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:

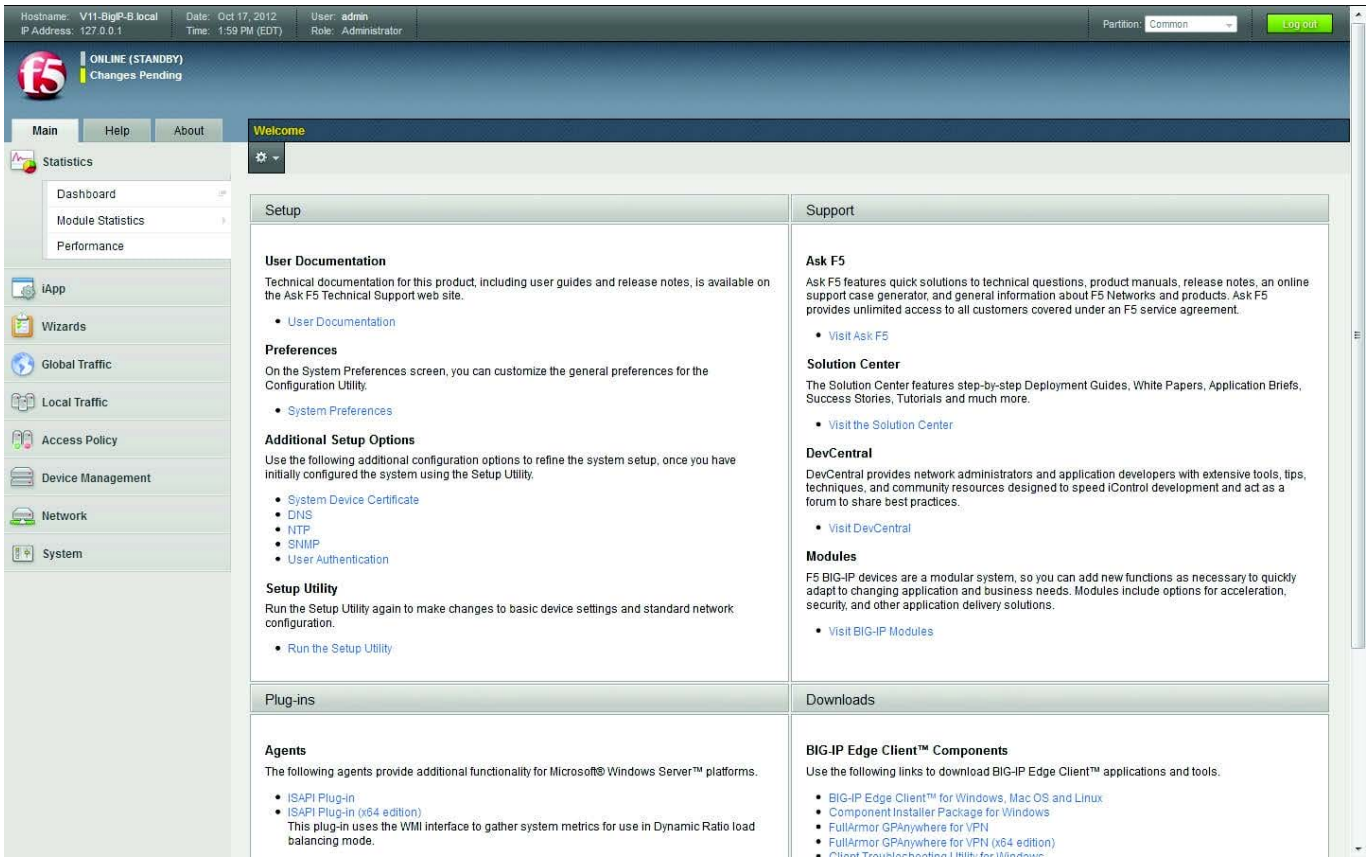
https://www.certbus.com/301b.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

-- Exhibit



-- Exhibit -Refer to the exhibit.

Which step should an LTM Specialist take to utilize AVR?

