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.geekcert.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

-- 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 creates 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, but they are able to connect to the application servers directly. Which change to the LTM device configuration will resolve the problem?

A. Install the server certificate/key and enable Proxy SSL.

B. Use the serverssl-insecure-compatible serverssl profile.

C. Configure the clientssl profile to require a client certificate.

D. Install the client\\'s issuing Certificate Authority certificate on the LTM device.

Correct Answer: A

QUESTION 2

-- Exhibit

```
Client IP address:      10.0.0.1
Virtual Server:         11.0.0.1
Web Server:             12.0.0.1

Capture taken on Web server interface eth1:12.0.0.1
-----------------------------------------------------

01:35:35.141396 IP 10.0.0.1.35285 > 12.0.0.1.http: S 3230388980:3230388980(0) win 8192 <mss 1416,nop,wscale 8,nop,nop,sackOK>
01:35:35.141466 IP 12.0.0.1.http > 10.0.0.1.35285: S 2242263384:2242263384(0) ack 3230388981 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 4>
01:35:35.177621 IP 10.0.0.1.25079 > 12.0.0.1.http: P 3570570638:3570571021(383) ack 1931745822 win 255
01:35:35.184475 IP 12.0.0.1.http > 10.0.0.1.25079: . 1:1417(1416) ack 383 win 700
01:35:35.184517 IP 12.0.0.1.http > 10.0.0.1.25079: . 1417:2833(1416) ack 383 win 700
01:35:35.184533 IP 12.0.0.1.http > 10.0.0.1.25079: P 2833:3905(1072) ack 383 win 700
01:35:35.297647 IP 10.0.0.1.35285 > 12.0.0.1.http: . ack 1 win 66
01:35:35.337992 IP 10.0.0.1.25079 > 12.0.0.1.http: . ack 2833 win 259
01:35:35.539349 IP 10.0.0.1.25079 > 12.0.0.1.http: . ack 3905 win 255
01:35:38.945404 IP 12.0.0.1.http > 10.0.0.1.35285: S 2242263384:2242263384(0) ack 3230388981 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 4>
01:35:39.096377 IP 10.0.0.1.35285 > 12.0.0.1.http: . ack 1 win 66 <nop,nop,sack 1 {0:1}>

Capture taken on LTM interface 0.0
-----------------------------------

17:32:30.828126 IP 10.0.0.1.10120 > 11.0.0.1.http: S 3414174673:3414174673(0) win 8192 <mss 1416,nop,wscale 2,nop,nop,sackOK> in slot1/tmm0 lis=
17:32:30.828172 IP 11.0.0.1.http > 10.0.0.1.10120: S 1751596785:1751596785(0) ack 3414174674 win 4248 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:30.981747 IP 10.0.0.1.10120 > 11.0.0.1.http: . ack 1 win 16638 in slot1/tmm0 lis=/Common/my_virtual
17:32:30.982820 IP 10.0.0.1.10120 > 11.0.0.1.http: P 1:560(559) ack 1 win 16638 in slot1/tmm0 lis=/Common/my_virtual
17:32:30.982871 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:30.982878 IP 11.0.0.1.http > 10.0.0.1.10120: . ack 560 win 4807 out slot1/tmm0 lis=/Common/my_virtual
17:32:33.982895 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:37.182627 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:40.382728 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:43.582864 IP 11.0.0.1.http > 10.0.0.1.10120: R 1:55(54) ack 560 win 4807 out slot1/tmm0 lis=/Common/my_virtual
```

-- Exhibit -

Refer to the exhibit.

A pair of LTM devices are configured for HA. The LTM Specialist observes from a capture that there is a successful connection from a client directly to a web server and an unsuccessful connection from a client via the LTM device to the same

web server.

Which two solutions will solve the configuration problem? (Choose two.)

