



301B^{Q&As}

BIG-IP Local Traffic Manager (LTM) Specialist: Maintain & Troubleshoot

Pass F5 301B Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/301b.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by F5 Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Given LTM device ltm log:

```
Sep 26 20:51:08 local/lb-d-1 notice promptstatusd[3695]: 01460006:5: semaphore mcpd.running(1) held
Sep 26 20:51:08 local/lb-d-1 notice promptstatusd[3695]: 01460006:5:
Sep 26 20:51:08 local/lb-d-1 warning promptstatusd[3695]: 01460005:4: mcpd.running(1) held, wait for mcpd
Sep 26 20:51:08 local/lb-d-1 info sod[3925]: 010c0009:6: Lost connection to mcpd - reestablishing.
Sep 26 20:51:08 local/lb-d-1 err bcm56xxd[3847]: 012c0004:3: Lost connection with MCP: 16908291 ... Exiting
bsx_connect.cpp(174)
Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0012:6: MCP Exit Status
Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0012:6: Info: LACP stats (time now:1348717868) : no traffic
Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0014:6: Exiting...
Sep 26 20:51:08 local/lb-d-1 err lind[3842]: 013c0004:3: IO error on recv from mcpd - connection lost
Sep 26 20:51:08 local/lb-d-1 notice bigd[3837]: 01060110:5: Lost connection to mcpd with error 16908291, will reinit
connection.
Sep 26 20:51:08 local/lb-d-1 err statsd[3857]: 011b0004:3: Initial subscription for system configuration failed with error
\\\'
Sep 26 20:51:08 local/lb-d-1 err statsd[3857]: 011b0001:3: Connection to mcpd failed with error \\\'011b0004:3: Initial
subscription for system configuration failed with error \\\'\\\'
Sep 26 20:51:08 local/lb-d-1 err csyncd[3851]: 013b0004:3: IO error on recv from mcpd - connection lost
.....skipping more logs.....
Sep 26 20:51:30 local/lb-d-1 notice sod[3925]: 01140030:5: HA proc_running bcm56xxd is now responding.
Sep 26 20:51:34 local/lb-d-1 notice sod[3925]: 01140030:5: HA proc_running mcpd is now responding.
Sep 26 20:51:34 local/lb-d-1 notice sod[3925]: 010c0018:5: Standby
```

Which daemon failed?

- A. promptstatusd
- B. mcpd
- C. sod
- D. bcm56xxd
- E. lind



Correct Answer: B

QUESTION 2

An LTM Specialist uploaded new releases .iso and .md5 files titled "BIGIP-FILENAME" via the GUI.

Which commands are run via the command line from the root directory to verify the integrity of the new .iso file?

- A. `cd /var/shared/images md5sum --check BIGIP-FILENAME.iso`
- B. `cd /shared/images md5sum --check BIGIP-FILENAME.iso`
- C. `cd /var/shared/images md5sum --check BIGIP-FILENAME.iso.md5`
- D. `cd /shared/images md5sum --check BIGIP-FILENAME.iso.md5`

Correct Answer: D

QUESTION 3

In preparation for a maintenance task, an LTM Specialist performs a "Force to Standby" on LTM device Unit 1. LTM device Unit 2 becomes active as expected. The maintenance task requires the reboot of Unit 1. Shortly after the reboot is complete, the LTM Specialist discovers that Unit 1 has become active and Unit 2 has returned to standby.

What would cause this behavior?

- A. Unit 1 is set with the redundancy state preference of active in devices groups.
- B. Unit 1 is set with the redundancy state preference of active in high availability.
- C. A traffic group is configured with Auto Failback, and Unit 1 is the default device.
- D. A device group is configured with Auto Failback, and Unit 1 is the default device.

Correct Answer: C

QUESTION 4

An LTM device has a virtual server configured as a Performance Layer 4 virtual listening on 0.0.0.0 to perform routing of packets to an upstream router. The client machine at IP address 192.168.0.4 is attempting to contact a host upstream of the LTM device on IP address 10.0.0.99.

