Number: 301b
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 301b

Exam Name: BIG IP Local Traffic Manager LTM Specialist Maintain & Troubleshoot

Exam A

QUESTION 1
-- Exhibit --

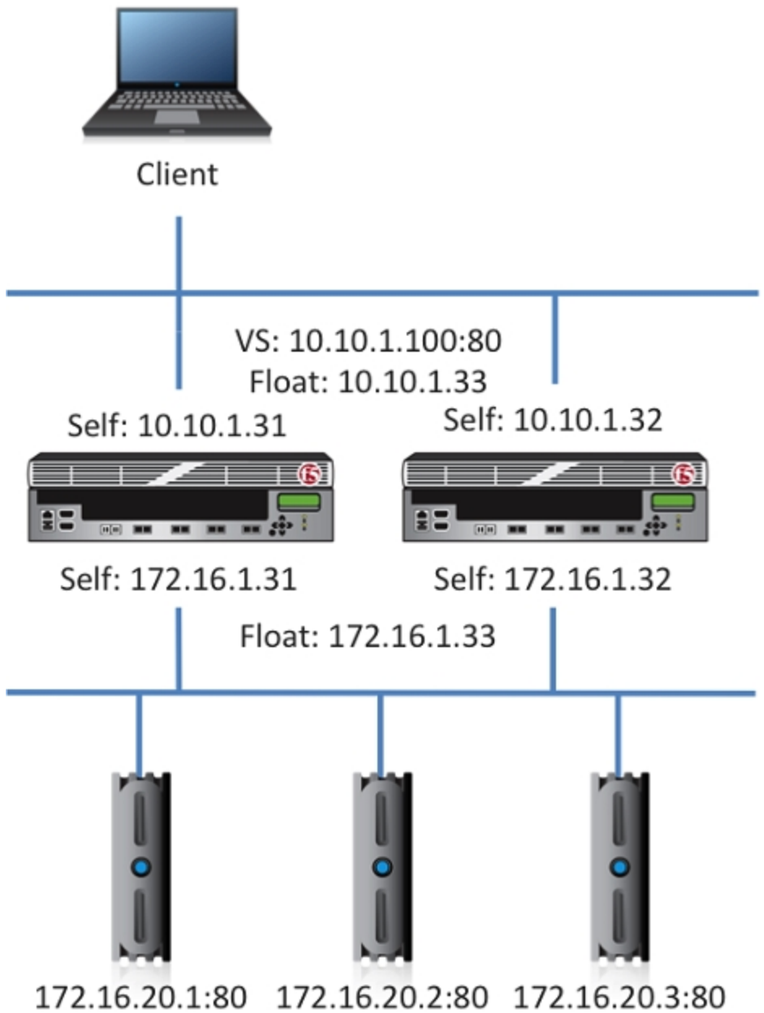
```
13:59:08.704108 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53347 > 172.16.20.2.http: S 1829726557:1829726557(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2395417926 0,sackOK,eol>
13:59:08.704144 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 74: 172.16.20.2.http > 10.10.1.30.53347: S 3203430150:3203430150(0) ack 1829726558 win 5792 <mss 1460,sackOK,timestamp 1165862 2395417926,nop,wscale 3>
13:59:08.705365 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 66: 10.10.1.30.53347 > 172.16.20.2.http: . ack 1 win 4380 <nop,nop,timestamp 2395417927 1165862>
13:59:08.705632 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 399: 10.10.1.30.53347 > 172.16.20.2.http: P 1:334(333) ack 1 win 4380 <nop,nop,timestamp 2395417927 1165862>
13:59:08.705647 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 66: 172.16.20.2.http > 10.10.1.30.53347: . ack 334 win 858 <nop,nop,timestamp 1165863 2395417927>
13:59:08.706277 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 528: 172.16.20.2.http > 10.10.1.30.53347: P 1:463(462) ack 334 win 858 <nop,nop,timestamp 1165864 2395417927>
13:59:08.706346 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 66: 172.16.20.2.http > 10.10.1.30.53347: F 463:463(0) ack 334 win 858 <nop,nop,timestamp 1165864 2395417927>
13:59:08.708576 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 66: 10.10.1.30.53347 > 172.16.20.2.http: . ack 464 win 4842 <nop,nop,timestamp 2395417930 1165864>
13:59:08.711554 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 66: 10.10.1.30.53347 > 172.16.20.2.http: F 334:334(0) ack 464 win 4842 <nop,nop,timestamp 2395417933 1165864>
13:59:08.711578 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 66: 172.16.20.2.http > 10.10.1.30.53347: . ack 335 win 858 <nop,nop,timestamp 1165869 2395417933>
13:59:10.440561 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53480 > 172.16.20.3.http: S 2990657892:2990657892(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2395779676 0,sackOK,eol>
13:59:10.440589 00:0c:29:2d:d7:13 > 00:0c:29:36:b6:06, ethertype IPv4 (0x0800), length 74: 172.16.20.3.http > 10.10.1.30.53480: S 3583899489:3583899489(0) ack 2990657893 win 5792 <mss 1460,sackOK,timestamp 1527617 2395779676,nop,wscale 3>
13:59:13.439632 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53480 > 172.16.20.3.http: S 2990657892:2990657892(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2395782676 0,sackOK,eol>
13:59:13.439658 00:0c:29:2d:d7:13 > 00:0c:29:36:b6:06, ethertype IPv4 (0x0800), length 74: 172.16.20.3.http > 10.10.1.30.53480: S 3583899489:3583899489(0) ack 2990657893 win 5792 <mss 1460,sackOK,timestamp 1530617 2395779676,nop,wscale 3>
13:59:16.639821 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53480 > 172.16.20.3.http: S 2990657892:2990657892(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2395785876 0,sackOK,eol>
13:59:16.639842 00:0c:29:2d:d7:13 > 00:0c:29:36:b6:06, ethertype IPv4 (0x0800), length 74: 172.16.20.3.http > 10.10.1.30.53480: S 3583899489:3583899489(0) ack 2990657893 win 5792 <mss 1460,sackOK,timestamp 1533817 2395779676,nop,wscale 3>
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist configures a virtual server that balances HTTP connections to a pool of three application servers. Approximately one out of every three connections to the virtual server fails.
Which two actions will resolve the problem? (Choose two.)

A. Assign a custom HTTP monitor to the pool.
B. Enable SNAT automap on the virtual server.
C. Verify that port lockdown is set to allow port 80.
D. Verify the default gateway on the application servers.
E. Increase the TCP timeout value in the default TCP profile.

Correct Answer: B, D
Section:

QUESTION 2
-- 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
Section:

QUESTION 3
-- Exhibit --

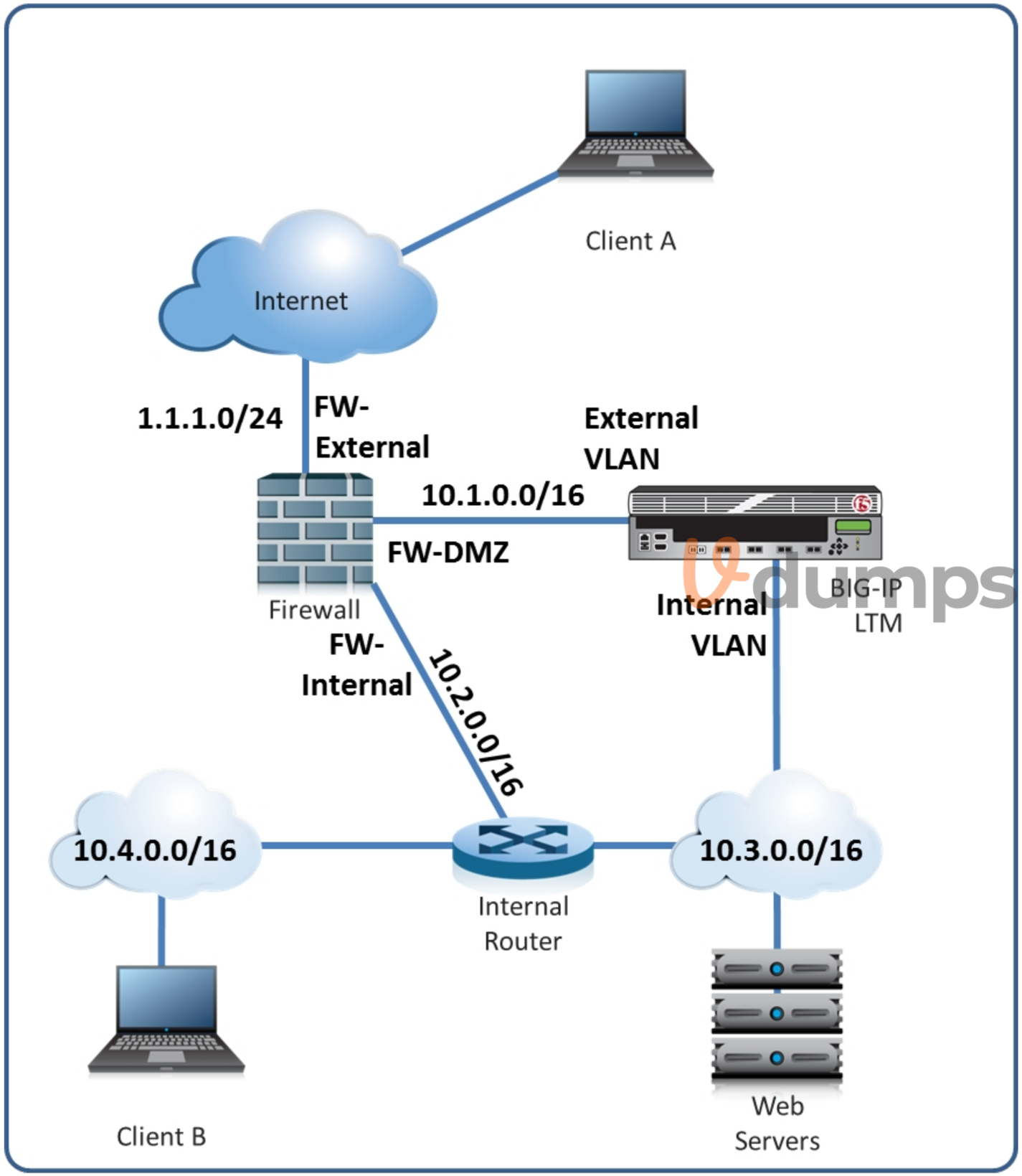
```
19:29:38.095440 IP 10.0.0.2.15885 > 10.0.0.1.http: S 233558736:233558736(0) win 8192 <mss 1416,nop,wscale 2,nop,nop,sackOK> in slot1/tmm1 lis=
   0x0000:  0b71 0800 4500 0034 35b8 4000 7606 5844  .q..E..45.@.v.XD
   0x0010:  ac11 014e ac1d 1d4b 3e0d 0050 0deb d2d0  ...N...K>..P....
   0x0020:  0000 0000 8002 2000 b961 0000 0204 0588  .........a......
   0x0030:  0103 0302 0101 0402 0105 0101 0001 00    ................
19:29:38.095485 IP 10.0.0.1.http > 10.0.0.2.15885: S 2486948624:2486948624(0) ack 233558737 win 4248 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm1 lis=/Common/test-vs
   0x0000:  0b71 0800 4500 0034 a9d4 4000 ff06 5b27  .q..E..4..@...['
   0x0010:  ac1d 1d4b ac11 014e 0050 3e0d 943b d310  ...K...N.P>..;..
   0x0020:  0deb d2d1 8012 1098 6243 0000 0204 05b4  ........bC......
   0x0030:  0103 0300 0402 0000 011c 0100 0001 172f  ................./
   0x0040:  436f 6d6d 6f6e 2f61 7263 682d 6263 6172  Common/test-vs

19:29:38.251761 IP 10.0.0.2.15885 > 10.0.0.1.http: . ack 1 win 16638 in slot1/tmm1 lis=/Common/test-vs
   0x0000:  0b71 0800 4500 0028 35d9 4000 7706 572f  .q..E..(5.@.w.W/
   0x0010:  ac11 014e ac1d 1d4b 3e0d 0050 0deb d2d1  ...N...K>..P....
   0x0020:  943b d311 5010 40fe 71a7 0000 011c 0101  .;..P.@.q.......
   0x0030:  0001 172f 436f 6d6d 6f6e 2f61 7263 682d  .../Common/arch-
   0x0040:  6263 6172 642d 7465 7374                 bcard-test
19:29:38.252723 IP 10.0.0.2.15885 > 10.0.0.1.http: P 1:426(425) ack 1 win 16638 in slot1/tmm1 lis=/Common/test-vs
   0x0000:  0b71 0800 4500 01d1 35da 4000 7706 5585  .q..E...5.@.w.U.
   0x0010:  ac11 014e ac1d 1d4b 3e0d 0050 0deb d2d1  ...N...K>..P....
   0x0020:  943b d311 5018 40fe 558e 0000 4745 5420  .;..P.@.U...GET.
   0x0030:  2f42 4947 2d49 505f 4d6f 6475 6c65 5f49  /some-file-name.
   0x0060:  7064 6620 4854 5450 2f31 2e31 0d0a 4163  pdf.HTTP/1.1..Ac
   0x0070:  6365 7074 3a20 2a2f 2a0d 0a52 616e 6765  cept:.*/*..Range
   0x0080:  3a20 6279 7465 733d 3234 3537 3630 2d32  :.bytes=245760-2
   0x0090:  3632 3134 330d 0a41 6363 6570 742d 456e  62143..Accept-En
   0x00a0:  636f 6469 6e67 3a20 677a 6970 2c20 6465  coding:.gzip,.de
   0x00b0:  666c 6174 650d 0a55 7365 722d 4167 656e  flate..User-Agen
   0x00c0:  743a 204d 6f7a 696c 6c61 2f34 2e30 2028  t:.Mozilla/4.0.(
   0x00d0:  636f 6d70 6174 6962 6c65 3b20 4d53 4945  compatible;.MSIE
   0x00e0:  2038 2e30 3b20 5769 6e64 6f77 7320 4e54  .8.0;.Windows.NT
   0x00f0:  2036 2e31 3b20 574f 5736 343b 2054 7269  .6.1;.WOW64;.Tri
   0x0100:  6465 6e74 2f34 2e30 3b20 534c 4343 323b  dent/4.0;.SLCC2;
   0x0110:  202e 4e45 5420 434c 5220 322e 302e 3530  ..NET.CLR.2.0.50
   0x0120:  3732 373b 202e 4e45 5420 434c 5220 332e  727;..NET.CLR.3.
   0x0130:  352e 3330 3732 393b 202e 4e45 5420 434c  5.30729;..NET.CL
   0x0140:  5220 332e 302e 3330 3732 393b 204d 6564  R.3.0.30729;.Med
   0x0150:  6961 2043 656e 7465 7220 5043 2036 2e30  ia.Center.PC.6.0
   0x0160:  3b20 2e4e 4554 342e 3043 3b20 496e 666f  ;..NET4.0C;.Info
   0x0170:  5061 7468 2e33 3b20 2e4e 4554 342e 3045  Path.3;..NET4.0E
   0x0180:  3b20 4d53 2d52 5443 204c 4d20 383b 2041  ;.MS-RTC.LM.8;.A
   0x0190:  736b 5462 4f52 4a2f 352e 3135 2e31 2e32  skTbORJ/5.15.1.2
   0x01a0:  3232 3239 290d 0a48 6f73 743a 2031 3732  2229)..Host:.10.
   0x01b0:  2e32 392e 3239 2e37 350d 0a43 6f6e 6e65  0.0.1......Conne
   0x01c0:  6374 696f 6e3a 204b 6565 702d 416c 6976  ction:.Keep-Aliv
   0x01d0:  650d 0a0d 0a01 1c01 0100 0117 2f43 6f6d  e............/Com
   0x01e0:  6d6f 6e2f 6172 6368 2d62 6361 7264 2d74  mon/test-vs
19:29:38.252761 IP 10.0.0.1.http > 10.0.0.2.15885: . ack 426 win 4673 out slot1/tmm1 lis=/Common/test-vs
   0x0000:  0b71 0800 4500 0028 a9d8 4000 ff06 5b2f  .q..E..(..@...[/
   0x0010:  ac1d 1d4b ac11 014e 0050 3e0d 943b d311  ...K...N.P>..;..
   0x0020:  0deb d47a 5010 1241 9ebb 0000 011c 0100  ...zP..A........
   0x0030:  0001 172f 436f 6d6d 6f6e 2f61 7263 682d  .../Common/test-vs

