would you recommend using connection mirroring?**
Long lived connections

Q6. **Where is connection mirroring configured?**
You can configure connection mirroring at VS and SNAT

Q7. **Where is persistence mirroring configured?**
You can configure persistence mirroring at Persistence

Q8. **What tmsh command is used to view mirrored connections?**
show /ltm persistence persist-records

Q9. **What tmsh command is used to view mirrored persistence?**
show /ltm persistence persist-records

Q10. **What can be the cause of primary unit returning to active state after initiating failover to standby?**
Show /sys connection all-properties

**tcpdump Packet Capture**

**Packet Captures of multiple interfaces simultaneously**

Q1. **What is the alternate method for capturing two interfaces simultaneously?**
tcpdump -ni eth1 -w /var/tmp/dump1.cap & tcpdump -ni eth2 -w /var/tmp/dump2.cap

Q2. **What interface does 0.0 represent?**
All interfaces

Q3. **What interface typically represents the management interface?**
eth0

Q4. **What is recommended method for packet captures on high load system?**
F5 recommends that you mirror traffic to a dedicated sniffing device

Q5. **Will tcpdump capture PVA accelerated traffic?**
No, you must disable PVA to capture traffic

**Performance Statistics**

**Observing performance statistics**

Q1. **What is the longest time interval available for performance statistics?**
30 Days
Connectivity Troubleshooting

Connectivity troubleshooting tools

Q1. Was echo response received?
Ping reply was successful

Q2. What is the status of the virtual servers?
ftp_vs and www_vs available, disabled - wildcard_vs unknown, disabled

Q3. Was echo response received?
Ping reply successful

Self IP Port Lockdown

Effects of Port Lockdown

Q1. Was echo response received?
Ping reply successful

Q2. Was ssh successful? Why not?
No. Port lockdown set to Allow None by default

Q3. Was ssh successful?
Yes

Q4. Does existing ssh window still work?
No

Q5. Was new ssh session established?
No

2.7.4 Module 4 - Support and Analytics

Support, Status and Logs

Qkview and iHealth

Q1. Are logs associated with qkview?
Yes

Q2. Where is default filename and location of qkview output?
/var/tmp/hostname.qkview

Q3. Where is the default filename and location of core dump?
/var/core/

Q4. What is Severity and Condition for unit failure in active/standby pair?
Severity 2, Site at Risk
Q5. If support case was opened online with Severity 4 and no call has been received in a week. What should you do?
Call support, reference open case and ask to escalate. This may require Duty Manager approval.
Q6. What is the procedure to escalate support case?
Call support, reference open case and ask to escalate. This may require Duty Manager approval.

**Network Map**

Q1. What is a node?
IP Address of Pool Member
Q2. What icon is reflected for 10.1.20.11 on the Network map?
Black
Q3. What is the color of the icon for pool members based on 10.1.20.11? Why?
Grey Circle
Q4. Does ftp_vs still work as expected?
No
Q5. Where is irule reflected on Network Map?
iRule is displayed between the Virtual Server and Pool

**Dashboard**

Q1. What is longest duration available for reporting?
1 Month
Q2. How can report be exported?
Reports may be exported as csv files.

**Log files**

Q1. Was an alert logged?
Yes
Q2. Was the alert logged here?
Yes
Q3. What command is needed to find all instances of err in /var/log/ltm?
grep err /var/log/ltm
iApps and Analytics

Create iApps Analytics

Q1. Did both pool members respond? Why?
No, only one responded because cookie persistence was built using the iApp

Q2. Can you determine which page took the longest to load?
If you select Latency > Page Load Time from the top bar you will find /bigtext.html took longest.

Q3. Could you add the pool member? Why?
No, because iApp strictness is on by default and the application can only be changed by going to the iApp application and selecting Reconfigure from the top bar.

Q4. Can you add the custom_analytics profile to the ftp_vs? Why?
No, analytics in v11.5 can only be done on HTTP and DNS virtual servers with a HTTP or DNS profile attached.

2.7.5 Module 5 - Managing the BIG-IP

UCS, BIG-IP Archive

Create UCS Archive Files

Q1. What extension must Archive have?
.ucs

Q2. What is the default location for ucs files?
/var/local/ucs

Q3. What is command for loading ucs file?
load /sys ucs <path to UCS>
load /sys ucs <path to UCS> no-license - This will not restore the license file

Q4. What issues will occur by restoring ucs file on RMA device?
Licensing and device cert keys must be updated.

Upgrading a BIG-IP Device Service Clusters (DSC)

Upgrading software

Q1. You are about to start your upgrade to 12.1, which device will you upgrade first?
You would begin the upgrade on the standby device, in this case that should be bigip02.