The network flow is asymmetrical, and the following TCP capture displays:

```
# tcpdump -nnni 0.0 \\\host 192.168.0.4 and host 10.0.0.99\\ tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on 0.0, link-type EN10MB (Ethernet), capture size 96 bytes
```



05:07:55.499954 IP 192.168.0.4.35345 > 10.0.0.99.443: S 3205656213:3205656213(0) ack 3267995082 win 1480
05:07:55.499983 IP 10.0.0.99.443 > 192.168.0.4.35345: R 1:1(0) ack 1 win 0 05:07:56.499960 IP 192.168.0.4.35345 >
10.0.0.99.443: S 3205656213:3205656213(0) ack 3267995082 win 1480 05:07:56.499990 IP 10.0.0.99.443 >
192.168.0.4.35345: R 1:1(0) ack 1 win 0 4 packets captured Which option within the fastL4 profile needs to be enabled
by the LTM Specialist to prevent the LTM device from rejecting the flow?

- A. Loose Close
- B. Loose Initiation
- C. Reset on Timeout
- D. Generate Initial Sequence Number

Correct Answer: B

QUESTION 5

A high-availability (HA) pair configuration uses only the hardwire serial cable connection to determine device state. A power outage occurs to the PDU powering the active unit. The standby unit takes over the active role as expected.

How is the peer unit able to determine the active unit is unavailable?

- A. voltage loss on serial cable
- B. no data stream received on serial port
- C. no response on management interface
- D. no heartbeat packets received on self IPs

Correct Answer: A

QUESTION 6

-- Exhibit -- Exhibit -



Hostname: V11-BigIP-A.local Date: Oct 17, 2012 User: admin
IP Address: 10.0.0.231 Time: 1:12 PM (EDT) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Not All Devices Synced

Main Help About System » Software Management : Image List

Image List Hotfix List Antivirus Check Updates Boot Locations

Installed Images

Product	Version	Build	Disk	Boot Location	Active	Media	Install Status
BIG-IP	11.2.1	797.0	HD1	HD1.1	Yes	hd	complete
BIG-IP	11.1.0	2268.0	HD1	HD1.2	No	hd	complete
BIG-IP	11.2.1	797.0	HD1	HD1.3	No	hd	complete

Available Images Import...

Status	Software Image	Version	Last Modified	Image Size	MD5 Verified	Available
<input type="checkbox"/>	<input checked="" type="checkbox"/> BIGIP-11.1.0.1943.0.iso	11.1.0	Tue Oct 2 10:37:31 2012	1012 MB	Yes	Yes
<input type="checkbox"/>	<input checked="" type="checkbox"/> BIGIP-11.2.1.797.0.iso	11.2.1	Wed Sep 26 13:19:27 2012	1213 MB	Yes	Yes

Delete Install...

Refer to the exhibit.

An LTM Specialist has uploaded a qkview to F5 iHealth.

Within the GUI, what is the correct procedure to comply with the recommendation shown in the exhibit?

- A. Obtain product version image from release.f5.com. Overwrite existing image with new product version image. Select product version image and click Install. Select the available disk and volume set name.
- B. Obtain product version image from images.f5.com. Overwrite existing image with new product version image. Select product version image and click Install. Select the available disk and volume set name.
- C. Obtain product version image from downloads.f5.com. Import product version image. Install image onto BIG-IP platform. Select product version image and click Install. Select the available disk and volume set name.
- D. Log a call requesting the product version image via websupport.f5.com Import product version image. Install image onto BIG-IP platform. Select product version image and click Install. Select the available disk and volume set name.

Correct Answer: C

QUESTION 7

An LTM device supports two power supplies. The value of the BigDB key "platform.powersupplymonitor" is equal to enable.

Where would the error message be visible if one of the power supplies fails or is NOT plugged in?