A. provision AVR

B. reboot the device

C. install the AVR add-on

D. license the device for AVR

Correct Answer: A

QUESTION 2

An LTM Specialist is tasked with ensuring that the syslogs for the LTM device are sent to a remote syslog server. The following is an extract from the config file detailing the node and monitor that the LTM device is using for the remote syslog server:

monitor Syslog_15002 { defaults from udp dest *:15002

}

node 91.223.45.231 { monitor Syslog_15002 screen RemoteSYSLOG

}

There seem to be problems communicating with the remote syslog server. However, the pool monitor shows that the remote server is up. The network department has confirmed that there are no firewall rules or networking issues preventing the LTM device from communicating with the syslog server. The department responsible for the remote syslog server indicates that there may be problems with the syslog server. The LTM Specialist checks the BIG-IP LTM logs for errors relating to the remote syslog server. None are found. The LTM Specialist does a tcpdump:

tcpdump -nn port 15002, with the following results: 21:28:36.395543 IP 192.168.100.100.44772 > 91.223.45.231.15002: UDP, length 19 21:28:36.429073 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 169 21:28:36.430714 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 181 21:28:36.840524 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 169 21:28:36.846547 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 181 21:28:39.886343 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 144

NotE. 192.168.100.100 is the self IP of the LTM device.

Why are there no errors for the remote syslog server in the log files?

A. The -log option for tcpdump needs to be used.

B. The monitor type used is inappropriate.

C. The "verbose" logging option needs to be enabled for the pool.

D. When the remote syslog sever fails, it returns to service before the timeout for the monitor has expired.

Correct Answer: B

QUESTION 3

A stand-alone LTM device is to be paired with a second LTM device to create an active/standby pair. The current stand-alone LTM device is in production and has several VLANs with floating IP addresses configured. The appropriate device service clustering (DSC) configurations are in place on both LTM devices.

Which two non-specific DSC settings should the LTM Specialist configure on the second LTM device to ensure no errors are reported when attempting to synchronize for the first time? (Choose two.)

A. pools

B. VLANs

C. default route

D. self IP addresses

Correct Answer: BD

QUESTION 4

An LTM Specialist is running the following packet capture on an LTM device:

ssldump -Aed -ni vlan301 \\'port 443\\'

Which two SSL record message details will the ssldump utility display by default? (Choose two.)

A. HTTP Version

B. User-Agent

C. ClientHello

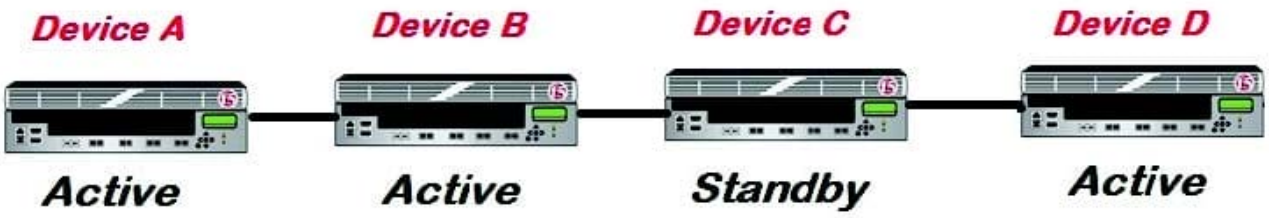
D. ServerHello

E. Issuer

Correct Answer: CD

QUESTION 5

-- Exhibit



-- Exhibit -Refer to the exhibit.

An LTM Specialist is upgrading the LTM devices.

Which device should be upgraded first?

