Get The Most Updated 303 Dumps To BIG-IP ASM Certification [Q252-Q268

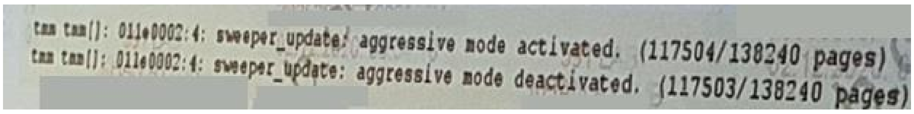
Get The Most Updated 303 Dumps To BIG-IP ASM Certification F5 Certified 303 Dumps Questions Valid 303 Materials QUESTION 252

An LTM HTTP pool has an associated monitor that sends a string equal to &#8216;GET /test.html&#8217;.

Which two configurations could an LTM Specialist implement to allow server administrators to disable their pool member servers without logging into the LTM device? (Choose two.)
* Set monitor to transparent and ask the server team to set string &#8216;TRANSPARENT&#8217; in test.html.
* Set &#8216;receive string&#8217; equal to &#8216;SERVER UP and ask the server team to set string &#8216;SERVER DOWN&#8217; in test.html.
* Set &#8216;alias&#8217; equal to &#8216;SERVER DOWN&#8217; and ask the server team to set string &#8216;SERVER DOWN&#8217; in test.html.
* Set &#8216;receive disable string&#8217; equal to &#8216;SERVER DOWN&#8217; and ask the server team to set string &#8216;SERVER DOWN&#8217; in test.html.
* Set &#8216;disable pool member&#8217; equal to &#8216;SERVER UP&#8217; and ask the server team to set string &#8216;SERVER DOWN&#8217; in test.html.

QUESTION 253

AN LTM Specialist receives reports that an external company application is having reliability issues. The F5 Administrator finds the following in /vat/log/ltm file.



```
tmm tmm[]: 011e0002:4: sweeper_update: aggressive mode activated. (117504/138240 pages)
tmm tmm[]: 011e0002:4: sweeper_update: aggressive mode deactivated. (117503/138240 pages)
```

The LTM Specialist determines that the F5 LTMdevice is entering into Aggressive Mode Adaptive Reaping, which is causing the site reliability issues.

What is the most likely reason that the LTM device has entered into Aggressive Mode Adaptive Reaping?

* The LTM device exceeds licensed traffic limits.
* The site has too many licensed modules.
* The LTM device has not provisioned AVR.
* The site is under DDOS attack

QUESTION 254

An LTM Specialist is configuring a client profile to offload processing a new application Company policy requires that clients can resume session for up to 30 minutes, but must renegotiate a new session after that.

Which setting should the LTM Specialist change to satisfy this requirement?

* Renegotiate Max Record Delay
* Renegotiation period
* Cachesize
* Cache timeout

Explanation

Question stem requires that you can resume SSL session within 30 minutes, then you need to define the ssl cache time in 30 minutes