- A. visible only via the console
- B. in the /var/log/ltn log file
- C. in the /var/log/kern.log file
- D. in the /var/log/tmm log file

Correct Answer: B

QUESTION 8

-- Exhibit -- Exhibit -Refer to the exhibits. An LTM Specialist is troubleshooting an issue with one of the virtual servers on an LTM device, and all requests are receiving errors. Testing directly against the server generates no errors. The LTM Specialist has captured the request and

Capture direct to application server

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
09:46:03.428985 IP 192.168.1.1.31214 > 192.168.10.80.8443: S 1295563595:1295563595(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:46:03.430000 IP 192.168.10.80.8443 > 192.168.1.1.31214: S 2962914236:2962914236(0) ack 1295563596 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 3>
09:46:03.430041 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 1 win 4380
09:46:03.463946 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 1:137(136) ack 1 win 4380
09:46:03.465072 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 137 win 864
09:46:03.466127 IP 192.168.10.80.8443 > 192.168.1.1.31214: P 1:139(138) ack 137 win 864
09:46:03.466150 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 139 win 4518
09:46:03.720163 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 137:196(59) ack 139 win 4518
09:46:03.720183 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 196:542(346) ack 139 win 4518
09:46:03.721853 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 542 win 998
09:46:03.723009 IP 192.168.10.80.8443 > 192.168.1.1.31214: . 139:1599(1460) ack 542 win 998
09:46:03.723023 IP 192.168.10.80.8443 > 192.168.1.1.31214: P 1599:2693(1094) ack 542 win 998
09:46:03.723026 IP 192.168.10.80.8443 > 192.168.1.1.31214: F 2693:2693(0) ack 542 win 998
09:46:03.723060 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 2693 win 7072
09:46:03.723072 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 2694 win 7072
09:46:03.818084 IP 192.168.1.1.31214 > 192.168.10.80.8443: F 542:542(0) ack 2694 win 7072
09:46:03.819820 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 543 win 998
```

Capture through LTM device

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on External, link-type EN10MB (Ethernet), capture size 96 bytes
16:52:54.866907 IP 192.168.1.1.6789 > 192.168.1.211.443: S 2995699259:2995699259(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:52:54.866974 IP 192.168.1.211.443 > 192.168.1.1.6789: S 2305990363:2305990363(0) ack 2995699260 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:52:54.868417 IP 192.168.1.1.6789 > 192.168.1.211.443: . ack 1 win 16425
16:52:54.868422 IP 192.168.1.1.6789 > 192.168.1.211.443: P 1:105(104) ack 1 win 16425
16:52:54.868451 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:52:54.868457 IP 192.168.1.211.443 > 192.168.1.1.6789: . ack 105 win 4484
16:52:57.869207 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:53:01.068627 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:53:04.268911 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,sackOK,eol>
16:53:07.468781 IP 192.168.1.211.443 > 192.168.1.1.6789: R 1:1(0) ack 105 win 4484
```

response on both client and server sides of the LTM device. What should the LTM Specialist do to fix this issue?

- A. Remove "header-erase Host" in http profile.
- B. Configure SNAT Automap on the virtual server.
- C. Assign OneConnect profile to the virtual server.
- D. Set "redirect-rewrite" to "selective" in http profile.

Correct Answer: A

QUESTION 9



The LTM device is configured to provide load balancing to a set of web servers that implement access control lists (ACL) based on the source IP address of the client. The ACL is at the network level and the web server is configured to send a TCP reset back to the client if it is NOT permitted to connect.

The virtual server is configured with the default OneConnect profile.

The ACL is defined on the web server as:

Permit: 192.168.136.0/24 Deny: 192.168.116.0/24

The packet capture is taken of two individual client flows to a virtual server with IP address 192.168.136.100.