19:29:38.252774 IP 10.0.0.1.http > 10.0.0.2.15885: R 1:50(49) ack 426 win 4673 out slot1/tmm1 lis=/Common/test-vs
   0x0000:  0b71 0800 4500 0059 a9da 4000 ff06 5afc  .q..E..Y..@...Z.
   0x0010:  ac1d 1d4b ac11 014e 0050 3e0d 943b d311  ...K...N.P>..;..
   0x0020:  0deb d47a 5014 1241 8e5b 0000 4249 472d  ...zP..A.[..BIG-
   0x0030:  4950 3a20 5b30 7831 3430 3264 6334 3a31  IP:.[0x1402dc4:1
   0x0040:  3432 375d 204e 6f20 706f 6f6c 206d 656d  427].No.pool.mem
   0x0050:  6265 7220 6176 6169 6c61 626c 6501 1c01  ber.available...
   0x0060:  0000 0117 2f43 6f6d 6d6f 6e2f 6172 6368  ..../Common/test-vs
```

-- Exhibit --
Refer to the exhibit.
A user is unable to access an HTTP application via a virtual server.
What is the cause of the failure?

A. The host header requires a host name.
B. The virtual server is in the disabled state.
C. The Connection: Keep-Alive header is set.
D. There is no pool member available to service the request.

Correct Answer: D
Section:

QUESTION 4
-- Exhibit --


Client A
Internet
1.1.1.0/24
FW-
External
External
VLAN
10.1.0.0/16
FW-DMZ
Firewall
FW-
Internal
10.2.0.0/16
Internal
VLAN
BIG-IP
LTM
10.4.0.0/16
Internal
Router
10.3.0.0/16
Client B
Web
Servers

-- Exhibit --
Refer to the exhibit.
A layer 2 nPath routing configuration has been deployed. A packet capture contains a client connection packet with the following properties:
Source IP: <Virtual Server>
Destination IP: <Client A>
At which two locations could the packet capture have been taken? (Choose two.)

A. the network interface of web server
B. the DMZ interface of the Internet firewall
C. the internal interface of the Internet firewall
D. the external VLAN interface of the LTM device

Correct Answer: A, C
Section:

QUESTION 5
-- Exhibit --

```
Monitor definition:

ltm monitor http test2 {
    defaults-from http
    destination *:*
    interval 5
    recv "200 OK"
    send "GET /webmail HTTP/1.1\\r\\nHost: webmail.example.com\\r\\nConnection: close\\r\\n\\r\\n"
    time-until-up 0
    timeout 16
}

HTTP Headers from tcpdump:

GET /webmail HTTP/1.1
Host: webmail.example.com
Connection: close

HTTP/1.1 301 Moved Permanently
Date: Tue, 16 Oct 2012 20:23:22 GMT
Server: Apache/2.2.3 (CentOS)
Location: http://webmail.example.com/webmail/
Content-Length: 327
Connection: close
```

-- Exhibit --
Refer to the exhibit.
An HTTP monitor always marks the nodes in the pool as down. The monitor's definition and the HTTP headers from the monitor request and response are provided.
What is the issue?

A. The response is compressed.
B. The send string is incorrect.
C. The monitor timeout is too short.
D. The monitor is NOT configured to follow the redirect.

Correct Answer: B

Section:

QUESTION 6
-- Exhibit --

```
ltm monitor http http_head {
    defaults-from http
    destination *:*
    interval 5
    recv <html>
    send "HEAD / HTTP/1.0\\r\\n\\r\\n"
    time-until-up 0
    timeout 16
}
ltm pool srv1_http_pool {
    members {
        192.168.2.1:http {
            address 192.168.2.1
            session monitor-enabled
            state down
        }
    }
    monitor http_head
}


TCPDUMP Output:

HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 24 Oct 2012 18:45:53 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
X-Powered-By: PHP/5.4.4
Connection: close
Content-Type: text/html
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is troubleshooting a new HTTP monitor on a pool. The pool member is functioning correctly when accessed directly through a browser. However, the monitor is marking the member as down. The LTM Specialist captures the monitor traffic via tcpdump.
What is the issue?

A. The server is marking the connection as closed.
B. The pool member is rejecting the monitor request.
C. The monitor request is NOT returning the page body.
D. The 'time-until-up' setting on the monitor is incorrect.

Correct Answer: C
Section:

QUESTION 7
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
Section:

QUESTION 8
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 <volume_name> <hotfix_name>.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 <hotfix_name>.iso volume <volume_name>
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 <volume_name> <hotfix_name>.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 <hotfix_name>.iso volume <volume_name>

Correct Answer: D
Section:

QUESTION 9
Which two alerting capabilities can be enabled from within an application visibility reporting (AVR) analytics profile? (Choose two.)

A. sFlow
B. SNMP
C. e-mail
D. LCD panel alert
E. high speed logging (HSL)

Correct Answer: B, C
Section:

QUESTION 10
What is a benefit provided by F5 Enterprise Manager?

A. Enterprise Manager allows administrators to analyze traffic flow and create custom application IPS signatures.
B. Enterprise Manager allows administrators to establish baseline application usage and generate an alert if an administratively set threshold for the application is exceeded.
C. Enterprise Manager allows administrators to identify application vulnerabilities. Virtual patches are then automatically generated and applied to remediate the detected application vulnerability.
D. Enterprise Manager allows administrators to monitor all application traffic. Configuration optimization suggestions based on the observed traffic patterns are then generated for the administrator to review and apply.

Correct Answer: B
Section:

QUESTION 11
Which two items can be logged by the Application Visibility Reporting analytics profile? (Choose two.)

A. User Agent

B. HTTP version
C. HTTP Response Codes
D. Per Virtual Server CPU Utilization

Correct Answer: A, C
Section:

QUESTION 12
Which file should be modified to create custom SNMP alerts?

A. /config/alert.conf
B. /etc/alertd/alert.conf
C. /config/user_alert.conf
D. /etc/alertd/user_alert.conf

Correct Answer: C
Section:

QUESTION 13
An LTM Specialist has set up a custom SNMP alert.
Which command line tool should the LTM Specialist use to test the alert?

A. logger
B. logtest
C. testlog
D. snmptest

Correct Answer: A
Section:

QUESTION 14
An LTM Specialist is customizing local traffic logging.
Which traffic management OS alert level provides the most detail?

A. Alert
B. Notice
C. Critical
D. Emergency
E. Informational

Correct Answer: E
Section:

QUESTION 15
A new web application is hosted at www.example.net, but some clients are still pointing to the legacy web application at www.example.com.
Which iRule will allow clients referencing www.example.com to access the new application?

A. when HTTP_REQUEST { if {[HTTP::host] equals 'www.example.*' }{ HTTP::redirect 'http://www.example.net' } }
B. when HTTP_REQUEST { if {[HTTP::host] equals 'www.example.com' }{ HTTP::redirect 'http://www.example.net' } }
C. when HTTP_DATA { if {[HTTP::host] equals 'www.example.*' }{ HTTP::redirect 'http://www.example.net' } }
D. when HTTP_RESPONSE { if {[HTTP::host] equals 'www.example.com' }{ HTTP::redirect 'http://www.example.net' } }

Correct Answer: B
Section:

QUESTION 16
Which iRule will instruct the client's browser to avoid caching HTML server responses?

A. when HTTP_REQUEST { if {[HTTP::header Content-Type] equals 'html'} { HTTP::header insert Pragma 'no-cache' HTTP::header insert Expires 'Fri, 01 Jan 1990 00:00:00 GMT' HTTP::header replace Cache-Control 'no-cache,no-store,must-revalidate' } }
B. when HTTP_REQUEST { if {[HTTP::header Content-Type] contains 'html'} { HTTP::header insert Pragma 'no-cache' HTTP::header insert Expires 'Fri, 01 Jan 1990 00:00:00 GMT' HTTP::header replace Cache-Control 'no-cache,no-store,must-revalidate' } }
C. when HTTP_RESPONSE { if {[HTTP::header Content-Type] contains 'html'} { HTTP::header insert Pragma 'no-cache' HTTP::header insert Expires 'Fri, 01 Jan 1990 00:00:00 GMT' HTTP::header replace Cache-Control 'no-cache,no-store,must-revalidate' } }
D. when HTTP_RESPONSE { if {[HTTP::header Content-Type] equals 'html'} { HTTP::header insert Pragma 'no-cache' HTTP::header insert Expires 'Fri, 01 Jan 1990 00:00:00 GMT' HTTP::header replace Cache-Control 'no-cache,no-store,must-revalidate' } }

Correct Answer: C
Section:

QUESTION 17
An IT administrator wants to log which server is being load balanced to by a user with IP address 10.10.10.25.
Which iRule should the LTM Specialist use to fulfill the request?

A. when SERVER_CONNECTED { if { [IP::addr [IP::remote_addr]] equals 10.10.10.25]} { log local0. 'client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]' } }
B. when CLIENT_ACCEPTED { if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25]} { log local0. 'client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]' } }
C. when SERVER_CONNECTED { if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25]} { log local0. 'client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]' } }
D. when CLIENT_ACCEPTED { if { [IP::addr [IP::remote_addr] equals 10.10.10.25]} { log local0. 'client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]' } }

Correct Answer: C
Section:

QUESTION 18
A customer needs to intercept all of the redirects its application is sending to clients. When a redirect is matched, the customer needs to log a message including the client IP address.
Which iRule should be used?

A. when HTTP_RESPONSE { if { [HTTP::is_3xx] } { log local0. 'redirecting client ip address [IP::addr [IP::remote_addr]]' } }
B. when HTTP_REQUEST { if { [HTTP::is_301] } { log local0. 'redirecting client ip address [IP::addr [IP::remote_addr]]' } }
C. when HTTP_REQUEST { if { [HTTP::is_redirect] } { log local0. 'redirecting client ip address [IP::addr [IP::remote_addr]]' } }
D. when HTTP_RESPONSE { if { [HTTP::is_redirect] } { log local0. 'redirecting client ip address [IP::addr [IP::remote_addr]]' } }

Correct Answer: D
Section:

QUESTION 19
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
Section:

QUESTION 20
Which iRule will reject any connection originating from a 10.0.0.0/8 network?

A. when CLIENT_ACCEPTED { set remote_ip [IP::addr [IP::remote_addr] mask 8] switch $remote_ip { '10.0.0.0' { reject } '11.0.0.0' { pool pool_http1} default { pool http_pool } } }
B. when CLIENT_ACCEPTED { set remote_ip [IP::addr [IP::local_addr] mask 8] switch $remote_ip { '10.0.0.0' { reject } '11.0.0.0' { pool pool_http1} default { pool http_pool } } }
C. when CLIENT_ACCEPTED { set remote_ip [IP::addr [IP::client_addr] mask 255.0.0.0] switch $remote_ip { '10.0.0.0' { reject } '11.0.0.0' { pool pool_http1} default { pool http_pool } } }
D. when CLIENT_ACCEPTED { set remote_ip [IP::addr [IP::local_addr] mask 255.0.0.0] switch $remote_ip { '10.0.0.0' { reject } '11.0.0.0' { pool pool_http1} default { pool http_pool } } }

Correct Answer: C
Section:

QUESTION 21
There is a fault with an LTM device load balanced trading application that resides on directly connected VLAN vlan-301. The application virtual server is 10.0.0.1:80 with trading application backend servers on subnet 192.168.0.0/25. The LTM Specialist wants to save a packet capture with complete payload for external analysis.
Which command should the LTM Specialist execute on the LTM device command line interface?

A. tcpdump -vvv -w /var/tmp/trace.cap 'net 192.168.0.0/25'
B. tcpdump -vvv -s 0 -w /var/tmp/trace.cap 'net 192.168.0.0/25'
C. tcpdump -vvv -nni vlan-301 -w /var/tmp/trace.cap 'net 192.168.0.0/25'
D. tcpdump -vvv -s 0 -nni vlan-301 -w /var/tmp/trace.cap 'net 192.168.0.0/25'

Correct Answer: D
Section:

QUESTION 22
An LTM Specialist has just captured trace /var/tmp/trace.cap for site www.example.com while listening on virtual address 10.0.0.1:443 configured on partition Application
A . The data payload being captured is SSL encrypted.
Which command should the LTM Specialist execute to decrypt the data payload?

A. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/Common_d/certificate_d/:Common:www.example.com.crt_1
B. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/Common_d/certificate_key_d/:Common:www.example.com.key_1
C. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/ApplicationA_d/certificate_d/:ApplicationA:www.example.com.crt_1
D. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/ApplicationA_d/certificate_key_d/:ApplicationA:www.example.com.key_1

Correct Answer: B
Section:

QUESTION 23
An LTM Specialist must perform a packet capture on a virtual server with an applied standard FastL4 profile. The virtual server 10.0.0.1:443 resides on vlan301.
Which steps should the LTM Specialist take to capture the data payload successfully while ensuring no other virtual servers are affected?

A. The standard FastL4 profile should have PVA acceleration disabled. Then the packet capture tcpdump -ni vlan301 should be executed on the command line interface.
B. The packet capture tcpdump -ni vlan301 should be executed on the command line interface. There is no need to change profiles or PVA acceleration.
C. A new FastL4 profile should be created and applied to the virtual server with PVA acceleration disabled. Then the packet capture tcpdump -ni vlan301 should be executed on the command line interface.
D. The LTM device is under light load. The traffic should be mirrored to a dedicated sniffing device. On the sniffing device, the packet capture tcpdump -ni vlan301 should be executed.

Correct Answer: C
Section:

QUESTION 24
A new VLAN vlan301 has been configured on a highly available LTM device in partition Application A . A new directly connected backend server has been placed on vlan301. However, there are connectivity issues pinging the default gateway. The VLAN self IPs configured on the LTM devices are 192.168.0.251 and 192.168.0.252 with floating IP 192.168.0.253. The LTM Specialist needs to perform a packet capture to assist with troubleshooting the connectivity.
Which command should the LTM Specialist execute on the LTM device command line interface to capture the attempted pings to the LTM device default gateway on VLAN vlan301?

A. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.253'
B. tcpdump -ni vlan301 'host 192.168.0.253'
C. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.251 or host 192.168.0.252'
D. tcpdump -ni vlan301 'host 192.168.0.251 or host 192.168.0.252'

Correct Answer: A
Section:

QUESTION 25
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.)

A. curl
B. telnet
C. ssldump
D. tcpdump

Correct Answer: A, C
Section:

QUESTION 26
An LTM Specialist needs to modify the logging level for tcpdump execution events. Checking the BigDB Key, the following is currently configured:
sys db log.tcpdump.level {
value 'Notice'
}
Which command should the LTM Specialist execute on the LTM device to change the logging level to informational?

A. tmsh set /sys db log.tcpdump.level value informational
B. tmsh set /sys db log.tcpdump.level status informational
C. tmsh modify /sys db log.tcpdump.level value informational
D. tmsh modify /sys db log.tcpdump.level status informational

Correct Answer: C
Section:

QUESTION 27
An application is configured on an LTM device:
Virtual server: 10.0.0.1:80 (VLAN vlan301)
SNAT IP: 10.0.0.1
Pool members: 10.0.1.1:8080, 10.0.1.2:8080, 10.0.1.3:8080 (VLAN vlan302)
Which packet capture should the LTM Specialist perform on the LTM device command line interface to capture only client traffic specifically for this virtual server?

A. tcpdump -ni 0.0:nnn -s 0 'host 10.0.0.1' -w /var/tmp/trace.cap
B. tcpdump -ni vlan301 -s 0 'port 80 and host 10.0.0.1' -w /var/tmp/trace.cap
C. tcpdump -ni vlan301 -s 0 'port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3' -w /var/tmp/trace.cap
D. tcpdump -ni vlan302 -s 0 'port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3' -w /var/tmp/trace.cap
E. tcpdump -ni 0.0:nnn -s 0 '(port 80 and host 10.0.0.1) or (port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap

Correct Answer: B
Section:

QUESTION 28
An application is configured on an LTM device:
Virtual server: 10.0.0.1:80 (VLAN vlan301)
SNAT IP: 10.0.0.1
Pool members: 10.0.1.1:8080, 10.0.1.2:8080, 10.0.1.3:8080 (VLAN vlan302)
Which packet capture should the LTM Specialist perform on the LTM device command line interface to capture only server traffic specifically for this application?

A. tcpdump -ni 0.0:nnn -s 0 'host 10.0.0.1' -w /var/tmp/trace.cap
B. tcpdump -ni vlan301 -s 0 'port 80 and host 10.0.0.1' -w /var/tmp/trace.cap
C. tcpdump -ni vlan302 -s 0 'port 8080 and (host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap
D. tcpdump -ni 0.0:nnn -s 0 '(port 80 and host 10.0.0.1) or (port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap

Correct Answer: C
Section:

QUESTION 29
An LTM Specialist sees these entries in /var/log/ltm:
Oct 25 03:34:31 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborteD. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborteD. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborteD. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborteD. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborteD. 172.16.20.1:443
Oct 25 03:34:33 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborteD. 172.16.20.1:443
Assume 172.16.20.0/24 is attached to the VLAN 'internal.'

What should the LTM Specialist use to troubleshoot this issue?

A. curl -d - -k https://172.16.20.1
B. ssldump -i internal host 172.16.20.1
C. tcpdump -i internal host 172.16.20.1 > /shared/ssl.pcap ssldump < /shared/ssl.pcap
D. tcpdump -s 64 -i internal -w /shared/ssl.pcap host 172.16.20.1 ssldump -r /shared/ssl.pcap

Correct Answer: B
Section:

QUESTION 30
A virtual server for a set of web services is constructed on an LTM device. The LTM Specialist has created an iRule and applied this iRule to the virtual server:
when HTTP_REQUEST {
switch [HTTP::uri] {
'/WS1/ws.jsp' {
log local0. '[HTTP::uri]-Redirected to JSP Pool'
pool JSP
}
default { log local0. '[HTTP::uri]-Redirected to Non-JSP Pool'
pool NonJSP
}
}
}
However, the iRule is NOT behaving as expected. Below is a snapshot of the log:
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/WS.jsp-Redirected to Non-JSP Pool
/ws1/WS.jsp-Redirected to Non-JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/ws1/ws.jsp-Redirected to Non-JSP Pool
What is the problem?

A. The condition in the iRule is case sensitive.
B. The 'switch' command in the iRule has been used incorrectly.
C. The pool members of both pools need to be set up as case-insensitive members.
D. The 'Process Case-Insensitivity' option for the virtual server needs to be selected.

Correct Answer: A
Section:

QUESTION 31
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
Section:

QUESTION 32
Given a tcpdump on an LTM device from both sides of a connection on the External and Internal VLANs, how should an LTM Specialist determine if SNAT is enabled for a particular pool?

A. by checking to see if the Source IP is carried through from the External Vlan to the Internal Vlan
B. by checking to see if the Destination port is carried through from the External Vlan to the Internal Vlan
C. by checking to see if the Source port is carried through from the External Vlan to the Internal Vlan
D. by checking to see if the Destination IP is carried through from the External Vlan to the Internal Vlan

Correct Answer: A
Section:

QUESTION 33
An LTM Specialist has a OneConnect profile and HTTP profile configured on a virtual server to load balance an HTTP application.
The following HTTP headers are seen in a network trace when a client connects to the virtual server:
Clientside:
GET / HTTP/1.1
Host: 192.168.136.100
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-EncodinG. gzip, deflate
Connection: keep-alive
Serverside:
HTTP/1.1 200 OK
DatE. 5 Jun 1989 17:06:55 GMT

Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Content-EncodinG. gzip
Content-LengtH. 3729
X-Cnection: close
Content-TypE. text/html
The LTM Specialist notices the OneConnect feature is working incorrectly.
Why is OneConnect functioning incorrectly?

A. Client must support HTTP/1.0.
B. Client must support HTTP keep-alive.
C. Server must support HTTP/0.9.
D. Server must support HTTP keep-alive.

Correct Answer: D
Section:

QUESTION 34
A virtual server for a set of web services is constructed on an LTM device. The LTM Specialist has created an iRule and applied this iRule to the virtual server:
when HTTP_REQUEST {
switch [HTTP::uri] {
'/ws1/ws.jsp' {
log local0. '[HTTP::uri]-Redirected to JSP Pool'
pool JSP
}
default { log local0. '[HTTP::uri]-Redirected to Non-JSP Pool'
pool NonJSP
}
}
}
However, the iRule is NOT behaving as expected. Below is a snapshot of the log:
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/WS.jsp-Redirected to Non-JSP Pool
/ws1/WS.jsp-Redirected to Non-JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/ws1/ws.jsp-Redirected to Non-JSP Pool
What should the LTM Specialist do to resolve this?

A. Use the followinG. switch -lc [HTTP::uri]
B. Use the followinG. switch [string tolower [HTTP::uri]]
C. Set the 'Case Sensitivity' option of each member to 'None'.
D. Select the 'Process Case-Insensitivity' option for the virtual server.

Correct Answer: B
Section:

QUESTION 35

An LTM device has a virtual server configured as a Performance Layer 4 virtual listening on 0.0.0.0:0 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
Section:

QUESTION 36
An LTM Specialist has configured a virtual server for www.example.com, load balancing connections to a pool of application servers that provide a shopping cart application. Cookie persistence is enabled on the virtual server. Users are able to connect to the application, but the user's shopping cart fails to update. A traffic capture shows the following:
Request:
GET /cart/updatecart.php HTTP/1.1
Host: www.example.com
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94 Safari/537.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-EncodinG. gzip,deflate,sdch
Accept-LanguagE. en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
CookiE. BIGipServerwebstore_pool=353636524.20480.0000
Response:
HTTP/1.1 200 OK
DatE. Wed, 24 Oct 2012 18:00:13 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.1
Set-CookiE. cartID=647A5EA6657828C69DB8188981CB5; path=/; domain=wb01.example.com
Keep-AlivE. timeout=5, max=100
Connection: Keep-Alive
Content-TypE. text/html
No changes can be made to the application.
What should the LTM Specialist do to resolve the problem?

A. Use an iRule to rewrite the cartID cookie domain.
B. Create a universal persistence profile on the cartID cookie.
C. Enable source address persistence as a fallback persistence method.

D. Create a cookie persistence profile with 'match across services' enabled.

Correct Answer: A
Section:

QUESTION 37
An LTM Specialist has been asked to configure a virtual server to distribute connections between a pool of two application servers with addresses 172.16.20.1 and 172.16.20.2. The application servers are listening on TCP ports 80 and 443. The application administrators have asked that clients be directed to the same node for both HTTP and HTTPS requests within the same session.
Virtual servers vs_http and vs_https have been created, listening on 1.2.3.100:80 and 1.2.3.100:443, respectively.
Which configuration option will result in the desired behavior?

A. Create pool app_pool with members 172.16.20.1:any and 172.16.20.2:any Assign app_pool as the default pool for both vs_http and vs_https Disable port translation for vs_http and vs_https
B. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80 Assign pool http_pool as the default pool for both vs_https and vs_https Disable port translation for vs_https Create an SSL persistence profile with 'match across virtual servers' enabled Assign the persistence profile to vs_http.
C. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80 Create pool https_pool with members 172.16.20.1:443 and 172.16.20.2:443 Assign http_pool as the default pool for vs_http Assign https_pool as the default pool for vs_https Create a source address persistence profile with 'match across services' enabled Assign the persistence profile to vs_http and vs_https
D. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80 Create pool https_pool with members 172.16.20.1:443 and 172.16.20.2:443 Assign http_pool as the default pool for vs_http Assign https_pool as the default pool for vs_https Create an SSL persistence profile with 'match across virtual servers' enabled Assign the persistence profile to vs_http

Correct Answer: C
Section:

QUESTION 38
An LTM Specialist is investigating reports from users that SSH connections are being terminated unexpectedly. SSH connections are load balanced through a virtual server. The users experiencing this problem are running SQL queries that take upwards of 15 minutes to return with no screen output. The virtual server is standard with a pool associated and no other customizations.
What is causing the SSH connections to terminate?

A. UDP IP ToS
B. TCP idle timeout
C. The virtual server has no persistence.
D. The pool has Reselect Retries set to 0.

Correct Answer: B
Section:

QUESTION 39
Users in a branch office are reporting a website is always slow. No other users are experiencing the problem. The LTM Specialist tests the website from the external VLAN along with testing the servers directly. All tests indicate normal behavior. The environment is a single HTTP virtual server on the external VLAN with a single pool containing three HTTP pool members on the internal VLAN.
Which two locations are most appropriate to collect additional protocol analyzer data? (Choose two.)

A. a user's machine
B. the switch local to the user
C. the LTM device's internal VLAN
D. the LTM device's external VLAN
E. a user's Active Directory authentication

Correct Answer: A, B
Section:

QUESTION 40
An LTM Specialist has a single HTTPS virtual server doing SSL termination. No server SSL profile is defined. The pool members are on the internal VLAN answering on HTTP port 80. Users with certain browsers are experiencing issues.
Which two locations are most appropriate to gather packets needed to determine the SSL issue? (Choose two.)

A. server interface
B. user's computer
C. LTM device's external VLAN
D. LTM device's internal VLAN
E. LTM device's management interface

Correct Answer: B, C
Section:

QUESTION 41
A user is having issues with connectivity to an HTTPS virtual server. The virtual server is on the LTM device's external vlan, and the pools associated with the virtual server are on the internal vlan. An LTM Specialist does a tcpdump on the external interface and notices that the host header is incomplete.
In which location should the LTM Specialist put a traffic analyzer to gather the most pertinent data?

A. server
B. external VLAN
C. internal VLAN
D. client machine

Correct Answer: D
Section:

QUESTION 42
An application owner claims an LTM device is delaying delivery of an HTTP application. The LTM device has two VLANs, an internal and an external. The application servers reside on the internal VLAN. The virtual server and clients reside on the external VLAN.
With appropriate filters applied, which solution is most efficient for obtaining packet captures in order to investigate the claim of delayed delivery?