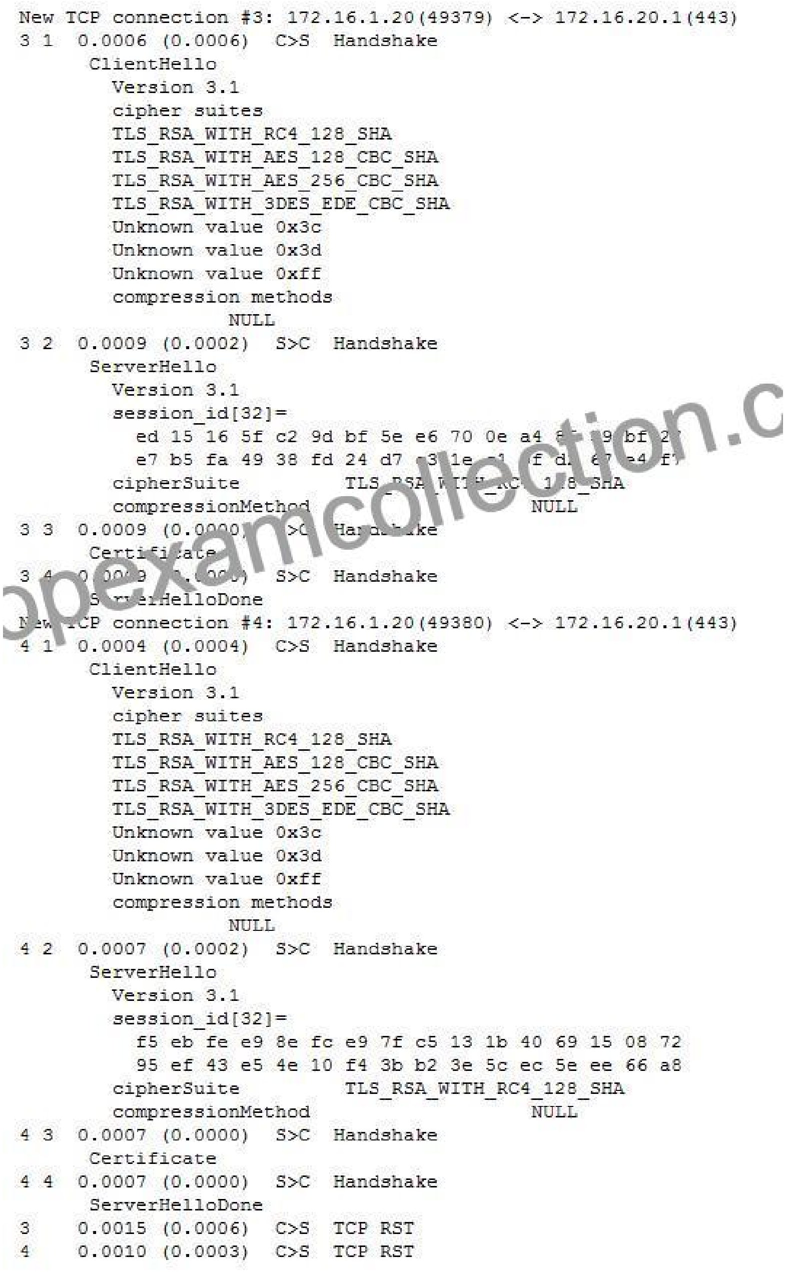
QUESTION 255

A BIG-IP Administrator assigns the default http health monitor to a pool that has three members listening on port 80 When the administrator connects to each pool member via the CURL utility, two of the members respond with a status of 404 Not Found while the third responds with 200 OK. What will the pool show for member availability?