Client A - Src IP 192.168.136.1 - Virtual Server 192.168.136.100:

Clientside:

```
09:35:11.073623 IP 192.168.136.1.55684 > 192.168.136.100.80: S 869998901:869998901(0) win 8192
09:35:11.073931 IP 192.168.136.100.80 > 192.168.136.1.55684: S 2273668949:2273668949(0) ack 869998902 win 4380
09:35:11.074928 IP 192.168.136.1.55684 > 192.168.136.100.80: . ack 1 win 16425
09:35:11.080936 IP 192.168.136.1.55684 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:35:11.081029 IP 192.168.136.100.80 > 192.168.136.1.55684: . ack 299 win 4678
```

Serverside:

```
09:35:11.081022 IP 192.168.136.1.55684 > 192.168.116.128.80: S 685865802:685865802(0) win 4380
09:35:11.081928 IP 192.168.116.128.80 > 192.168.136.1.55684: S 4193259095:4193259095(0) ack 685865803 win 5840
09:35:11.081943 IP 192.168.136.1.55684 > 192.168.116.128.80: . ack 1 win 4380
09:35:11.081955 IP 192.168.136.1.55684 > 192.168.116.128.80: P 1:299(298) ack 1 win 4380
09:35:11.083765 IP 192.168.116.128.80 > 192.168.136.1.55684: . ack 299 win 108
```

Client B - Src IP 192.168.116.1 - Virtual Server 192.168.136.100:

Clientside:

```
09:36:11.244040 IP 192.168.116.1.55769 > 192.168.136.100.80: S 3320618938:3320618938(0) win 8192
09:36:11.244152 IP 192.168.136.100.80 > 192.168.116.1.55769: S 3878120666:3878120666(0) ack 3320618939 win 4380
09:36:11.244839 IP 192.168.116.1.55769 > 192.168.136.100.80: . ack 1 win 16425
09:36:11.245830 IP 192.168.116.1.55769 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:36:11.245922 IP 192.168.136.100.80 > 192.168.116.1.55769: . ack 299 win 4678
```

Serverside:

```
09:36:11.245940 IP 192.168.136.1.55684 > 192.168.116.128.80: P 599:897(298) ack 4525 win 8904
09:36:11.247847 IP 192.168.116.128.80 > 192.168.136.1.55684: P 4525:5001(476) ack 897 win 142
```

Why was the second client flow permitted by the web server?

- A. A global SNAT is defined.
- B. SNAT automap was enabled on the virtual server.
- C. The idle TCP session from the first client was re-used.
- D. A source address persistence profile is assigned to the virtual server.

Correct Answer: C



QUESTION 10

-- Exhibit



```

New TCP connection #1: 10.1.1.1(32021) <-> 10.1.1.2(443)
1 1 1351011538.3477 (0.1562) C>S Handshake
    ClientHello
        Version 3.0
        cipher suites
        SSL_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
        SSL_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
        SSL_DHE_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_AES_256_CBC_SHA
        SSL_RSA_WITH_CAMELLIA_256_CBC_SHA
        SSL_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_RC4_128_SHA
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_DSS_WITH_AES_128_CBC_SHA
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA256
        SSL_RSA_WITH_RC4_128_SHA
        SSL_RSA_WITH_RC4_128_MD5
        SSL_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
            NULL
1 2 1351011538.3477 (0.0000) S>C Handshake
    ServerHello
        Version 3.0
        session_id[0]=

        cipherSuite          SSL_RSA_WITH_RC4_128_SHA
        compressionMethod    NULL
1 3 1351011538.3477 (0.0000) S>C Handshake
    Certificate
1 4 1351011538.3477 (0.0000) S>C Handshake
    CertificateRequest
        certificate_types          rsa_sign
        certificate_authority
            30 81 98 31 0b 30 09 06 03 55 04 06 13 02 55 53
            31 0b 30 09 06 03 55 04 08 13 02 57 41 31 10 30
            0e 06 03 55 04 07 01 07 53 65 61 74 74 6c 65 31
            12 30 10 06 03 55 04 0a 13 09 4d 79 43 6f 6d 70
            61 6e 79 31 0b 30 09 06 03 55 04 0b 13 02 49 54
            31 1e 30 df 06 03 55 04 03 13 15 6c 6f 63 61 6c
            68 6f 73 74 2e 6c 6f 63 61 6c 64 6f 6d 61 69 6e
            31 29 30 27 06 09 2a 86 48 86 f7 0d 01 09 01 16
            1a 72 6f 6f 74 40 6c 6f 63 61 6c 68 6f 73 74 2e
            6c 6f 63 61 6c 64 6f 6d 61 69 6e
1 5 1351011538.3477 (0.0000) S>C Handshake
    ServerHelloDone
1 6 1351011538.5112 (0.1635) C>S Alert
    level          warning
    value          unknown value
1 7 1351011538.5112 (0.0000) C>S Handshake
    ClientKeyExchange
1 8 1351011538.5112 (0.0000) C>S ChangeCipherSpec
1 9 1351011538.5112 (0.0000) C>S Handshake
    Finished
1 10 1351011538.5113 (0.0000) S>C Alert
    level          fatal
    value          handshake_failure
1 1351011538.5113 (0.0000) S>C TCP FIN
1 1351011538.6866 (0.1753) C>S TCP FIN