A. Device A

B. Device B

C. Device C

D. Device D

Correct Answer: C

QUESTION 6

-- Exhibit

```
Through LTM Device:
New TCP connection #1: 172.16.1.3(63936) <-> 172.16.20.21(443)
1 1  0.0013 (0.0013)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_AES_256_CBC_SHA256
        Unknown value 0xff
        compression methods
                  NULL
1 2  0.0038 (0.0025)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          7c 00 d2 cf 81 f8 cd ab 6b 48 c0 9a cc 19 df f7
          12 5f f2 c8 2a a2 e8 ef 1e f1 10 41 61 99 6d 27
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
1 3  0.0038 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0038 (0.0000)  S>C  Handshake
      CertificateRequest
        certificate_types                   rsa_sign
        certificate_types                   dss_sign
        certificate_types                   unknown value
        certificate_authority
          30 81 90 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 13 07 53 65 61 74 74 6c 65 31
          14 30 12 06 03 55 04 0a 13 0b 45 78 61 6d 70 6c
          65 2e 43 6f 6d 31 14 30 12 06 03 55 04 0b 13 0b
          45 6e 67 69 6e 65 65 72 69 6e 67 31 36 30 34 06
          03 55 04 03 13 2d 43 4e 3d 4a 6f 68 6e 20 55 73
          65 72 2c 4f 55 3d 45 6e 67 69 6e 65 65 72 69 6e
          67 2c 44 43 3d 65 78 61 6d 70 6c 65 2c 44 43 3d
          63 6f 6d
      ServerHelloDone
1 5  0.0040 (0.0002)  C>S  Handshake
      Certificate
1 6  0.0040 (0.0000)  C>S  Handshake
      ClientKeyExchange
1 7  0.0040 (0.0000)  C>S  ChangeCipherSpec
1 8  0.0044 (0.0003)  C>S  Handshake
1 9  0.0049 (0.0004)  S>C  Alert
    level           fatal
    value           handshake_failure
1    0.0049 (0.0000)  S>C  TCP FIN
1    0.0049 (0.0000)  C>S  TCP RST

Direct to application server:
New TCP connection #1: 1.1.2.150(64506) <-> 172.16.20.21(443)
1 1  0.0027 (0.0027)  C>S  Handshake
      ClientHello
        Version 3.1
        resume [32]=
          96 55 ee e0 53 90 e5 63 f8 46 3c 5c 19 59 8a fa
          c4 e6 2f 5f 6e 80 40 dd 08 05 5c 74 f7 3a d6 61
        cipher suites
        Unknown value 0xc00a
        Unknown value 0xc014
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
        TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
        Unknown value 0xc00f
        Unknown value 0xc005
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        Unknown value 0xc007
        Unknown value 0xc009
        Unknown value 0xc011
        Unknown value 0xc013
        Unknown value 0x45
        Unknown value 0x44
        TLS_DHE_DSS_WITH_RC4_128_SHA
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        TLS_DHE_DSS_WITH_AES_128_CBC_SHA
        Unknown value 0xc00c
        Unknown value 0xc00e
        Unknown value 0xc002
        Unknown value 0xc004
        Unknown value 0x96
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_RC4_128_MD5
        TLS_RSA_WITH_AES_128_CBC_SHA
        Unknown value 0xc008
        Unknown value 0xc012
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        Unknown value 0xc00d
        Unknown value 0xc003
        Unknown value 0xfeff
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
1 2  0.0098 (0.0071)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[0]=

        cipherSuite         TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
        compressionMethod                   NULL
1 3  0.0098 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0098 (0.0000)  S>C  Handshake
      ServerKeyExchange
1 5  0.0098 (0.0000)  S>C  Handshake
      CertificateRequest
        certificate_types                   rsa_fixed_dh
        certificate_types                   dss_fixed_dh
        certificate_types                   rsa_sign
        certificate_types                   dss_sign
        certificate_types                   unknown value
        certificate_authority
          30 81 90 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 13 07 53 65 61 74 74 6c 65 31
          14 30 12 06 03 55 04 0a 13 0b 45 78 61 6d 70 6c
          65 2e 43 6f 6d 31 14 30 12 06 03 55 04 0b 13 0b
          45 6e 67 69 6e 65 65 72 69 6e 67 31 36 30 34 06
          03 55 04 03 13 2d 43 4e 3d 4a 6f 68 6e 20 55 73
          65 72 2c 4f 55 3d 45 6e 67 69 6e 65 65 72 69 6e
          67 2c 44 43 3d 65 78 61 6d 70 6c 65 2c 44 43 3d
          63 6f 6d
      ServerHelloDone
1    0.0448 (0.0349)  C>S  TCP FIN
1    0.0460 (0.0012)  S>C  TCP FIN
```

-- Exhibit -

Refer to the exhibit.