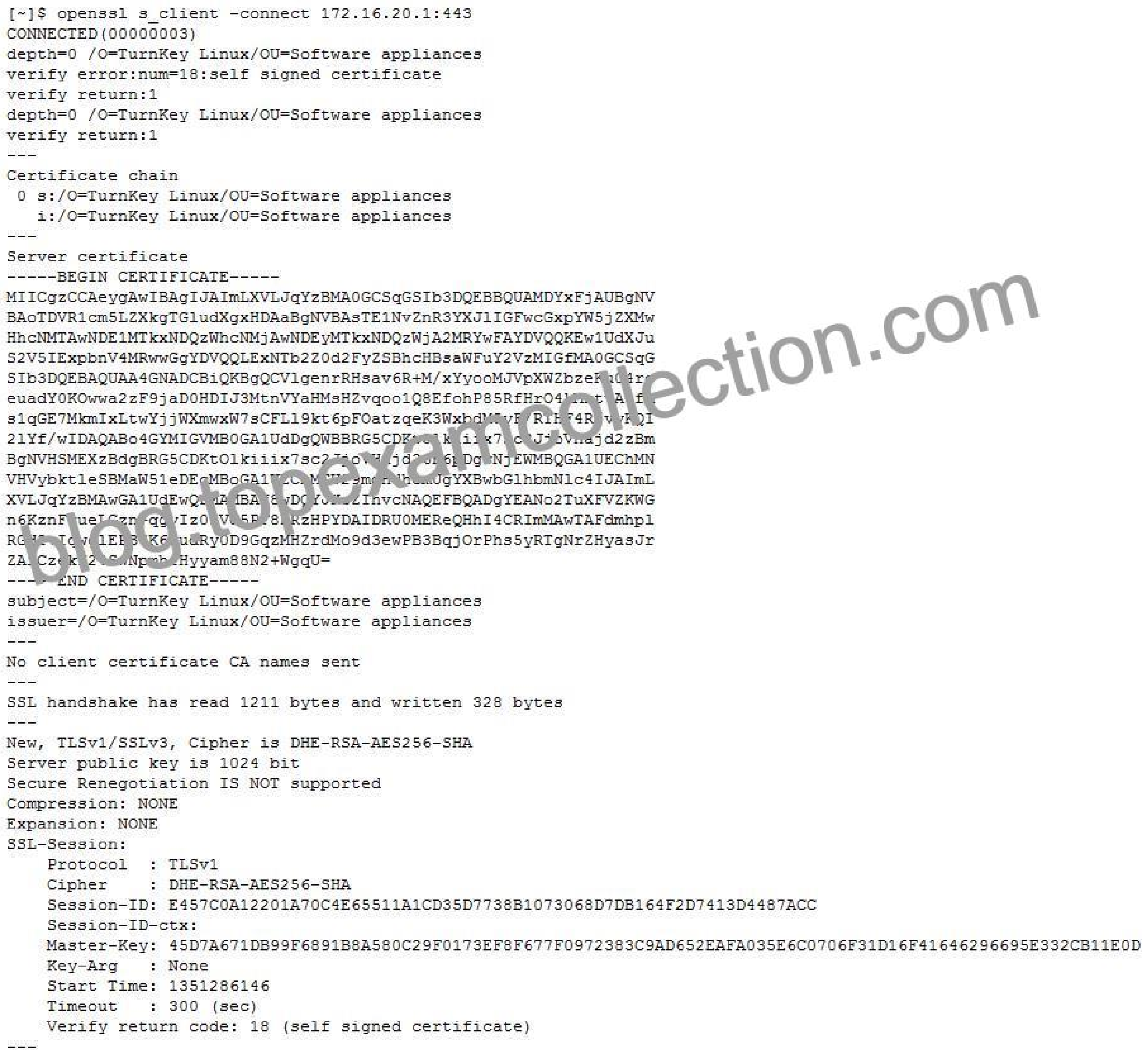
* All members offline.
* Two members offline and one member online.
* Two members online and one member offline.
* All members online.