```



-- Exhibit -Refer to the exhibit.

A user is unable to access a secure application via a virtual server.

What is the cause of the issue?

- A. The client authentication failed.
- B. The virtual server does NOT have a pool configured.
- C. The client and server CANNOT agree on a common cipher.
- D. The virtual server does NOT have a client SSL profile configured.

Correct Answer: A

QUESTION 11

Which iRule statement demotes a virtual server from CMP?

- A. set ::foo 123
- B. set static::foo 123
- C. persist source_addr 1800
- D. [class match \$HTTP_CONTENT contains my_data_class]

Correct Answer: A

QUESTION 12

An LTM Specialist configures a new HTTP virtual server on an LTM device external VLAN. The web servers are connected to the LTM device internal VLAN. Clients trying to connect to the virtual server are unable to establish a connection. A packet capture shows an HTTP response from a web server to the client and then a reset from the client to the web server.

From which two locations could the packet capture have been collected? (Choose two.)

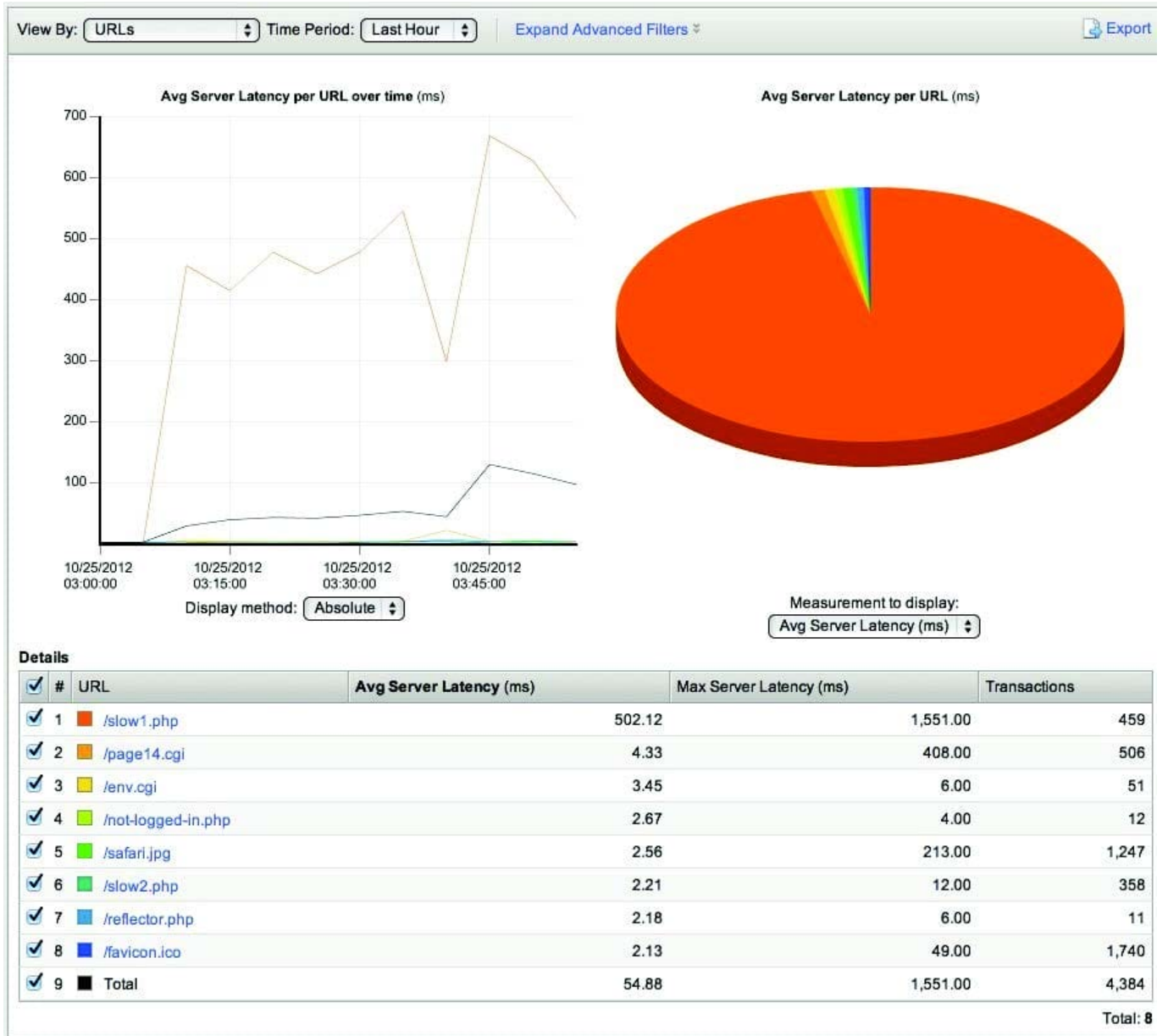
- A. network interface of web server
- B. network interface of client machine
- C. internal VLAN interface of the LTM device
- D. external VLAN interface of the LTM device
- E. management VLAN interface of the LTM device