A. Configure SNAT on the pool.

B. Configure SNAT on the virtual server.

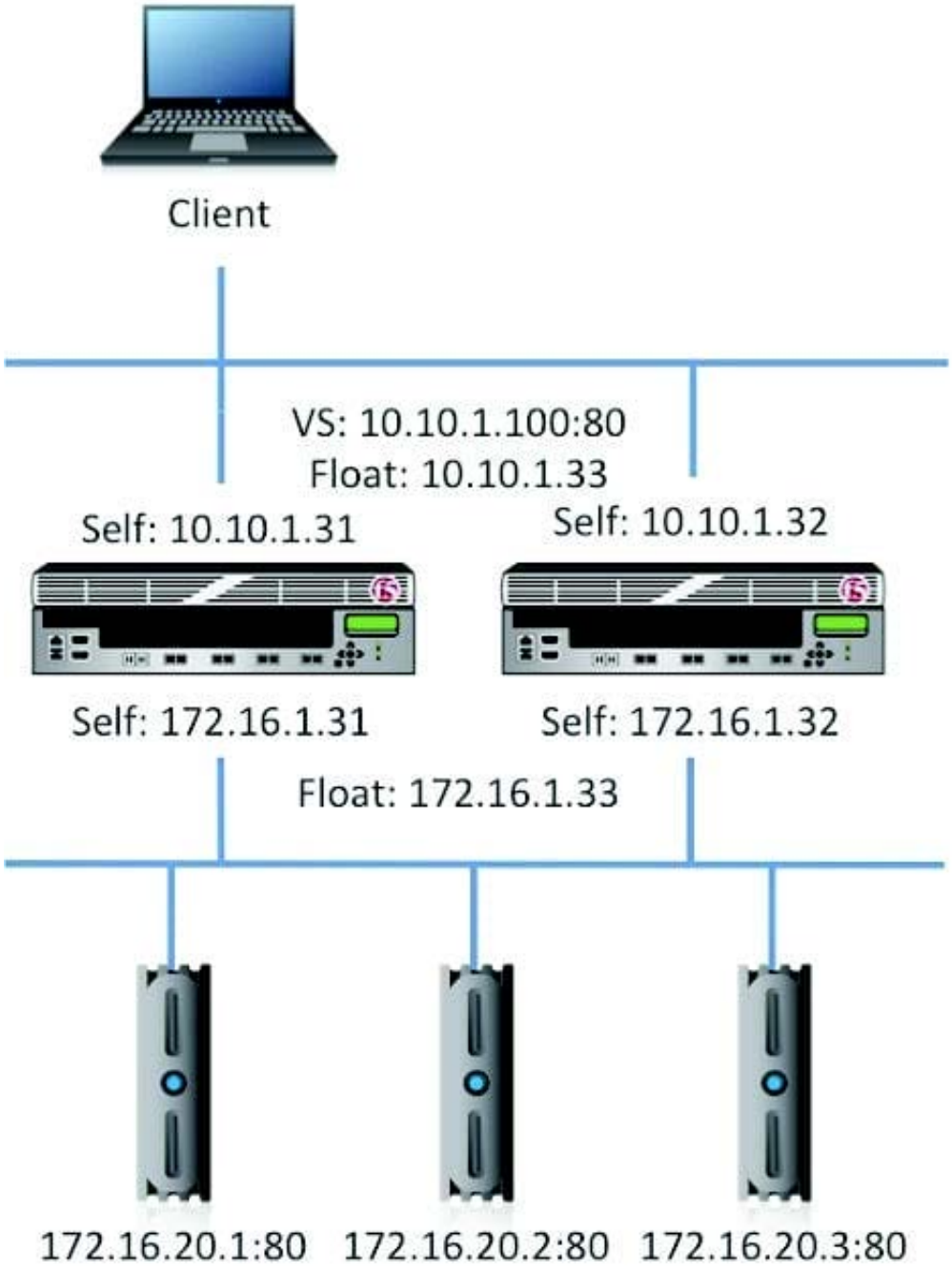
C. Change server default gateway to point at LTM internal self IP.

D. Change server default gateway to point at LTM internal floating IP.

Correct Answer: BD

QUESTION 3

-- Exhibit



-- Exhibit -Refer to the exhibit.

A server administrator notices that one server is intermittently NOT being sent any HTTP requests. The server logs display no issues. The LTM Specialist notices log entries stating the node (172.16.20.1) status cycling between down and up.

The pool associated with the virtual server (10.10.1.100) has a custom HTTP monitor applied. Which tcpdump filter will help trace the monitor?

A. tcpdump -i internal port 80 and host 172.16.1.31

B. tcpdump -i external port 80 and host 10.10.1.100

C. tcpdump -i internal port 80 and host 172.16.1.33

D. tcpdump -i external port 80 and host 172.16.20.1

Correct Answer: A

QUESTION 4

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 5

-- Exhibit

```
Virtual Server details

Type                                Standard
Protocol                            TCP
Protocol Profile (Client)      tcp-wan-optimised
Protocol Profile (Server)      tcp-lan-optimised
OneConnect Profile                  None
NTLM Conn Pool                      None
HTTP Profile                        None
FTP Profile                         None
Stream Profile                      None
XML Profile                         None
SSL Profile (Client)           None
SSL Profile (Server)           None
Authentication Profiles        None

RTSP Profile                        None
SMTP Profile                        None
Diameter Profile               None
SIP Profile                         None
Statistics Profile                  None

SNAT Pool                           None
Rate Class                          None
Traffic Class                       None

Connection Limit               None
Connection Mirroring           None
Address Translation            Enabled
Port Translation               Enabled
Source Port                         Preserve
Clone Pool (Client)            None
Clone Pool (Server)            None
Last Hop Pool                       None

Pool details:

10.40.242.12: 443
10.40.242.13: 443
```

-- Exhibit -Refer to the exhibit.

An LTM device is used to load balance web content over a secure channel.

The developers of the web content have done a trace using an HTTP profiler application. They believe that allowing the LTM device to compress traffic to the client will improve performance. The client can utilize GZIP or deflate compression

algorithms.

An LTM Specialist must implement the compression.

The LTM Specialist has completed the following actions:

1.

Create the relevant profile.

2.

Apply the relevant profile to the virtual server (VS).

After applying the relevant profile, the LTM device is failing to compress the traffic. Instead, the traffic is being served with an error.

What is the problem?

A. The incorrect compression algorithm is applied to the compression profile.

B. The LTM device CANNOT SSL offload the traffic in order to read and compress it.

C. The Protocol Profile (Client) option of "Allow Compression" needs to be enabled.

D. The Protocol Profile (Server) option of "Allow Compression" needs to be enabled.

Correct Answer: B