QUESTION 256

&#8212; Exhibit &#8211;



```
New TCP connection #3: 172.16.1.20(49379) <-> 172.16.20.1(443)
3 1  0.0006 (0.0006)  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
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
3 2  0.0009 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          ed 15 16 5f c2 9d bf 5e e6 70 0e a4 8f 39 bf 27
          e7 b5 fa 49 38 fd 24 d7 e3 1e c1 9f d1 67 e4 f7
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
3 3  0.0009 (0.0000)  S>C  Handshake
      Certificate
3 4  0.0009 (0.0000)  S>C  Handshake
      ServerHelloDone
New TCP connection #4: 172.16.1.20(49380) <-> 172.16.20.1(443)
4 1  0.0004 (0.0004)  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
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
4 2  0.0007 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          f5 eb fe e9 8e fc e9 7f c5 13 1b 40 69 15 08 72
          95 ef 43 e5 4e 10 f4 3b b2 3e 5c ec 5e ee 66 a8
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
4 3  0.0007 (0.0000)  S>C  Handshake
      Certificate
4 4  0.0007 (0.0000)  S>C  Handshake
      ServerHelloDone
3    0.0015 (0.0006)  C>S  TCP RST
4    0.0010 (0.0003)  C>S  TCP RST
```



```
[~]$ openssl s_client -connect 172.16.20.1:443
CONNECTED(00000003)
depth=0 /O=TurnKey Linux/OU=Software appliances
verify error:num=18:self signed certificate
verify return:1
depth=0 /O=TurnKey Linux/OU=Software appliances
verify return:1
---
Certificate chain
 0 s:/O=TurnKey Linux/OU=Software appliances
   i:/O=TurnKey Linux/OU=Software appliances
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICgzCCAeygAwIBAgIJAImLXVLJqYzBMA0GCSqGSIb3DQEBBQUAMDYxFjAUBgNV
BAoTDVR1cm5LZXkgTGludXgxHDAaBgNVBAsTE1NvZnR3YXJlIGFwcGxpYW5jZXMw
HhcNMTAwNDE1MTkxNDQzWhcNMjAwNDEyMTkxNDQzWjA2MRYwFAYDVQQKEw1UdXJu
S2V5IExpbnV4MRwwGgYDVQQLExNTb2Z0d2FyZSBhcHBsaWFuY2VzMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCVlgenrRHsav6R+M/xYyooMJVpXWZbzeK[illegible]4r[illegible]
euadY0KOwwa2zF9jaD0HDIJ3MtnVYaHMsHZvqoo1Q8EfohP85RfHrO4[illegible]A[illegible]f[illegible]
s1qGE7MkmIxLtwYjjWXmwxW7sCFLl9kt6pFOatzqeK3Wxbd[illegible]RIH[illegible]4R[illegible]KQI
21Yf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBRG5CDK[illegible]k[illegible]x7[illegible]J[illegible]bVhajd2zBm
BgNVHSMEXzBdgBRG5CDKtOlkiiix7sc2[illegible]jd2[illegible]6p[illegible]Dg[illegible]NjEWMBQGA1UEChMN
VHVybktleSBMaW51eDEcMBoGA1U[illegible]gYXBwbGlhbmNlc4IJAImL
XVLJqYzBMAwGA1UdEwQ[illegible]MA[illegible]BA[illegible]8wDQYJ[illegible]ZIhvcNAQEFBQADgYEANo2TuXFVZKWG
n6KznF[illegible]ueLCzn[illegible]qg[illegible]Iz0[illegible]V[illegible]5P[illegible]8[illegible]RzHPYDAIDRU0MEReQHhI4CRImMAwTAFdmhpl
RG[illegible]Iq[illegible]v[illegible]1EB[illegible]K6[illegible]uRy0D9GqzMHZrdMo9d3ewPB3BqjOrPhs5yRTgNrZHyasJr
ZA[illegible]Cz[illegible]k[illegible]2[illegible]Np[illegible]Hyyam88N2+WgqU=
-----END CERTIFICATE-----
subject=/O=TurnKey Linux/OU=Software appliances
issuer=/O=TurnKey Linux/OU=Software appliances
---
No client certificate CA names sent
---
SSL handshake has read 1211 bytes and written 328 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: E457C0A12201A70C4E65511A1CD35D7738B1073068D7DB164F2D7413D4487ACC
    Session-ID-ctx:
    Master-Key: 45D7A671DB99F6891B8A580C29F0173EF8F677F0972383C9AD652EAFA035E6C0706F31D16F41646296695E332CB11E0D
    Key-Arg   : None
    Start Time: 1351286146
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
```

&#8212; Exhibit &#8212;

Refer to the exhibits.

After upgrading LTM from v10 to v11, users are unable to connect to an application. The virtual server is using a client SSL profile for re-terminating SSL for payload inspection, but a server SSL profile is being used to re-encrypt the request.