A. one capture on interface 0.0
B. one capture on the internal interface
C. one capture on the external interface
D. one capture on the management interface

Correct Answer: A
Section:

QUESTION 43
A client (10.10.1.30) connecting to an HTTPS virtual server (10.10.1.100) with a clientssl profile is getting an SSL error.
Which options will trace this issue?

A. tcpdump -i external -X -e -nn -vvv -w /shared/ssl_problem.cap port 443 and host 10.10.1.30 ssldump -r /shared/ssl_problem.cap -n -x
B. tcpdump -i external -s 0 -w /shared/ssl_problem.cap port 443 and host 10.10.10.30 and host 10.10.1.100 ssldump -r /shared/ssl_problem.cap -n -x
C. tcpdump -i external -X -s 0 -vvv src host 10.10.10.30 and dst host 10.10.1.100 and port 443 > /shared/ssl_problem.cap ssldump -r /shared/ssl_problem.cap -n -x

D. tcpdump -i external -X -e -nn -vv port 443 and host 10.10.1.100 and host 10.10.1.30 > /shared/ssl_problem.cap ssldump -n -x < /shared/ssl_problem.cap

Correct Answer: B
Section:

QUESTION 44
An LTM device is deployed in a one-armed topology. The virtual server, clients, and web servers are connected on the LTM device internal VLAN. A client tries to connect to the virtual server and is unable to establish a connection. A packet capture from the LTM device internal VLAN shows that the HTTP request is being forwarded to the web server.
From which two additional locations should protocol analyzer data be collected? (Choose two.)

A. network interface of web server
B. network interface of client machine
C. internal VLAN interface of LTM device
D. external VLAN interface of LTM device
E. any network interface of the Internet firewall

Correct Answer: A, B
Section:

QUESTION 45
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: A, B
Section:

QUESTION 46
The LTM device is configured for RADIUS authentication. Remote logins are failing and the LTM Specialist must verify the RADIUS configuration.
How should the LTM Specialist check the RADIUS server and shared secret configured on the LTM device?

A. tmsh show running-config /auth radius
B. tmsh show running-config /sys auth radius
C. tmsh show running-config /auth configuration
D. tmsh show running-config /sys auth radius-server

Correct Answer: A
Section:

QUESTION 47
An F5 LTM Specialist needs to perform an LTM device configuration backup prior to RMA swap.

Which command should be executed on the command line interface to create a backup?

A. bigpipe config save /var/tmp/backup.ucs
B. tmsh save /sys ucs /var/tmp/backup.ucs
C. tmsh save /sys config /var/tmp/backup.ucs
D. tmsh save /sys config ucs /var/tmp/backup.ucs

Correct Answer: B
Section:

QUESTION 48
An LTM Specialist notices the following error on the stdout console:
mcpd[2395]: 01070608:0: License is not operational(expired or digital signature does not match contents)
Which command should be executed to verify the LTM device license?

A. bigpipe version
B. tmsh show /sys license
C. tmsh /util bigpipe version
D. tmsh show /sys license status

Correct Answer: B
Section:

QUESTION 49
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.)

A. checking that the configurations are synchronized
B. checking the configuration of the VLAN used for failover
C. checking the configuration of the VLAN used for mirroring
D. checking the open ports in firewalls between the LTM devices
E. checking synchronization of system clocks among the network devices

Correct Answer: B, D
Section:

QUESTION 50
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
Section:

QUESTION 51
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: C, D
Section:

QUESTION 52
Given this as the first packet displayed of an ssldump:
2 2 1296947622.6313 (0.0001) S>CV3.1(74) Handshake
ServerHello
random[32]=
19 21 d7 55 c1 14 65 63 54 23 62 b7 c4 30 a2 f0
b8 c4 20 06 86 ed 9c 1f 9e 46 0f 42 79 45 8a 29
session_id[32]=
c4 44 ea 86 e2 ba f5 40 4b 44 b4 c2 3a d8 b4 ad
4c dc 13 0d 6c 48 f2 70 19 c3 05 f4 06 e5 ab a9
cipherSuite TLS_RSA_WITH_RC4_128_SHA
compressionMethod NULL
In reviewing the rest of the ssldump, the application data is NOT being decrypted.
Why is ssldump failing to decrypt the application data?

A. The application data is encrypted with SSLv3.
B. The application data is encrypted with TLSv1.
C. The data is contained within a resumed TLS session.
D. The BigDB Key Log.Tcpdump.Level needs to be adjusted.

Correct Answer: C
Section:

QUESTION 53
An LTM Specialist is troubleshooting virtual server 10.0.0.1:443 residing on VLAN vlan301. The web application is accessed via www.example.com. The LTM Specialist wants to save a packet capture with complete decrypted payload for external analysis.
Which command should the LTM Specialist execute on the LTM device command line interface?

A. tcpdump -vvv -s 0 'host 10.0.0.1 and port 443' -w /var/tmp/trace.cap
B. tcpdump -vvv -s 0 -ni vlan301 'host 10.0.0.1 and port 443' -w /var/tmp/trace.cap
C. ssldump -Aed -k /config/filestore/files_d/Common_d/certificate_key_d/:Common:www.example.com.key_1 > /var/tmp/trace.cap
D. ssldump -Aed -ni vlan301 -k /config/filestore/files_d/Common_d/certificate_key_d/:Common:www.example.com.key_1 > /var/tmp/trace.cap

Correct Answer: D
Section:

QUESTION 54
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
Section:

QUESTION 55
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
Section:

QUESTION 56
While investigating the cause of a device failover, an LTM Specialist discovers the following events in /var/log/ltm:
01010029:5: Clock advanced by 518 ticks
01010029:5: Clock advanced by 505 ticks
01010029:5: Clock advanced by 590 ticks
01010029:5: Clock advanced by 568 ticks
01010029:5: Clock advanced by 1681 ticks
01010029:5: Clock advanced by 6584 ticks
01140029:5: HA daemon_heartbeat tmm fails action is failover and restart.
010c0026:5: Failover condition, active attempting to go standby.
Which issue caused the failover?

A. NTP being out of sync
B. TMM being descheduled
C. VLAN Fail-safe heartbeats
D. HA missing heartbeat packets

Correct Answer: B
Section:

QUESTION 57
A failover event is recorded in the log messages:
Jan 01 00:00:50 BIG-IP notice sod[5855]: 01140029:5: HA proc_running tmm fails action is go offline and down links.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c0050:5: Sod requests links down.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c0054:5: Offline for traffic group /Common/traffic-group-1.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c003e:5: Offline
Jan 01 00:00:50 BIG-IP notice logger: /usr/bin/tmipsecd --tmmcount 4 ==> /usr/bin/bigstart stop racoon
Jan 01 00:00:50 BIG-IP info lacpd[5502]: 01160016:6: Failover event detected. (Switchboard failsafe disabled while offline)
Jan 01 00:00:51 BIG-IP err bcm56xxd[5296]: 012c0010:3: Failover event detected. Marking external interfaces down. bsx.c(3633)
Jan 01 00:00:51 BIG-IP info bcm56xxd[5296]: 012c0015:6: Link: 1.1 is DOWN
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 0107143c:5: Connection to CMI peer 10.0.0.3 has been removed
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 0107143a:5: CMI reconnect timer: enabled
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 01071431:5: Attempting to connect to CMI peer 10.0.0.3 port 6699
What is the cause of the failover?

A. TMM failed, and VLAN fail-safe initiated the failover.
B. TMM failed, and system fail-safe initiated the failover.
C. Loss of connection to CMI peer 10.0.0.3 initiated the failover.
D. A switchboard failure caused system fail-safe to initiate the failover.

Correct Answer: B
Section:

QUESTION 58
An LTM Specialist has just manually failed the active LTM device over to the standby LTM device. The LTM Specialist notices the newly active LTM device is NOT currently receiving traffic. The LTM Specialist verifies the newly active device is responding to ARP but still no traffic is hitting the virtual servers. The LTM Specialist also notices that the virtual servers eventually start responding.
What should be added to the configuration to resolve the problem?

A. vlan failsafe
B. floating self IP
C. network failover
D. MAC masquerading
E. connection mirroring

Correct Answer: D
Section:

QUESTION 59
-- Exhibit --

```
ltm node /test/10.1.1.1 {
    address 10.1.1.1
}
ltm node /test/10.1.1.2 {
    address 10.1.1.2
}
ltm node /test/10.1.1.3 {
    address 10.1.1.3
}
ltm pool /test/test1_pool {
    members {
        /test/10.1.1.1:80 {
            address 10.1.1.1
        }
        /test/10.1.1.2:8080 {
            address 10.1.1.2
        }
    }
}
ltm pool /test/test2_pool {
    members {
        /test/10.1.1.1:8080 {
            address 10.1.1.1
        }
        /test/10.1.1.3:8080 {
            address 10.1.1.3
        }
    }
}
ltm virtual /test/test1_vs {
    destination /test/172.16.20.1:80
    ip-protocol tcp
    mask 255.255.255.255
    pool /test/test2_pool
    profiles {
        /Common/http { }
        /Common/tcp { }
    }
    translate-address enabled
    translate-port enabled
    vlans-disabled
}
ltm virtual-address /test/172.16.20.1 {
    address 172.16.20.1
    mask 255.255.255.255
    traffic-group /Common/traffic-group-1
}
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is reviewing the 'test' partition.
Which objects, in order, can be removed from the partition?

A. delete pool test1_pool, delete node 10.1.1.2
B. delete node 10.1.1.2, delete pool test2_pool
C. delete pool test1_pool, delete node 10.1.1.2, delete node 10.1.1.1
D. delete virtual test1_vs, delete pool test2_pool, delete node 10.1.1.1
E. delete pool test1_pool, delete pool test2_pool, delete node 10.1.1.3

Correct Answer: A
Section:

QUESTION 60
-- Exhibit --