Correct Answer: AB



QUESTION 13

-- Exhibit -- Exhibit -Refer to the exhibit.



Which URL should be reported to the server/application team as getting user-visible errors?

- A. /env.cgi
- B. /page14.cgi
- C. /reflector.php
- D. /browserspecific.html



Correct Answer: B

QUESTION 14

-- Exhibit

```
bigipA
# devices <devgroup [device cid.id cid.orig cid.time last_sync
11 48 Groupe-HA bigipA.f5.com 2 bigipB.f5.com 12:39:19 : :
10 Groupe-HA bigipA.f5.com 2 bigipB.f5.com 12:39:19 12:40:55
11 Groupe-HA bigipB.f5.com 4 bigipB.f5.com 12:42:19 12:32:09
10 48 Groupe-HA bigipB.f5.com 4 bigipB.f5.com 12:42:19 : :
10 11 Groupe-HA bigipC.f5.com 2 bigipB.f5.com 12:39:19 : :
48 Groupe-HA bigipC.f5.com 2 bigipB.f5.com 12:39:19 12:40:54
```

-- Exhibit -Refer to the exhibit.

An LTM Specialist is troubleshooting a sync-failover group of three BIG-IP LTM devices. The command used is "tmsh run cm watch-devicegroup-device."

What does the output mean?

- A. Configuration is synchronized between all the devices.
- B. Configuration is not synchronized. Some modifications have been done on bigipA.
- C. Configuration is not synchronized. Some modifications have been done on bigipB.
- D. Configuration is not synchronized. Some modifications have been done on bigipC.

Correct Answer: C

QUESTION 15

A OneConnect profile is applied to a virtual server. The LTM Specialist would like the client source IP addresses within the 10.10.10.0/25 range to reuse an existing server side connection. Which OneConnect profile source mask should the LTM Specialist use?

- A. 0.0.0.0
- B. 255.255.255.0
- C. 255.255.255.128
- D. 255.255.255.224
- E. 255.255.255.255

Correct Answer: C



VCE & PDF

PassApply.com

<https://www.passapply.com/301b.html>

2024 Latest passapply 301B PDF and VCE dumps Download

[Latest 301B Dumps](#)

[301B Exam Questions](#)

[301B Braindumps](#)