A client side ssldump did NOT show any differences between the traffic going directly to the server and the traffic being processed by the LTM device. However, packet capture was done on the server, and differences were noted.

Which modification will allow the LTM device to process the traffic correctly?

* Enable Strict Resume.
* Change Secure Renegotiation to &#8220;Request.&#8221;

* Enable ProxySSL option in the server SSL profile.
* Change to different ciphers on the server SSL profile.

QUESTION 257

The BIG-IP appliance fails to boot. The BIG-IP Administrator needs to run the End User Diagnostics (EUD) utility to collect data to send to F5 Support.

Where can the BIG-IP Administrator access this utility?
* Console Port
* Internal VLAN interface
* External VLAN interface
* Management Port

QUESTION 258

A web server administrator informs the BIG-IP Administrator that web servers are overloaded Starting next month, the BIG-IP device will terminate SSL to reduce web server load. The BIG-IP device is ready using client SSL client profile and Rules on HTTP level. What actions should the BIG-IP Administrators to achieve the desired configuration?
* Remove the server SSL profile and configure the Pool Members to use HTTP
* Remove the client SSL profile and configure the Pool Members to US HTTP
* Remove the chart SSL profile and change the Virtual Server to accept HTTP
* Remove the server SSL profile and change the Virtual Server to accept HTTP traffic

QUESTION 259

What should the 816-IP Administrator provide when opening a new ticket with F5 Support?
* bigip.license file
* QKViewfile
* Device root password
* SSL private keys

QUESTION 260

An LTM Specialist must reconfigure a BIG-IP system that load balances traffic to a web application. The security department has informed the LTM Specialist that the following cipher string must be used for TLS connections from BIG-IP to the web application.

NATIVE:IMDS:EXPORT:IDHE:EDH@SPEED

In which virtual server profile should the cipher string be configured?
* Server SSL

CB. Client SSL
* SPDY profile
* Rewrite profile
Explanation

Require SSL and flow F5 to server, server ssl

QUESTION 261

A BIG-IP Administrator needs to apply a health monitor for a pool of database servers named DB_Pool that uses TCP port 1521.

Where should the BIG-IP Administrator apply this monitor?
* Local Traffic > Profiles > Protocol > TCP
* Local Traffic > Nodes > Default Monitor
* Local Traffic > Pools > De Pool > Members
* Local Traffic > Pools > DB Pool > Properties

QUESTION 262

A BIG-IP Administrator is creating a new Trunk on the BIG-IP device. What objects should be added to the new Trunk being created?
* Interfaces
* Network routes
* VLANS
* IP addresses
Explanation

trunk is a portchannel, you need to add a physical interface.

QUESTION 263

Exhibit.

&#8211; The ITM devices LTM 1 and LTM2 are configured in Device Group X (Sync-Failover)

&#8211; LTM3 and LTM4 are configured in Device Group Y (Sync-Only)

&#8211; An LTM specialist configures Device Group Z (Sync-Only) to keep several profiles in (sync-Only) to keep several profiles in sync across all devices.

&#8211; Device GROUP X has four Traffic Groups A.B.C and D configured.

&#8211; Device Group Y has four Traffic Groups E, F, G, and H configured

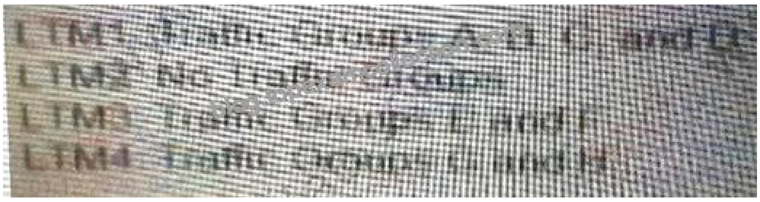
&#8211; Auto Fallback IS NOT Enabled.