```
ltm rule /Common/vs1-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs1") && not ([HTTP::uri] starts_with "/app") } {
HTTP::redirect "https://vs1/app/"
return
}
}
}
ltm rule /Common/vs2-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs2") && not ([HTTP::uri] starts_with "/app4") } {
HTTP::redirect "https://vs2/app4/"
return
}
}
}
ltm rule /Common/vs3-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs3") && not ([HTTP::uri] starts_with "/app2") } {
HTTP::redirect "https://vs3/app2/"
return
}
}
}
ltm rule /Common/vs4-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs4") && not ([HTTP::uri] starts_with "/app") } {
HTTP::redirect "https://vs4/app/"
return
}
}
}
ltm rule /Common/vs5-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs5") && not ([HTTP::uri] starts_with "/app3") } {
HTTP::redirect "https://vs5/app3/"
return
}
}
}
```

-- Exhibit --
Refer to the exhibit.
Which two items can be consolidated to simplify the LTM configuration? (Choose two.)

A. /Common/vs1-https-redirect
B. /Common/vs2-https-redirect
C. /Common/vs3-https-redirect

D. /Common/vs4-https-redirect
E. /Common/vs5-https-redirect

Correct Answer: A, D
Section:

QUESTION 61
-- Exhibit --

Data Format	Normalized
Auto Refresh	Disabled Refresh

Search

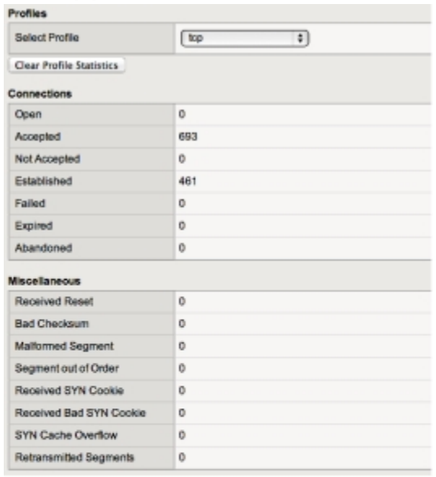
				Bits		Packets		Connections			Requests	Request Queue	
	Status	Pool/Member	Partition / Path	In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age
		DNS_pool	Common	0	0	0	0	0	0	0		0	0
		-- 172.16.20.1:53	Common	0	0	0	0	0	0	0	0	0	0
		-- 172.16.20.2:53	Common	0	0	0	0	0	0	0	0	0	0
		-- 172.16.20.3:53	Common	0	0	0	0	0	0	0	0	0	0
		ecomm_pool	Common	21.6K	60.2K	20	16	0	1	2		0	0
		-- ecomm_server:80	Common	21.6K	60.2K	20	16	0	1	2	5	0	0
		ftp_pool	Common	10.9K	8.9K	24	15	1	1	1		0	0
		-- 172.16.20.1:21	Common	10.9K	8.9K	24	15	1	1	1	0	0	0
		-- 172.16.20.2:21	Common	0	0	0	0	0	0	0	0	0	0
		-- 172.16.20.3:21	Common	0	0	0	0	0	0	0	0	0	0
		hello_world_pool	Common	0	0	0	0	0	0	0		0	0
		-- ecomm_server:81	Common	0	0	0	0	0	0	0	0	0	0
		http_pool	Common	142.2K	1.5M	137	173	0	6	10		0	0
		-- 172.16.20.1:80	Common	43.6K	639.1K	48	66	0	2	3	6	0	0
		-- 172.16.20.2:80	Common	30.7K	369.8K	34	44	0	2	3	4	0	0
		-- 172.16.20.3:80	Common	67.8K	537.2K	55	63	0	2	4	11	0	0
		iOS_pool	Common	0	0	0	0	0	0	0		0	0
		-- ecomm_server:82	Common	0	0	0	0	0	0	0	0	0	0
		server1_80	Common	24.9M	190.0M	56.4K	56.3K	0	1	9.5K		0	0
		-- 172.16.20.1:80	Common	24.9M	190.0M	56.4K	56.3K	0	1	9.5K	0	0	0
		server2_80_pool	Common	24.8M	190.1M	56.3K	56.6K	0	1	9.5K		0	0
		-- 172.16.20.2:80	Common	24.8M	190.1M	56.3K	56.6K	0	1	9.5K	0	0	0
		server_pool	Common	0	0	0	0	0	0	0		0	0
		-- 172.16.20.1:0	Common	0	0	0	0	0	0	0	0	0	0
		-- 172.16.20.2:0	Common	0	0	0	0	0	0	0	0	0	0
		-- 172.16.20.3:0	Common	0	0	0	0	0	0	0	0	0	0
		webgoat_pool	Common	0	0	0	0	0	0	0		0	0
		-- webgoat_8080:8080	Common	0	0	0	0	0	0	0	0	0	0

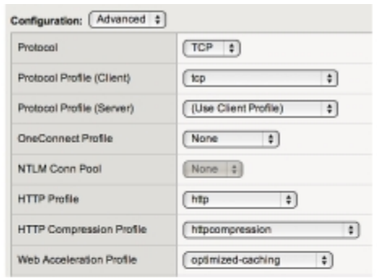
-- Exhibit --
Refer to the exhibit.
Which pool can be removed without affecting client traffic?

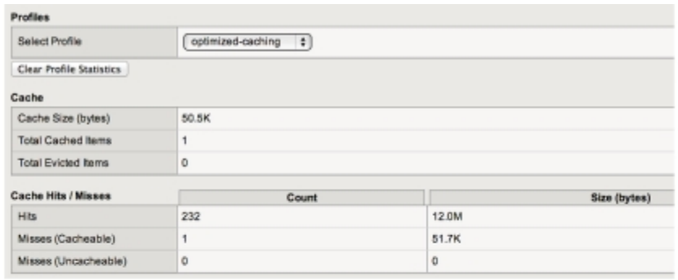
A. ftp_pool
B. http_pool
C. server1_80
D. server_pool

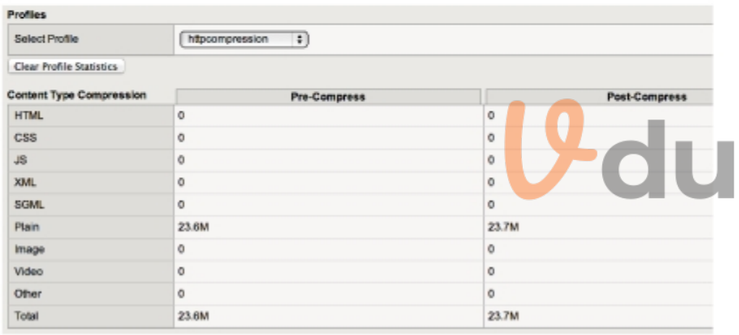
Correct Answer: D
Section:

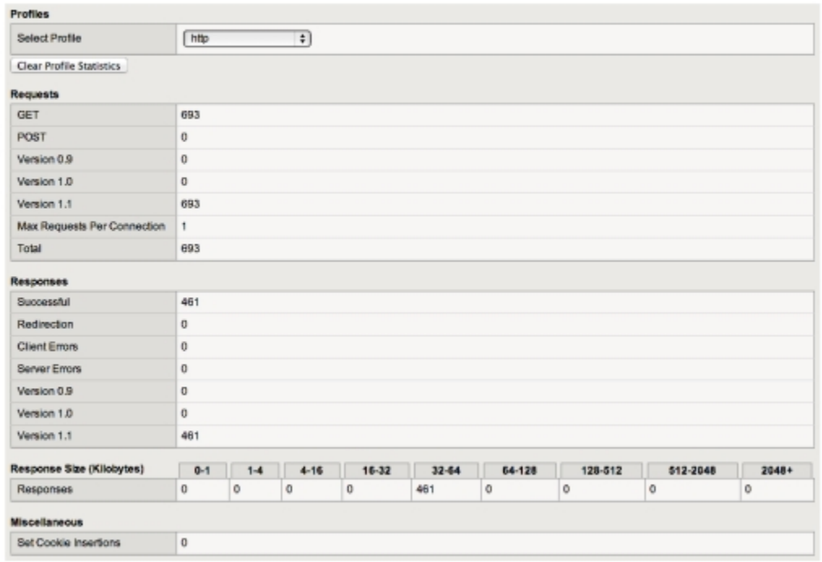
QUESTION 62
-- Exhibit --









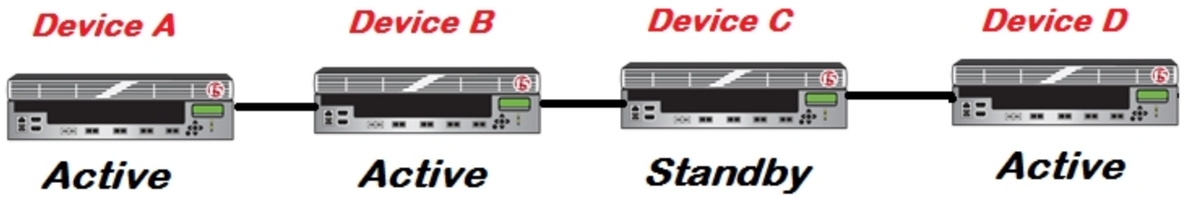


-- Exhibit --
Refer to the exhibit.
Which profile could be removed or changed on this virtual server to reduce CPU load on the LTM device without increasing server side bandwidth usage?

A. tcp
B. http
C. httpcompression
D. optimized-caching

Correct Answer: C
Section:

QUESTION 63
-- Exhibit --

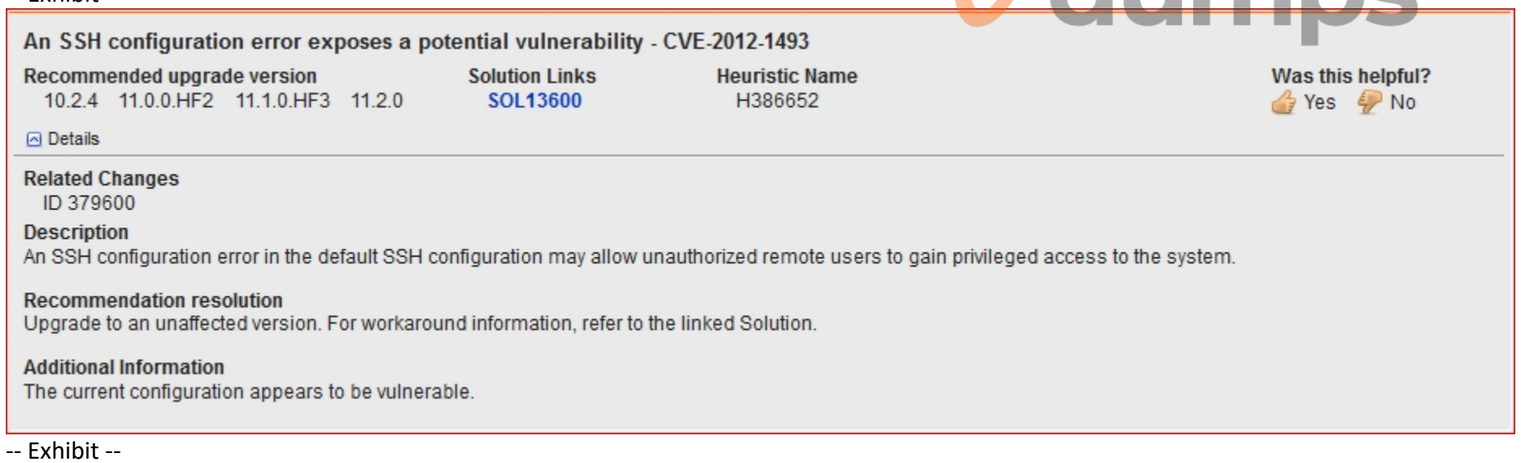


-- Exhibit --
Refer to the exhibit.
An LTM Specialist is upgrading the LTM devices.
Which device should be upgraded first?

A. Device A
B. Device B
C. Device C
D. Device D

Correct Answer: C
Section:

QUESTION 64
-- Exhibit --

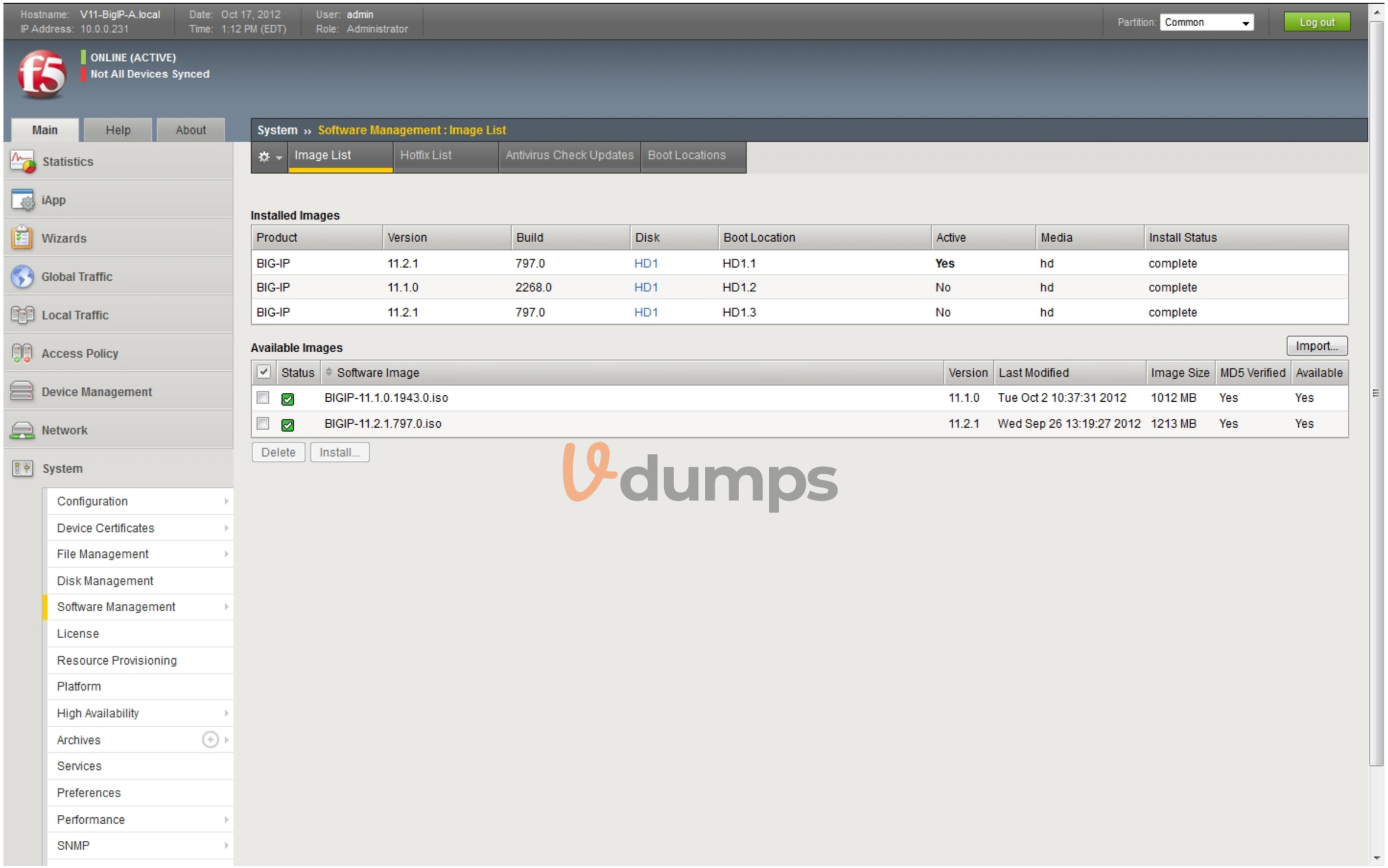


-- Exhibit --
Refer to the exhibit.
An LTM Specialist is working on an LTM 11.0.0 installation and has identified a security vulnerability as shown in the exhibit. The LTM Specialist is tasked with applying the latest available hotfix to resolve the problem.
Which procedure resolves the problem?

A. Browse to System > Software Management > Hotfix List. Import TMOS 11.2.0 to the available hotfix images. Select the imported hotfix image and installation location and click Install.
B. Browse to System > Software Management > Hotfix List. Import 11.1.0.HF3 to the available hotfix images. Select the imported hotfix image and installation location and click Install.
C. Browse to System > Software Management > Image List. Import TMOS 11.2.0 to the available hotfix images. Select the imported hotfix image and installation location and click Install.
D. Browse to System > Software Management > Image List. Import 11.1.0.HF3 to the available hotfix images. Select the imported hotfix image and installation location and click Install.

Correct Answer: B
Section:

QUESTION 65
-- Exhibit --

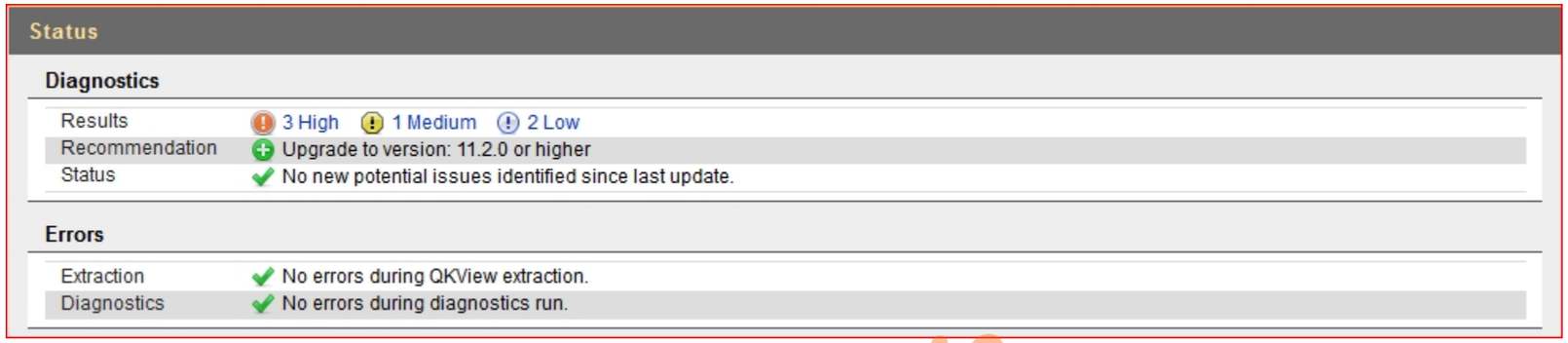


-- Exhibit --
Refer to the exhibit.
An LTM Specialist has uploaded a qkview to F5 iHealth.
Within the GUI, what is the correct procedure to comply with the recommendation shown in the exhibit?

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
Section:

QUESTION 66
-- Exhibit --

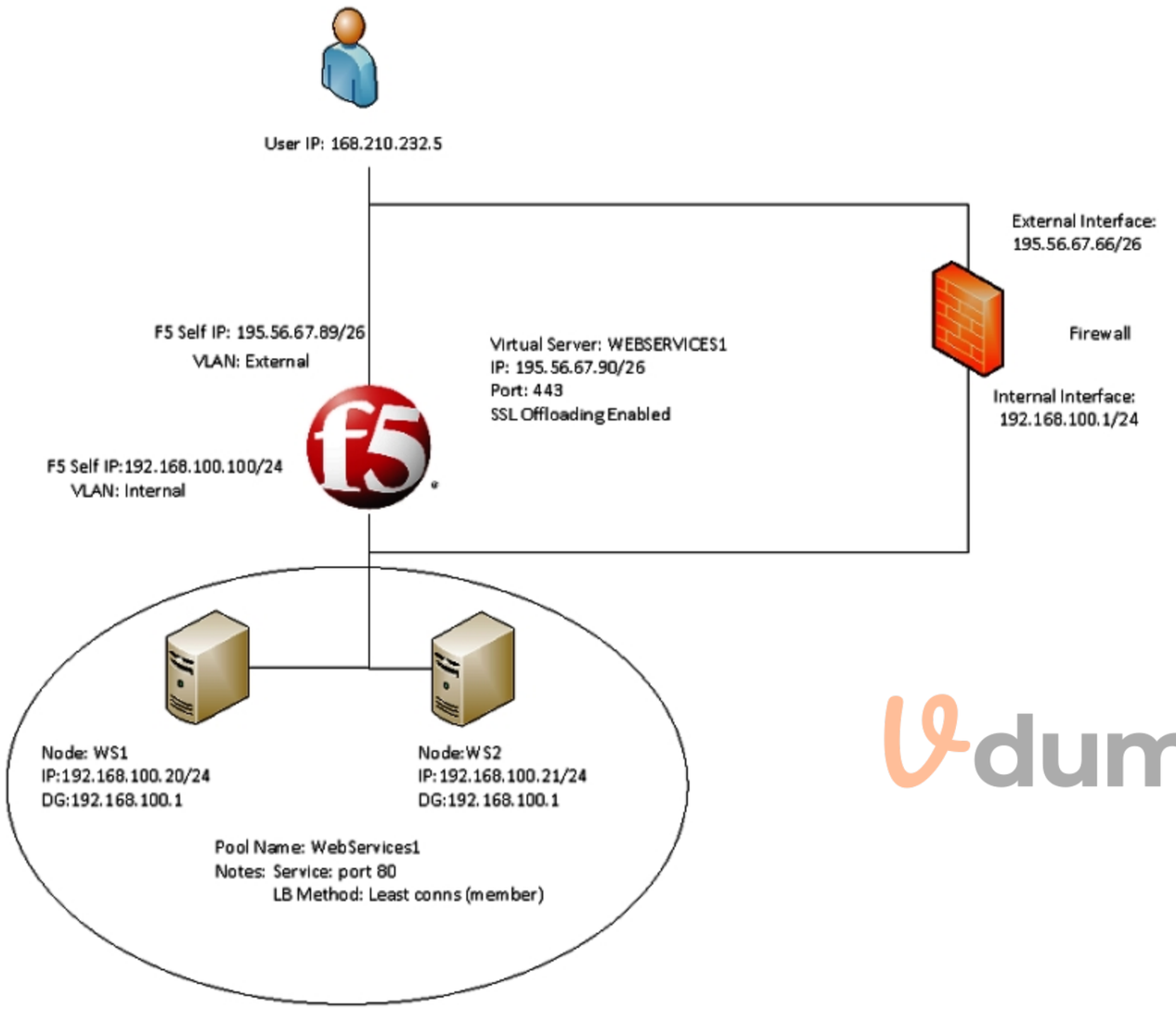


-- Exhibit --
Refer to the exhibit.
Which step should an LTM Specialist take next to finish upgrading to HD1.3?

A. Install image to HD1.3
B. Install hotfix to HD1.3
C. Activate HD1.3
D. Relicense HD1.3

Correct Answer: C
Section:

QUESTION 67
-- 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 <mss 1450,nop,nop,sackOK>
00:25:07.598537 IP 195.56.67.90.https > 168.210.232.5.33159: S 2690691360:2690691360(0) ack 1920647965 win 4350 <mss 1460,sackOK,eol>
00:25:07.598851 IP 168.210.232.5.33160 > 195.56.67.90.https: S 2763858764:2763858764(0) win 8192 <mss 1450,nop,nop,sackOK>
00:25:07.598858 IP 195.56.67.90.https > 168.210.232.5.33160: S 1905576176:1905576176(0) ack 2763858765 win 4350 <mss 1460,sackOK,eol>
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 <mss 1460,nop,wscale 0,sackOK,eol>
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
Section:

QUESTION 68
-- Exhibit --