An LTM Specialist has created a virtual server to load balance traffic to a pool of HTTPS servers. The servers use client certificates for user authentication. The virtual server has clientssl, serverssl, and http profiles enabled. Clients are unable

to connect to the application through the virtual server. Clients are able to connect to the application servers directly.

What is the root cause of the problem?

A. The application server does NOT support 2048-bit keys.

B. The clientssl profile is NOT set to require a client certificate.

C. The LTM device does NOT trust the issuing CA of the client certificate.

D. The application server does NOT see the client certificate due to SSL offload.

Correct Answer: D

QUESTION 7

A web application requires knowledge of the client\\'s true IP address for logging and analysis purposes. Instances of the application that can decode X-Forwarded-For HTTP headers reside in pool_a, while pool_b instances assume the source

IP is the true address of the client.

Which iRule provides the proper functionality?

A. when HTTP_DATA { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b

}

}

B. when HTTP_RESPONSE { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b

}

}

C. when HTTP_REQUEST { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b

}

}

D. when HTTP_OPEN { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b

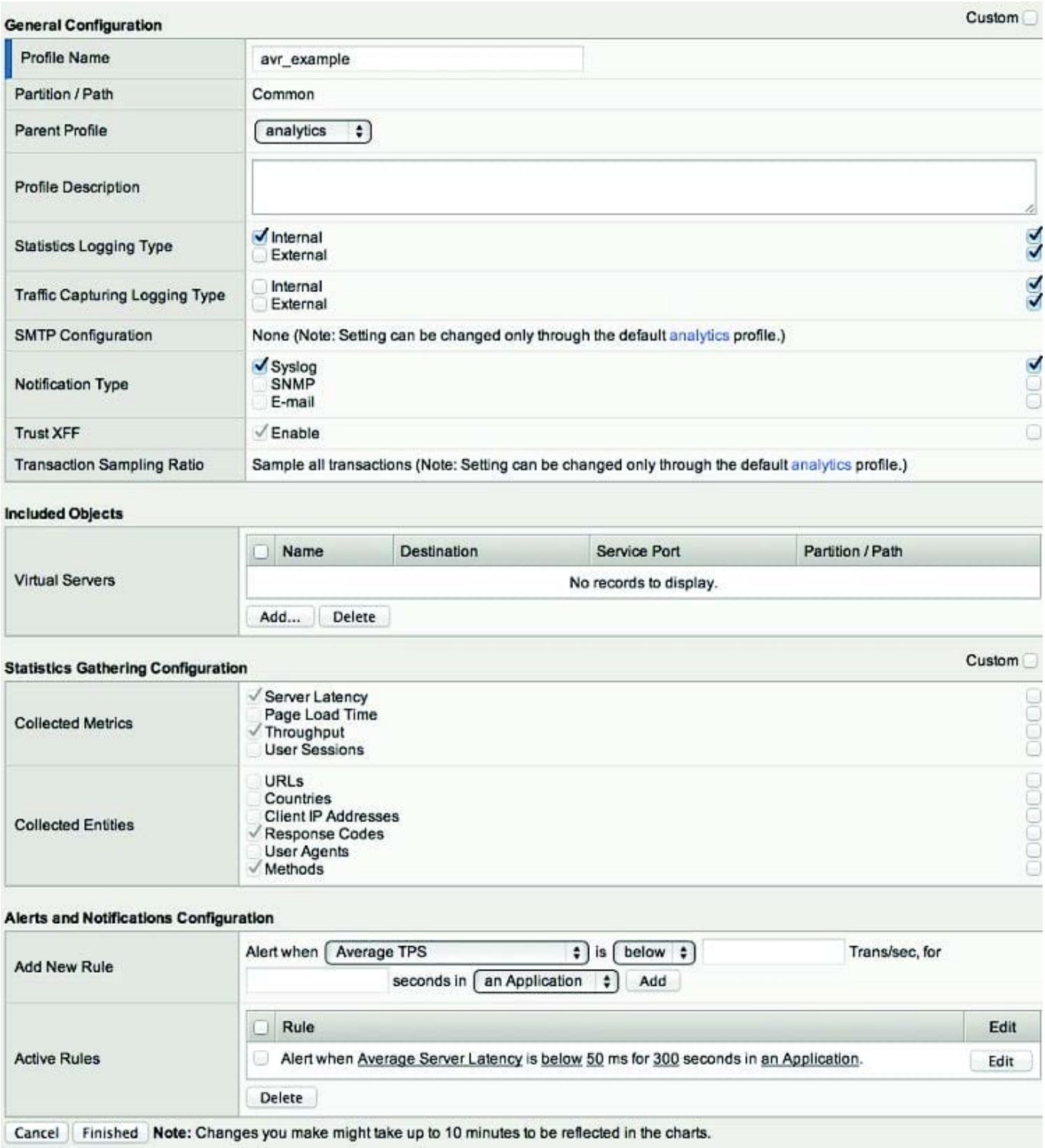
}

}

Correct Answer: C

QUESTION 8

-- Exhibit



-- Exhibit -

Refer to the exhibit.

An LTM Specialist sets up AVR alerts and notifications for a specific virtual server if the server latency exceeds 50ms. The LTM Specialist simulates a fault so that the server latency is consistently exceeding the 50ms threshold; however, no

