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.leads4pass.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

An LTM Specialist must perform a hot fix installation from the command line.

What is the correct procedure to ensure that the installation is successful?

A. import the hot fix to the /var/shared/images directory check the integrity of the file with an md5 checksum tmsh apply sys software hotfix volume .iso

B. import the hot fix to the /var/shared/images directory check the integrity of the file with an md5 checksum tmsh install sys software hotfix .iso volume

C. import the hot fix to the /shared/images directory check the integrity of the file with an md5 checksum tmsh apply sys software hotfix volume .iso

D. import the hot fix to the /shared/images directory check the integrity of the file with an md5 checksum tmsh install sys software hotfix .iso volume

Correct Answer: D

QUESTION 2

-- 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 3

These log entries can have different root causes:

Jun 28 05:01:21 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: enabled Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071431:5: Attempting to connect to CMI peer 1.1.1.2 port 6699 Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071432:5: CMI peer connection established to 1.1.1.2 port 6699 Jun 28 05:01:26 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: disabled, all peers are connected

Which two commands should be used to obtain additional information on these entries? (Choose two.)

A. tmsh show /sys mcpd

B. bigstart status mcpd

C. tmsh modify /sys db log.mcpd.level value debug

D. tmsh modify /sys db log.cmi.level value debug

Correct Answer: BC

QUESTION 4

-- 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 5

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