&#8211; Each Device group is healthy and able to pass traffic for any traffic groupassigned to that Device Group.

The data center that contains LTM2 and LTM4 loses power. After 10 minutes; power is restored and all devices are up and healthy.

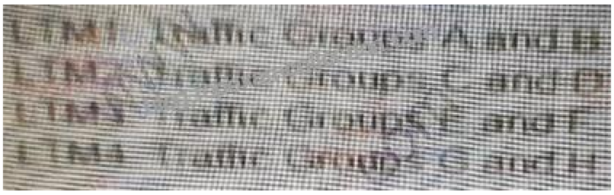
What is the state of each Traffic Group on each ITM device after power is restored?

A)



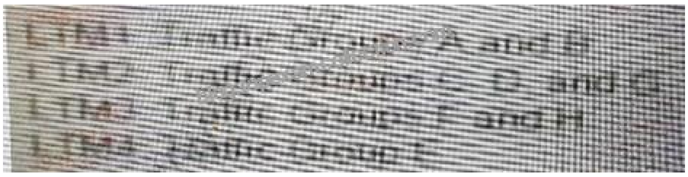
LTM1 Traffic Groups A, B, C, and D
LTM2 No Traffic Groups
LTM3 Traffic Groups E and F
LTM4 Traffic Groups G and H

B)



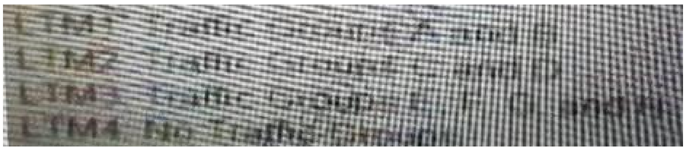
LTM1 Traffic Groups A and B
LTM2 Traffic Groups C and D
LTM3 Traffic Groups E and F
LTM4 Traffic Groups G and H

C)



LTM1 Traffic Groups A and B
LTM2 Traffic Groups C, D, and G
LTM3 Traffic Groups F and H
LTM4 Traffic Group E

D)



LTM1 Traffic Groups A and B
LTM2 Traffic Groups C and D
LTM3 Traffic Groups E, F, G, and H
LTM4 No Traffic Groups

- Option A
- Option B
- Option C

* Option D

QUESTION 264

A BIG-IP Administrator has configured a BIG-IP cluster with remote user authentication against dcOl f5trn.com. Only local users can successfully log into the system. Configsync is also failing.

Which two tools should the 8IG-IP Administrator use to further investigate these issues? (Choose two)

* ntpq
* pam_timestamp_check
* passwd
* pwck
* dig

QUESTION 265

An active/standby pair of LTM devices deployed with network failover are working as desired. After external personnel perform maintenance on the network, the LTM devices are active/active rather than active/standby.

No changes were made on the LTM devices during the network maintenance.

Which two actions would help determine the cause of the malfunction? (Choose two.)

* checking that the configurations are synchronized
* checking the configuration of the VLAN used for failover
* checking the configuration of the VLAN used for mirroring
* checking the open ports in firewalls between the LTM devices
* checking synchronization of system clocks among the network devices