alerts are being received.

Which configuration should the LTM Specialist modify to achieve the expected results?

A. The rule should be adjusted to trigger when server latency is above 50ms.

B. SNMP alerting should be enabled to allow e-mail to be sent to the support team.

C. User Agents needs to be enabled to ensure the correct information is collected to trigger the alert.

D. The metric "Page Load Time" needs to be enabled to ensure that the correct information is collected.

Correct Answer: A

QUESTION 9

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 10

An LTM Specialist configures the following iRule on an LTM device: when HTTP_REQUEST { if {[string tolower [HTTP::uri]] contains "/URI1/" } { pool Pool1 } elseif {[string tolower [HTTP::uri]] contains "/URI2/" } { pool Pool2 } elseif {[string tolower [HTTP::uri]] contains "/URI3/" } { pool Pool3 }

else { pool Pool4} } Given the following request: http://www.example.comURI1/index.html?fu=barandpass=1234

Which pool will be selected by the iRule?

A. Pool1

B. Pool2

C. Pool3

D. Pool4

Correct Answer: D

QUESTION 11

When re-licensing an LTM device from the command line interface, which tmsh command should the LTM Specialist use to generate the required information to provide on the F5 licensing portal?

A. tmsh run /util get-dossier

B. tmsh generate /sys dossier

C. tmsh list /sys registration-key

D. tmsh install /sys license registration-key

Correct Answer: A

QUESTION 12

An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user\\'s shopping cart is shown as empty. The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.

What is the issue?