Q2. True or false? Once the install is complete, the BIG-IP will automatically reboot to the new volume.
False, you will have to set the new volume as the Active volume and then reboot the BIG-IP

Q3. What steps would be required to complete the upgrade?
   1. Set the new volume to the active volume
2. Reboot the BIG-IP

3. Confirm the reboot was successful and the BIG-IP is running

4. Force the BIG-IP with the old software to Standby, making virtual servers, and other listeners active on the upgraded BIG-IP

5. Test that traffic is passing correctly.

6. Upgrade the BIG-IP with the older software.

**BIG-IQ**

**Peruse BIG-IQ**

Q1. What BIG-IPs are being managed?
bigip01.f5demo.com and bigip02.f5demo.com

Q2. Where are configurations currently being display from?
The configuration displayed was retrieved from the BIG-IP

Q3. What is the difference between displaying from BIG-IQ and displaying from BIG-IP?
If you are displaying configuration from BIG-IP the configuration is maintained and updated on that BIG-IP. If you are displaying configuration from the BIG-IQ, then BIG-IQ owns the configuration and can push changes out to the BIG-IP, no change should be made to the BIG-IP directly.

Q4. What now appears in the Nodes title when you hover the mouse over it?
A (+) appears in the title area because you can now modify the device via the BIG-IQ.

**Make a modification via the BIG-IQ**

Q1. Was `new_node` added to bigip02?
No, it was not.

Q2. What is being added? What is in the New Version window?
`new_node` is being added and the REST commands to do that are show in the New Version window.

Q3. Check bigip02, was `new_node` created?
Yes

**2.7.6 Module 6 - Modify and Troubleshoot Pools and Virtual Servers**

**Modify and Troubleshoot Virtual Servers**

**Troubleshooting virtual servers**

Q1. Where would you start?
I would go on the BIG-IP and test connectivity from the BIG-IP to the pool members.

Q2. Attempt to ping one of the pool members. Does it work? What does this tell you?
The ping should be successful. This means the server IP is up and I have basic connectivity.
Q3. **Attempt a curl -i against a pool member. Does it work? What does this tell you?**

The curl should be successful and you should see the request come back. The application is running.

Q4. **Since the problem affects all pool members, what would you suspect as a possible issue?**

Since I can see all pool members are functioning I would suspect the monitor is the issue. You could start debugging the monitor directly, or you could put the default HTTP monitor and see if the pool members come up. If they do, then the monitor is the issue and needs correction. In the case, you would check the Send and Receive strings. I would use a curl -i (to include the header and response codes) to look for the receive string. In this case it’s obvious, we are looking for a 200 OK (successful response), but have fat-finger 020 OK in the Receive box. Correct the receive string and reapply the monitor. The pool should come up Available (Green).

**Note:** The default HTTP monitor usually, but does not always, work on an HTTP application.

Q5. **Did you correct the issue?**

Yes

Q6. **Now the pool is working and purple_vs is available can you access the page through the virtual?**

No

Q7. **What do you think would be the next step in debugging the issue would be?**

I would clear the virtual server statistics and try again and see if the traffic is hitting purple_vs. The virtual server statistics should show traffic being processed.

Q8. **What command(s) could you use to watch traffic hit the virtual server and leave toward the pool?**

I would create two tcpdumps one on the client-side and the other on the server-side. I would want to limit the captures to watch for my PC IP address 10.1.10.51. You will need two terminal windows.

Terminal Window 1 (Client to BIG-IP)

`tcpdump -i client_vlan -X -s0 host 10.1.10.51 and 10.1.10.105`

(This command will only watch client-side traffic between the PC and virtual server. The -s0 command will dump the entire packet -X command will dump hex and ascii code of the packet. You will be able to see the HTTP request and response in the dump)

Terminal Window 2 (BIG-IP to Pool)

`tcpdump -i server_vlan -X -s0 host 10.1.10.51`

(This command will only watch server-side traffic from the PC and to the pool. The -s0 command will dump the entire packet -X command will dump hex and ascii code of the packet. You will be able to see the HTTP request and response in the dump)

Q9. **Did you see traffic hit the virtual server? Did you see BIG-IP send traffic to a pool member?**

You should have seen traffic hit the virtual server in Window 1 and in Window 2 BIG-IP should have picked a pool member and sent traffic to it.

Q10. **Did you see the return traffic? If there was no response, what is your step?**

No, you should not have received a response. Because the BIG-IP is not the default gateway, so the response went someplace else.

1. You can add and SNAT Pool or do SNAT Automap on the virtual server.

2. You can add 10.1.20.240 as a self IP address on the BIG-IP. This should be a floating IP in traffic_group_1 so that the default gateway for the servers is still available upon failover.
Working with profiles

Q1. Did site work? Why not?
SSL connection error

Q2. Did site work?
Yes

Q3. What was needed to add cookie persistence?
http profile

Q4. What is the name of the cookie inserted begin with?
BIGipServerwww_pool

Q5. Did site work?
No

Q6. What profile was needed to correct the error?
Server side ssl profile