```
1 1  0.2423 (0.2423)  C>S  Handshake
      ClientHello
        Version 3.2
        cipher suites
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
         TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
Unknown SSL content type 72
1 2  0.2432 (0.0008)  S>CShort record
1    0.2432 (0.0000)  S>C  TCP FIN
New TCP connection #2: 168.210.232.5(24782) <->
193.33.229.103(443)
2 1  0.2393 (0.2393)  C>S  Handshake
      ClientHello
        Version 3.2
        cipher suites
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
         TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
Unknown SSL content type 72
2 2  0.2404 (0.0010)  S>CShort record
2    0.2404 (0.0000)  S>C  TCP FIN
2 3  0.4738 (0.2333)  C>S  Alert
    level           fatal
    value           unexpected_message
2    0.4742 (0.0003)  C>S  TCP FIN
1 3  0.4857 (0.2425)  C>S  Alert
    level           fatal
    value           unexpected_message
1    0.4857 (0.0000)  C>S  TCP FIN
```

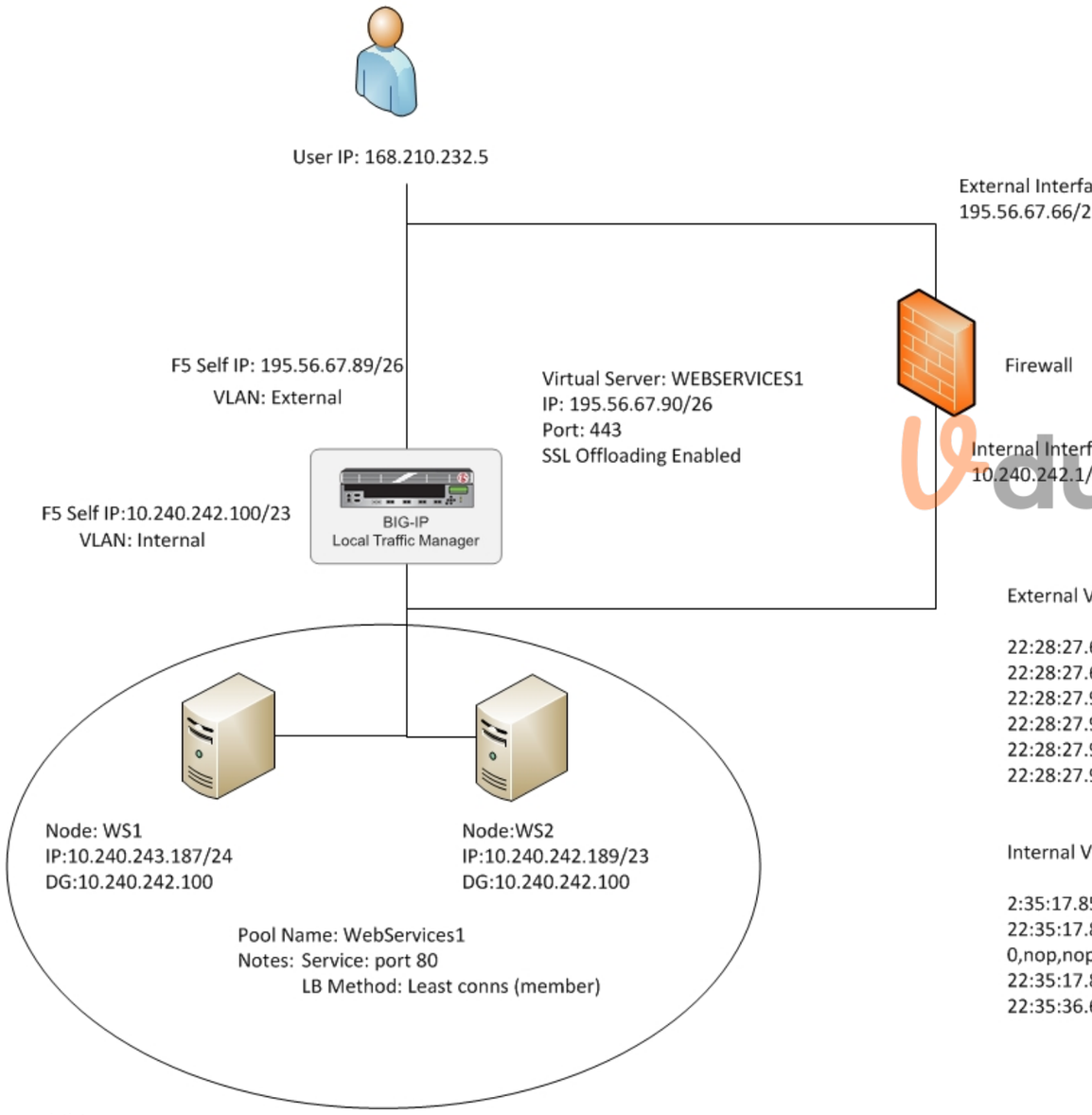
-- Exhibit --
Refer to the exhibit.
A client attempts to connect from a Google Chrome browser to a virtual server on a BIG-IP LTM. The virtual server is SSL Offloaded. When the client connects, the client receives an SSL error. After trying Mozilla Firefox and Internet Explorer browsers, the client still receives the same errors.
The LTM Specialist does an ssldump on the virtual server and receives the results as per the exhibit.
What is the problem?

A. The SSL key length is incorrect.

B. The BIG-IP LTM is NOT serving a certificate.
C. The BIG-IP LTM is NOT listening on port 443.
D. The client needs to be upgraded to the appropriate cipher-suite.

Correct Answer: B
Section:

QUESTION 69
-- Exhibit --



External Vlan tcpdump

22:28:27.689421 IP 168.210.232.5.27820 > 195.56.67.90.https: S 4159851702:4159851702(0) win 8192 <mss 1450,nop,nop,sackOK>
22:28:27.689433 IP 195.56.67.90.https > 168.210.232.5.27820: S 876741540:876741540(0) ack 4159851703 win 4350 <mss 1460,sackOK,eol>
22:28:27.919524 IP 168.210.232.5.27820 > 195.56.67.90.https: . ack 1 win 1450
22:28:27.921141 IP 168.210.232.5.27820 > 195.56.67.90.https: P 1:104(103) ack 1 win 65250
22:28:27.922822 IP 195.56.67.90.https > 168.210.232.5.27820: P 1:506(505) ack 104 win 4453
22:28:27.922839 IP 195.56.67.90.https > 168.210.232.5.27820: F 506:506(0) ack 104 win 4453

Internal Vlan tcpdump

2:35:17.858896 IP 168.210.232.5.27820 > 10.40.242.189.http: S 3302554564:3302554564(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
22:35:17.862769 IP 10.40.242.189.http > 168.210.232.5.27820: S 4222909244:4222909244(0) ack 3302554565 win 65535 <mss 1310,nop,wscale 0,nop,nop,sackOK>
22:35:17.862786 IP 168.210.232.5.27820 > 10.40.242.189.http: . ack 1 win 4380
22:35:36.636255 IP 168.210.232.5.33202 > 10.240.243.187.http: S 2389057240:2389057240(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>

-- Exhibit --
Refer to the exhibit.
An LTM Specialist has a virtual server set up on the LTM device as per the exhibit. The LTM Specialist receives reports of intermittent issues. Some clients are connecting fine while others are failing to connect.
The LTM Specialist does a tcpdump on the relevant interfaces, with the following results extracted:

What is causing the intermittent issues?

A. The firewall is dropping the packets from WS1.
B. The default gateway is inaccessible from WS1.
C. The load balancing (LB) method is inappropriate.
D. The pool members have been set up as an active/standby pair, with WS1 as the standby.

Correct Answer: B
Section:

QUESTION 70
-- Exhibit --

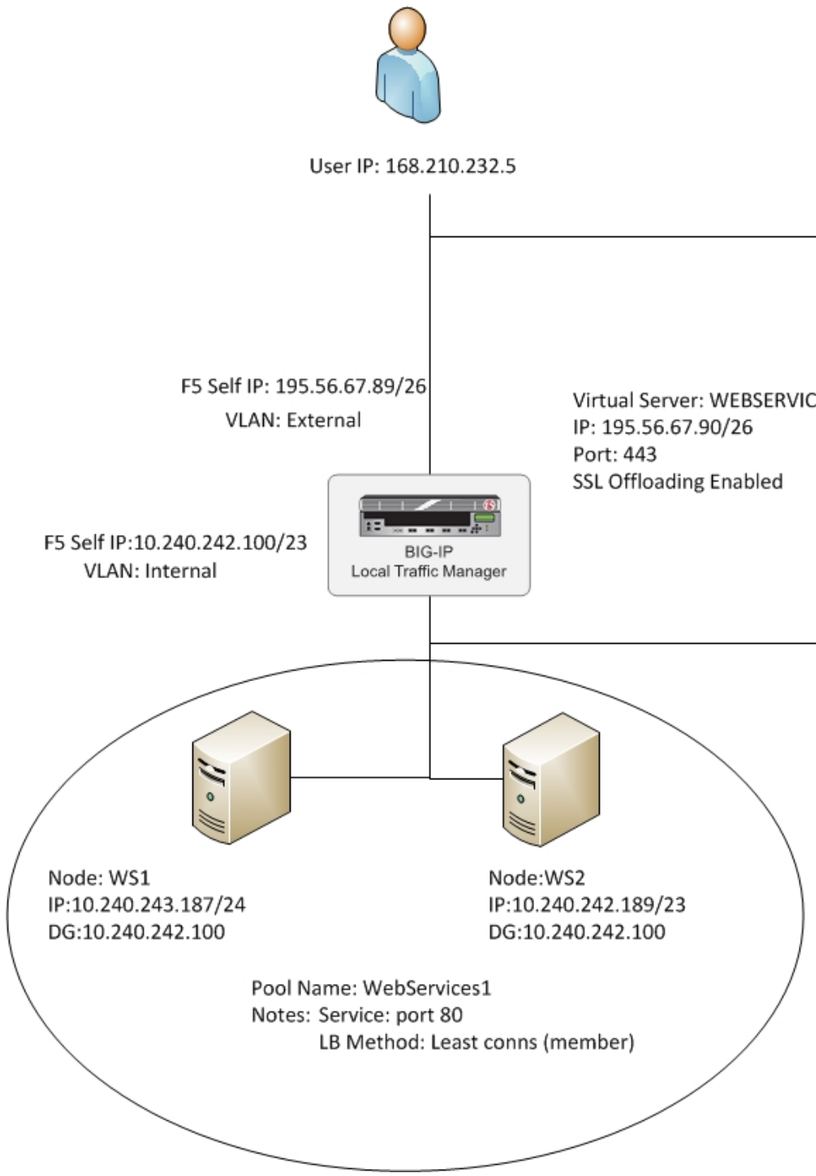
```
External Vlan tcpdump:

16:38:10.184240 IP 168.210.232.5.59156 > 66.212.246.58.1990: S 1208467898:1208467898(0) win 8192 <mss 1380,nop,wscale 8,nop,nop,sackOK>
16:38:10.184249 IP 66.212.246.58.1990 > 168.210.232.5.59156: S 2009182511:2009182511(0) ack 1208467899 win 4140 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:10.454030 IP 168.210.232.5.59156 > 66.212.246.58.1990: . ack 1 win 5
16:38:52.809723 IP 168.210.232.5.31084 > 66.212.246.58.1991: S 2991752264:2991752264(0) win 8192 <mss 1380,nop,wscale 8,nop,nop,sackOK>
16:38:52.809734 IP 66.212.246.58.1991 > 168.210.232.5.31084: S 2217364875:2217364875(0) ack 2991752265 win 4140 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:52.737749 IP 168.210.232.5.59172 > 66.212.246.58.2002: S 3158709238:3158709238(0) win 8192 <mss 1380,nop,wscale 8,nop,nop,sackOK>
16:38:52.737766 IP 66.212.246.58.2002 > 168.210.232.5.59172: S 7716150:7716150(0) ack 3158709239 win 4140 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.007421 IP 168.210.232.5.59172 > 66.212.246.58.2002: . ack 1 win 5
16:38:53.078216 IP 168.210.232.5.31084 > 66.212.246.58.1991: . ack 1 win 5
16:43:21.434766 IP 168.210.232.5.59156 > 66.212.246.58.1990: R 830:830(0) ack 94934 win 0

Internal Vlan tcpdump:

16:38:11.887217 IP 168.210.232.5.10033 > 10.240.243.65.1989: S 2408612037:2408612037(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:11.887559 IP 10.240.243.65.1989 > 168.210.232.5.10033: S 165435577:165435577(0) ack 2408612038 win 8192 <mss 1310,nop,nop,sackOK>
16:38:11.887566 IP 168.210.232.5.10033 > 10.240.243.65.1989: . ack 1 win 4380
16:38:53.007459 IP 168.210.232.5.59172 > 10.240.243.66.2002: S 26149351:26149351(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.007908 IP 10.240.243.66.2002 > 168.210.232.5.59172: S 3860985485:3860985485(0) ack 26149352 win 8192 <mss 1310,nop,nop,sackOK>
16:38:53.007916 IP 168.210.232.5.59172 > 10.240.243.66.2002: . ack 1 win 4380
16:38:53.078499 IP 168.210.232.5.31084 > 10.240.242.197.1991: S 2788170026:2788170026(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.078861 IP 10.240.242.197.1991 > 168.210.232.5.31084: S 2169754248:2169754248(0) ack 2788170027 win 8192 <mss 1310,nop,wscale 8,nop,nop,sackOK>
16:38:53.078871 IP 168.210.232.5.31084 > 10.240.242.197.1991: . ack 1 win 4380
16:43:29.434782 IP 168.210.232.5.10033> 10.240.243.65.1989: R 181:181(0) ack 88278 win 65535
```

-- Exhibit --
Refer to the exhibit.
A company uses a complex piece of client software that connects to one or more virtual servers (VS) hosted on an LTM device. The client software is experiencing issues. An LTM Specialist is tasked with finding the cause of the problem.
The LTM Specialist has the tcpdump extract and knows the client software has at least one connection to a VS on port 1990. However, when a tcpdump runs on the internal VLAN, there is no record of port 1990 in the tcpdump.
Why is there no record of port 1990 in the tcpdump?

A. The LTM device drops the connection.
B. Port 1990 is a well-known port, so its use is restricted.
C. The LTM device performs a Port Address Translation (PAT).
D. The LTM device performs a Network Address Translation (NAT).

Correct Answer: C
Section:

QUESTION 71
-- Exhibit --



External Vlan tcpdump

22:28:27.689421 IP 168.210.232.5.27820 > 195.56.67.90.https: S 4159851702:4159851702(0) win 8192 <mss 1450,nop,nop,sackOK>
22:28:27.689433 IP 195.56.67.90.https > 168.210.232.5.27820: S 876741540:876741540(0) ack 4159851703 win 4350 <mss 1460,sackOK,eol>
22:28:27.919524 IP 168.210.232.5.27820 > 195.56.67.90.https: . ack 1 win 1450
22:28:27.921141 IP 168.210.232.5.27820 > 195.56.67.90.https: P 1:104(103) ack 1 win 65250
22:28:27.922822 IP 195.56.67.90.https > 168.210.232.5.27820: P 1:506(505) ack 104 win 4453
22:28:27.922839 IP 195.56.67.90.https > 168.210.232.5.27820: F 506:506(0) ack 104 win 4453

Internal Vlan tcpdump

2:35:17.858896 IP 168.210.232.5.27820 > 10.40.242.189.http: S 3302554564:3302554564(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
22:35:17.862769 IP 10.40.242.189.http > 168.210.232.5.27820: S 4222909244:4222909244(0) ack 3302554565 win 65535 <mss 1310,nop,wscale 0,nop,nop,sackOK>
22:35:17.862786 IP 168.210.232.5.27820 > 10.40.242.189.http: . ack 1 win 4380
22:35:36.636255 IP 168.210.232.5.33202 > 10.240.243.187.http: S 2389057240:2389057240(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>

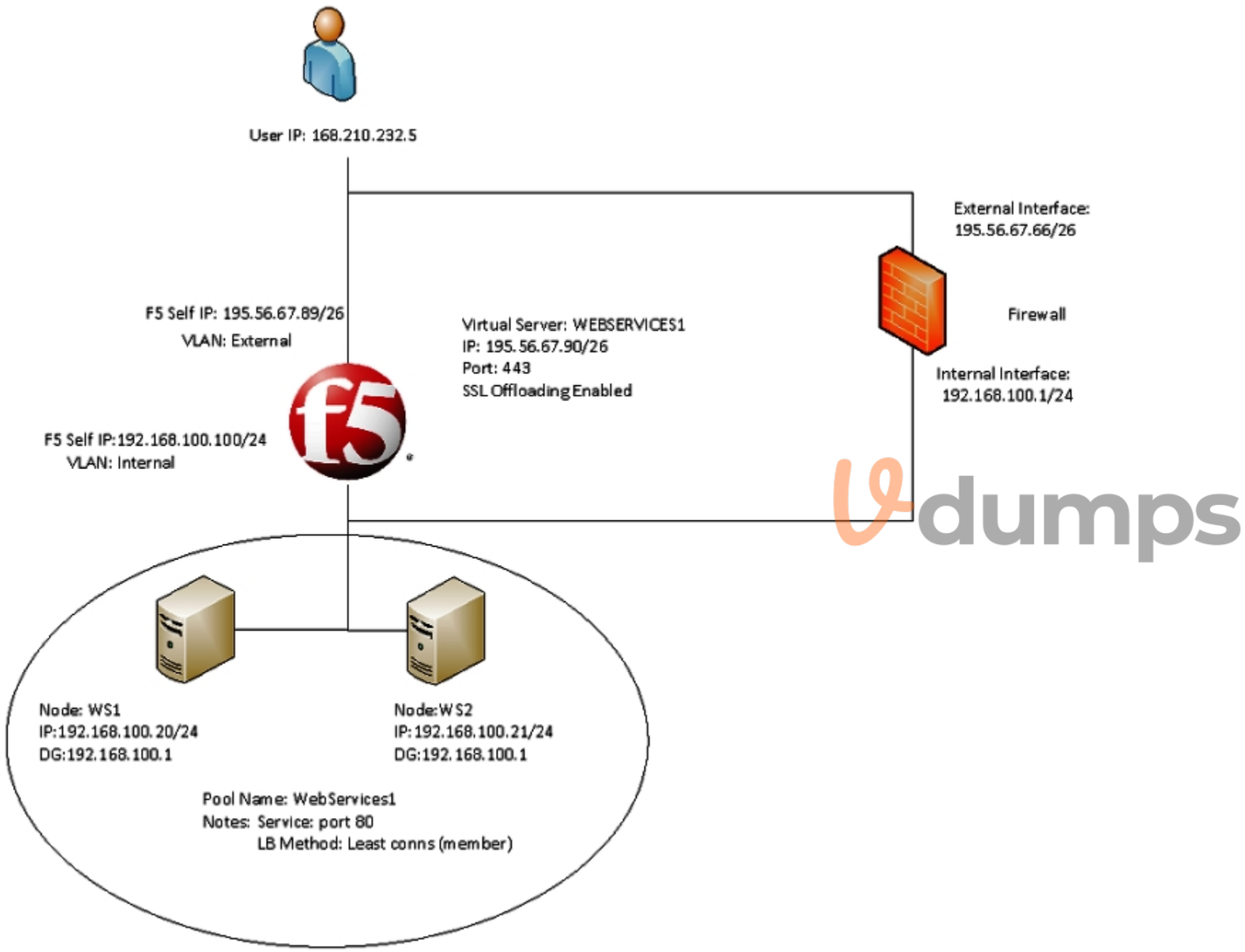
-- Exhibit --
Refer to the exhibit.
A company uses a complex piece of client software that connects to one or more virtual servers hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem.
The LTM Specialist has the tcpdump extract and knows the client source IP is 168.210.232.5.
Assuming no wildcard virtual servers, how many distinct virtual servers does the client connect to on the LTM device?

A. 2
B. 3
C. 4

D. 6

Correct Answer: B
Section:

QUESTION 72
-- Exhibit --



-- Exhibit --
Refer to the exhibit.
A company uses a complex piece of client software that connects to one or more virtual servers (VS) hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem.
The LTM Specialist is seeing a client source IP of 168.210.232.5 in the tcpdump. However, the client source IP is actually 10.123.17.12.
Why does the IP address of 10.123.17.12 fail to appear in the tcpdump?

A. The LTM device performed NAT on the individual's IP address.

B. The Secure Network Address Translation (SNAT) pool on the virtual server is activated.
C. Network Address Translation (NAT) has occurred in the path between the client and the LTM device.
D. The individual's data stream is being routed to the LTM device by a means other than the default route.

Correct Answer: C
Section:

QUESTION 73
-- Exhibit --

```
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 86 59 bf 27
          e7 b5 fa 49 38 fd 24 d7 c3 1e c1 9f d2 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
```

-- Exhibit --

Refer to the exhibit.

A company uses a complex piece of client software that connects to one or more virtual servers (VS) hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem. The LTM Specialist has the tcpdump extract. The client loses connection with the LTM device.

Where is the reset originating?

A. the local switch
B. the application server
C. the device initiating the connection
D. the destination device of the initial connection

Correct Answer: C
Section:

QUESTION 74
-- 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
Section:

QUESTION 75
-- Exhibit --

```
source-address - 78.24.213.79:443 - 10.72.250.52:80
-------------------------------------------------------
  TMM           0
  Mode          source-address
  Key           168.210.232.5
  Age (sec.)    140
  Virtual Name  VS1
  Virtual Addr  78.24.213.79:443
  Node Addr     10.72.250.52:80
  Pool Name     CDN-ITS
  Client Addr   168.210.232.5

  source-address - 78.24.213.79:443 - 10.72.250.52:80
-------------------------------------------------------
  TMM           1
  Mode          source-address
  Key           82.171.210.22
  Age (sec.)    404
  Virtual Name  VS1
  Virtual Addr  78.24.213.79:443
  Node Addr     10.72.250.52:80
  Pool Name     CDN-ITS
  Client Addr   82.171.210.22

  source-address - 78.24.213.79:443 - 10.72.250.60:80
-------------------------------------------------------
  TMM           0
  Mode          source-address
  Key           78.24.213.193
  Age (sec.)    9
  Virtual Name  VS1
  Virtual Addr  78.24.213.79:443
  Node Addr     10.72.250.60:80
  Pool Name     CDN-ITS
  Client Addr   78.24.213.193

source-address - 78.24.213.79:443 - 10.72.250.60:80
-------------------------------------------------------
  TMM           1
  Mode          source-address
  Key           78.24.213.193
  Age (sec.)    10
  Virtual Name  VS1
  Virtual Addr  78.24.213.79:443
  Node Addr     10.72.250.60:80
  Pool Name     CDN-ITS
  Client Addr   78.24.213.193

  source-address - 78.24.213.79:443 - 10.72.250.52:80
-------------------------------------------------------
  TMM           0
  Mode          source-address
  Key           87.209.154.107
  Age (sec.)    61
  Virtual Name  VS1
  Virtual Addr  78.24.213.79:443
  Node Addr     10.72.250.52:80
  Pool Name     CDN-ITS
  Client Addr   87.209.154.107
```

-- Exhibit --
Refer to the exhibit.
A virtual server is set up on an LTM device as follows:
Virtual server address 78.24.213.79
Default Persistence ProfilE. source_addr, 600s.
Pool NamE. Pool1
Pool Members: 10.72.250.52:80 and 10.72.250.60:80 (both on Internal Vlan)
There are several current connections to the virtual server, and pool member 10.72.250.52:80 has been set to a 'Disabled' state.
A tcpdump on the Internal Vlan shows traffic going to 10.72.250.52:80.
How soon after the persistence table query was run can existing connections be refreshed/renewed to ensure that no requests are sent to 10.72.250.52?

A. 196 seconds
B. 460 seconds
C. 539 seconds
D. 590 seconds
E. 591 seconds

Correct Answer: C
Section:

QUESTION 76
-- Exhibit --