A. The port 80 pool member is deleting the user\\'s session cookie.

B. The port 443 pool member is deleting the user\\'s session cookie.

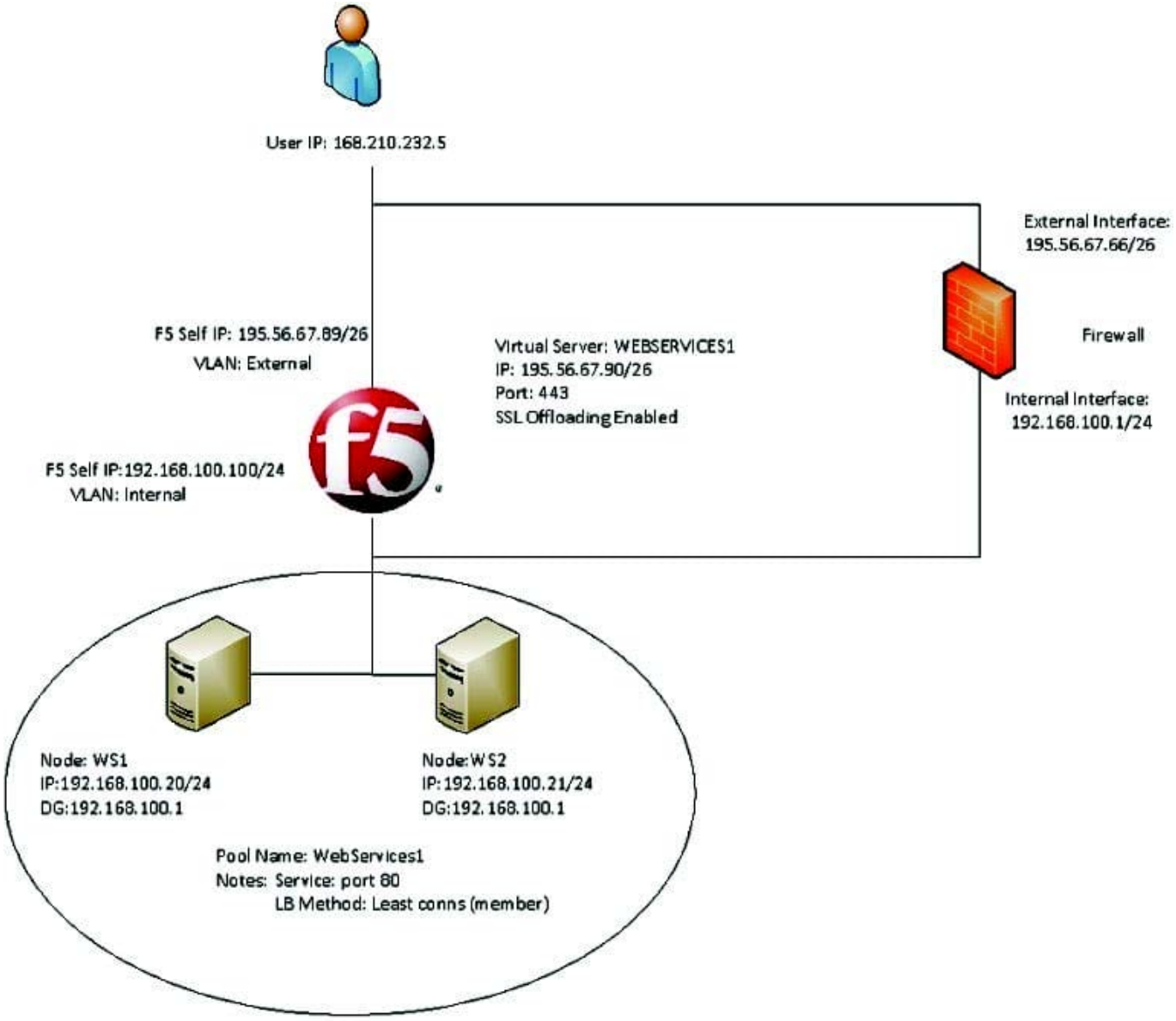
C. The port 80 and port 443 connections are balanced to the same node.

D. The port 80 and port 443 connections are balanced to different nodes.

Correct Answer: D

QUESTION 13

-- Exhibit -- Exhibit -



Refer to the exhibit.

Users receive an error when attempting to connect to the website https://website.com. The website has a DNS record of 195.56.67.90. The upstream ISP has confirmed that there is nothing wrong with the routing between the user and the

LTM device.

The following tcpdump outputs have been captured:

External Vlan, filtered on IP 168.210.232.5

00:25:07.598519 IP 168.210.232.5.33159 > 195.56.67.90.https: S 1920647964:1920647964(0) win 8192

00:25:07.598537 IP 195.56.67.90.https > 168.210.232.5.33159: S 2690691360:2690691360(0) ack 1920647965 win 4350

00:25:07.598851 IP 168.210.232.5.33160 > 195.56.67.90.https: S 2763858764:2763858764(0) win 8192

00:25:07.598858 IP 195.56.67.90.https > 168.210.232.5.33160: S 1905576176:1905576176(0) ack 2763858765 win 4350

Internal Vlan, filtered on IP 168.210.232.5

00:31:46.171124 IP 168.210.232.5.33202 > 192.168.100.20.http: S 2389057240:2389057240(0) win 4380

What is the problem?