QUESTION 266

The following decoded TCPDump capture shows the trace of a failing health monitor.

```
00:00:13.245104 IP 10.29.29.60.51947 > 10.0.0.12.http: P 1:59(58) ack 1 win 46 <nop,nop,timestamp

2494782300 238063789> out slot1/tmm3 lis=

0x0000: 4500 006e 3b19 4000 4006 ce0c 0a1d 1d3c E..n;.@.@&#8230;&#8230;<

0x0010: 0a00 000c caeb 0050 8be5 aca3 dd65 e3e1 &#8230;&#8230;.P&#8230;..e..

0x0020: 8018 002e 1b41 0000 0101 080a 94b3 5b5c &#8230;..A&#8230;&#8230;..[

0x0030: 0e30 90ad 4745 5420 2f74 6573 745f 7061 .0..GET./test_pa

0x0040: 6765 2e68 746d 6c20 4854 5450 312e 310d ge.html.HTTP1.1.

0x0050: 0a48 6f73 743a 200d 0a43 6f6e 6e65 6374 .Host:&#8230;Connect

0x0060: 696f 6e3a 2043 6c6f 7365 0d0a 0d0a 0105 ion:.Close&#8230;&#8230;
0x0070: 0100 0003 00 &#8230;..

00:00:13.245284 IP 10.0.0.12.http > 10.29.29.60.51947: . ack 59 win 362 <nop,nop,timestamp 238063789

2494782300> in slot1/tmm3 lis=

0x0000 0ffd 0800 4500 00c9 6f68 4000 8006 755d &#8230;.E&#8230;oh@&#8230;u]

0x0010 0a29 0015 0a29 0103 0050 e0d6 4929 90eb .)&#8230;)&#8230;P..I)..

0x0020 6f12 d83c 8019 fab3 9b31 0000 0101 080a o..<&#8230;..1&#8230;&#8230;

0x0030 0068 4e10 5240 6150 4854 5450 2f31 2e31 .hN.R@aPHTTP/1.1

0x0040 2034 3030 2042 6164 2052 6571 7565 7374 .400.Bad.Request

0x0050 0d0a 436f 6e74 656e 742d 5479 7065 3a20 ..Content-Type:.

0x0060 7465 7874 2f68 746d 6c0d 0a44 6174 653a text/html..Date:

0x0070 2054 6875 2c20 3231 204a 616e 2032 3031 .Mon,.01.Jan.201

0x0080 3020 3138 3a35 383a 3537 2047 4d54 0d0a 2.00:00:01.GMT..

0x0090 436f 6e6e 6563 7469 6f6e 3a20 636c 6f73 Connection:.clos

0x00a0 650d 0a43 6f6e 7465 6e74 2d4c 656e 6774 e..Content-Lengt

0x00b0 683a 2032 300d 0a0d 0a3c 6831 3e42 6164 h:.20&#8230;.<h1>Bad

0x00c0 2052 6571 7565 7374 3c2f 6831 3e .Request</h1>
```

The health monitor is sending the string shown in the capture; however, the server response is NOT as expected. The correct response should be an HTML page including the string &#8216;SERVER IS UP&#8217;.

What is the issue?
* The /test_page.html does NOT exist on the web server.
* Incorrect syntax in send string. &#8216;HTTP1.1&#8217; should be &#8216;HTTP/1.1&#8217;.
* Incorrect syntax in send string. &#8216;Connection: Close&#8217; should be &#8216;Connection: Open&#8217;.
* The wrong HTTP version is specified in the send string. Version 1.2 should be used instead of version

1.1.

QUESTION 267

An LTM device pool has suddenly been marked down by a monitor. The pool consists of members

10.0.1.1:443 and 10.0.1.2:443 and are verified to be listening. The affected virtual server is 10.0.0.1:80.

Which two tools should the LTM Specialist use to troubleshoot the associated HTTPS pool monitor via the command line interface?

(Choose two.)
* curl
* telnet
* ssldump
* tcpdump

QUESTION 268

A company plans to launch a huge marketing campaign and expects increase demand of their secure website.

With the current virtual server setup, the LTM Specialist expects that the LTM device will reach its capacity limits. For the wen application to function properly. Cookies persistence is required. The LTM Specialist needsto reduce LTM device load without breaking the application.

Which two settings should the LTM Specialist modify to meet the requirement? (Choose two.)
* Remove HTTP compression profile
* Remove HTTP profile
* Remove web acceleration profile.
* Modify virtual Server type to performance (Layer 4)
* Remove ClientSSL profile
Explanation

It is required that cookie persist must be used and http profile must be used, and SSL offloading must also be required. It must be in standard mode,excluding BD E.