A. The filters on the tcpdumps are incorrect.

B. The DNS entry for website.com is incorrect.

C. The virtual server \\'WEBSERVICES1\\' is listening on the incorrect port.

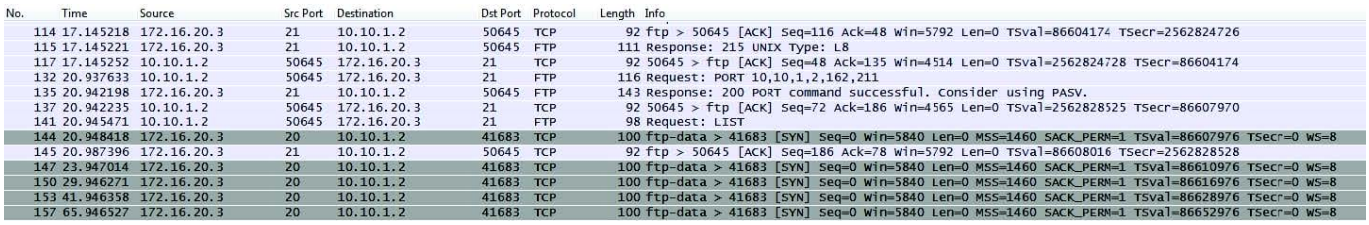
D. The firewall is dropping the connection coming from the pool members returned to the client.

E. The subnet masks of the pool members of pool WebServices1 and the f5 \\'Internal\\' Vlan are incorrect.

Correct Answer: D

QUESTION 14

-- Exhibit



No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
114	17.145218	172.16.20.3	21	10.10.1.2	50645	TCP	92	ftp > 50645 [ACK] Seq=116 Ack=48 Win=5792 Len=0 TSval=86604174 TSecr=2562824726
115	17.145221	172.16.20.3	21	10.10.1.2	50645	FTP	111	Response: 215 UNIX Type: L8
117	17.145252	10.10.1.2	50645	172.16.20.3	21	TCP	92	50645 > ftp [ACK] Seq=48 Ack=135 Win=4514 Len=0 TSval=2562824728 TSecr=86604174
132	20.937633	10.10.1.2	50645	172.16.20.3	21	FTP	116	Request: PORT 10,10,1,2,162,211
135	20.942198	172.16.20.3	21	10.10.1.2	50645	FTP	143	Response: 200 PORT command successful. Consider using PASV.
137	20.942235	10.10.1.2	50645	172.16.20.3	21	TCP	92	50645 > ftp [ACK] Seq=72 Ack=186 Win=4565 Len=0 TSval=2562828525 TSecr=86607970
141	20.945471	10.10.1.2	50645	172.16.20.3	21	FTP	98	Request: LIST
144	20.948418	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=86607976 TSecr=0 WS=8
145	20.987396	172.16.20.3	21	10.10.1.2	50645	TCP	92	ftp > 50645 [ACK] Seq=186 Ack=78 Win=5792 Len=0 TSval=86608016 TSecr=2562828528
147	23.947014	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=86610976 TSecr=0 WS=8
150	29.946271	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=86616976 TSecr=0 WS=8
153	41.946358	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=86628976 TSecr=0 WS=8
157	65.946527	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=86652976 TSecr=0 WS=8

-- Exhibit -Refer to the exhibit.

An LTM Specialist is investigating reports that users are unable to perform some commands through an FTP virtual server. The LTM Specialist performs a capture on the server side of the LTM device.

What is the issue with the application?

A. data connection failing

B. LIST command disallowed

C. PORT command disallowed

D. command connection failing

Correct Answer: A

QUESTION 15

An LTM Specialist with the Administrator role and terminal access of "tmsh" logs in via ssh and is in the Traffic Manager Shell. The LTM Specialist wants to enter the bash shell to review log files. Which command does the LTM Specialist need to run to access the bash shell?

A. exit

B. quit

C. run /cli bash

D. run /util bash

Correct Answer: D