```
1 1   0.2423 (0.2423)  C>S  Handshake
      ClientHello
        Version 3.2
        cipher suites
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
         TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
Unknown SSL content type 72
1 2   0.2432 (0.0008)  S>CShort record
1     0.2432 (0.0000)  S>C  TCP FIN
New TCP connection #2: 168.210.232.5(24782) <-> 193.33.229.103(443)
2 1   0.2393 (0.2393)  C>S  Handshake
      ClientHello
        Version 3.2
        cipher suites
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
         TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
Unknown SSL content type 72
2 2   0.2404 (0.0010)  S>CShort record
2     0.2404 (0.0000)  S>C  TCP FIN
2 3   0.4738 (0.2333)  C>S  Alert
    level           fatal
    value           unexpected_message
2     0.4742 (0.0003)  C>S  TCP FIN
1 3   0.4857 (0.2425)  C>S  Alert
    level           fatal
    value           unexpected_message
1     0.4857 (0.0000)  C>S  TCP FIN
```

-- Exhibit --
Refer to the exhibit.
A client attempts to connect from a Google Chrome browser to a virtual server on a BIG-IP LTM. The virtual server is SSL Offloaded. When the client connects, the client receives an SSL error. The client receives the same errors when trying Mozilla Firefox and Internet Explorer browsers.
The LTM Specialist does an ssldump on the virtual server and receives the results as per the exhibit.
How should this be resolved?

A. Set the virtual server to listen on port 443 (HTTPS).
B. Upgrade the client to support the appropriate SSL cipher suite.
C. Select the appropriate 'SSL Profile (Client)' in the virtual server settings.
D. Adjust the SSL key length in the SSL profile to match the minimum required by the client.

Correct Answer: C
Section:

QUESTION 77
-- Exhibit --

```
13:20:26.194324 IP 10.10.1.1.42923 > 172.16.20.2.ftp: S 1642091015:1642091015(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2403895569 0,sackOK,eol>
13:20:26.196505 IP 172.16.20.2.ftp > 10.10.1.1.42923: S 3574712268:3574712268(0) ack 1642091016 win 5792 <mss 1460,sackOK,timestamp 9643612 2403895569,nop,wscale 3>
13:20:26.196514 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 1 win 4380 <nop,nop,timestamp 2403895573 9643612>
13:20:26.199257 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 1:21(20) ack 1 win 724 <nop,nop,timestamp 9643615 2403895573>
13:20:26.199274 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 21 win 4400 <nop,nop,timestamp 2403895575 9643615>
13:20:28.436817 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 1:15(14) ack 21 win 4400 <nop,nop,timestamp 2403897813 9643615>
13:20:28.438230 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 15 win 724 <nop,nop,timestamp 9645855 2403897813>
13:20:28.438234 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 21:55(34) ack 15 win 724 <nop,nop,timestamp 9645855 2403897813>
13:20:28.438251 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 55 win 4434 <nop,nop,timestamp 2403897814 9645855>
13:20:30.860614 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 15:29(14) ack 55 win 4434 <nop,nop,timestamp 2403900237 9645855>
13:20:30.901297 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 29 win 724 <nop,nop,timestamp 9648319 2403900237>
13:20:40.864453 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 55:78(23) ack 29 win 724 <nop,nop,timestamp 9658281 2403900237>
13:20:40.864522 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 78 win 4457 <nop,nop,timestamp 2403910241 9658281>
13:20:40.865948 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 29:35(6) ack 78 win 4457 <nop,nop,timestamp 2403910242 9658281>
13:20:40.867799 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 35 win 724 <nop,nop,timestamp 9658284 2403910242>
13:20:40.867803 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 78:97(19) ack 35 win 724 <nop,nop,timestamp 9658284 2403910242>
13:20:40.867816 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 97 win 4476 <nop,nop,timestamp 2403910244 9658284>
13:20:47.199810 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 35:43(8) ack 97 win 4476 <nop,nop,timestamp 2403916576 9658284>
13:20:47.201215 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 97:128(31) ack 43 win 724 <nop,nop,timestamp 9664618 2403916576>
13:20:47.201233 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 128 win 4507 <nop,nop,timestamp 2403916577 9664618>
13:20:47.202263 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 43:67(24) ack 128 win 4507 <nop,nop,timestamp 2403916578 9664618>
13:20:47.203810 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 128:179(51) ack 67 win 724 <nop,nop,timestamp 9664620 2403916578>
13:20:47.203822 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 179 win 4558 <nop,nop,timestamp 2403916580 9664620>
13:20:47.205035 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 67:82(15) ack 179 win 4558 <nop,nop,timestamp 2403916581 9664620>
13:20:47.206441 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp 9664623 0,nop,wscale 3>
13:20:47.245894 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 82 win 724 <nop,nop,timestamp 9664663 2403916581>
13:20:50.205908 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp 9667623 0,nop,wscale 3>
13:20:56.205528 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp 9673623 0,nop,wscale 3>
13:21:08.205649 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp 9685623 0,nop,wscale 3>
13:21:32.205498 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp 9709623 0,nop,wscale 3>
13:21:47.204625 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 179:216(37) ack 82 win 724 <nop,nop,timestamp 9724623 2403916581>
13:21:47.204646 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 216 win 4595 <nop,nop,timestamp 2403976581 9724623>
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist configures a virtual server to load balance to a pool of FTP servers. File transfers are failing. The virtual server is configured as follows:

```
ltm virtual ftp_vs {
destination 10.10.1.103:ftp
ip-protocol tcp
mask 255.255.255.255
pool ftp_pool
profiles {
tcp { }
}
vlans-disabled
}
```

Which change will resolve the problem?

A. Add an FTP monitor to the pool.
B. Add an FTP profile to the virtual server.
C. Enable loose initiation in the TCP profile.
D. Increase the TCP timeout value in the TCP profile.

Correct Answer: B
Section:

QUESTION 78
-- 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
Section:

QUESTION 79
-- Exhibit --

No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
101	6.093319	10.10.17.50	21	10.10.1.2	50589	FTP	115	Response: 230 Login successful.
104	6.096106	10.10.1.2	50589	10.10.17.50	21	FTP	98	Request: SYST
105	6.096133	172.16.17.33	50589	172.16.20.3	21	FTP	98	Request: SYST
108	6.097086	172.16.20.3	21	172.16.17.33	50589	FTP	111	Response: 215 UNIX Type: L8
109	6.097113	10.10.17.50	21	10.10.1.2	50589	FTP	111	Response: 215 UNIX Type: L8
124	8.153091	10.10.1.2	50589	10.10.17.50	21	FTP	115	Request: PORT 10,10,1,2,160,88
126	8.153145	172.16.17.33	50589	172.16.20.3	21	FTP	115	Request: PORT 10,10,1,2,160,88
128	8.154290	172.16.20.3	21	172.16.17.33	50589	FTP	119	Response: 500 Illegal PORT command.
130	8.154336	10.10.17.50	21	10.10.1.2	50589	FTP	119	Response: 500 Illegal PORT command.
150	10.241918	10.10.1.2	50589	10.10.17.50	21	FTP	98	Request: QUIT
151	10.241963	172.16.17.33	50589	172.16.20.3	21	FTP	98	Request: QUIT
154	10.243124	172.16.20.3	21	172.16.17.33	50589	FTP	106	Response: 221 Goodbye.
156	10.243159	10.10.17.50	21	10.10.1.2	50589	FTP	106	Response: 221 Goodbye.

```
⊞ Frame 126: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
⊞ Ethernet II, Src: Vmware_29:00:9c (00:50:56:29:00:9c), Dst: Vmware_29:01:be (00:50:56:29:01:be)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 4093
⊞ Internet Protocol Version 4, Src: 172.16.17.33 (172.16.17.33), Dst: 172.16.20.3 (172.16.20.3)
⊞ Transmission Control Protocol, Src Port: 50589 (50589), Dst Port: ftp (21), Seq: 48, Ack: 135, Len: 23
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 10,10,1,2,160,88\r\n
      Request command: PORT
      Request arg: 10,10,1,2,160,88
      Active IP address: 10.10.1.2 (10.10.1.2)
      Active port: 41048
      Active IP NAT: True
```

-- 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 users are receiving the FTP error '500 Illegal PORT command.' The virtual server is configured to SNAT using automap. The LTM Specialist performs a capture on the server side of the LTM device.

Why is the server returning this error?

A. LIST command disallowed
B. PORT command disallowed
C. Active IP address in PORT command
D. Active IP address in LOGIN command

Correct Answer: C
Section:

QUESTION 80
-- Exhibit --

```
ltm monitor http http_head {
    defaults-from http
    destination *:*
    interval 5
    recv <html>
    send "HEAD / HTTP/1.0\\r\\n\\r\\n"
    time-until-up 0
    timeout 16
}
ltm pool srv1_http_pool {
    members {
        192.168.2.1:http {
            address 192.168.2.1
            session monitor-enabled
            state down
        }
    }
    monitor http_head
}
```

TCPDUMP Output:

```
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 24 Oct 2012 18:45:53 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
X-Powered-By: PHP/5.4.4
Connection: close
Content-Type: text/html
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is troubleshooting a new HTTP monitor on a pool. The pool member is functioning correctly when accessed directly through a browser, although the monitor is marking the member as down. As part of the troubleshooting, the LTM Specialist has captured the monitor traffic via tcpdump.
How should the LTM Specialist resolve this issue?

A. Add the 'http' monitor to the pool.
B. Add the 'icmp' monitor to the node.
C. Modify the receive string to valid content.
D. Correct the firewall rules on the pool member.

Correct Answer: C
Section:

QUESTION 81
-- Exhibit --

```
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;.@.@......<
        0x0010:  0a00 000c caeb 0050 8be5 aca3 dd65 e3e1  .......P.....e..
        0x0020:  8018 002e 1b41 0000 0101 080a 94b3 5b5c  .....A........[\
        0x0030:  0e30 90ad 4745 5420 2f74 6573 745f 7061  .0..GET./test_pa
        0x0040:  6765 2e68 746d 6c20 4854 5450 312e 310d  ge.html.HTTP/1.1.
        0x0050:  0a48 6f73 743a 200d 0a43 6f6e 6e65 6374  .Host:...Connect
        0x0060:  696f 6e3a 2043 6c6f 7365 0d0a 0d0a 0105  ion:.Close......
        0x0070:  0100 0003 00                             .....
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:  4500 0260 a62e 4000 4006 6105 0a00 000c  E..`..@.@.a.....
        0x0010:  0a1d 1d3c 0050 bf46 fa3b dc73 bb22 2817  ...<.P.F.;.s."(.
        0x0020:  8018 016a 5738 0000 0101 080a 0e37 7a5f  ...jW8.......7z_
        0x0030:  94f8 7d87 4854 5450 2f31 2e31 2034 3034  ..}.HTTP/1.1.404
        0x0040:  204e 6f74 2046 6f75 6e64 0d0a 4461 7465  .Not.Found..Date
        0x0050:  3a20 5765 642c 2032 3420 4f63 7420 3230  :.Mon,.01.Jan.20
        0x0060:  3132 2032 323a 3530 3a34 3320 474d 540d  00.00:00:01.GMT.
        0x0070:  0a53 6572 7665 723a 2041 7061 6368 652f  .Server:.Apache.
        0x00c0:  0d0a 436f 6e74 656e 742d 4c65 6e67 7468  ..Content-Length
        0x00d0:  3a20 3332 370d 0a43 6f6e 6e65 6374 696f  :.327..Connectio
        0x00e0:  6e3a 2063 6c6f 7365 0d0a 436f 6e74 656e  n:.close..Conten
        0x00f0:  742d 5479 7065 3a20 7465 7874 2f68 746d  t-Type:.text/htm
        0x0100:  6c3b 2063 6861 7273 6574 3d69 736f 2d38  l;.charset=iso-8
        0x0110:  3835 392d 310d 0a0d 0a3c 2144 4f43 5459  859-1....<!DOCTY
        0x0120:  5045 2048 544d 4c20 5055 424c 4943 2022  PE.HTML.PUBLIC."
        0x0130:  2d2f 2f49 4554 462f 2f44 5444 2048 544d  -//IETF//DTD.HTM
        0x0140:  4c20 322e 302f 2f45 4e22 3e0a 3c68 746d  L.2.0//EN">.<htm
        0x0150:  6c3e 3c68 6561 643e 0a3c 7469 746c 653e  l><head>.<title>
        0x0160:  3430 3420 4e6f 7420 466f 756e 643c 2f74  Ooops.Sorry..</t
        0x0170:  6974 6c65 3e0a 3c2f 6865 6164 3e3c 626f  itle>.</head><bo
        0x0180:  6479 3e0a 3c68 313e 4e6f 7420 466f 756e  dy>.<h1>Not.Foun
        0x0190:  643c 2f68 313e 0a3c 703e 5468 6520 7265  d</h1>.<p>Your.r
        0x01a0:  7175 6573 7465 6420 5552 4c20 2f74 6573  quest.could.not
        0x01b0:  745f 7061 6765 2e68 746d 6c20 7761 7320  be.completed.by.
        0x01c0:  6e6f 7420 666f 756e 6420 6f6e 2074 6869  this.server..Sor
        0x01d0:  7320 7365 7276 6572 2e3c 2f70 3e0a 3c68  ry.......</p>.<h
        0x01e0:  723e 0a3c 6164 6472 6573 733e 4170 6163  r>.<address>Apac
        0x01f0:  6865 2f32 2e32 2e34 2028 5562 756e 7475  he/x.x.x.(xxxxxx
        0x0200:  2920 5048 502f 352e 322e 332d 3175 6275  ).PHP/x.x.x-1ubu
        0x0210:  6e74 7536 2e35 206d 6f64 5f73 736c 2f32  ntu6.5.mod_ssl/2
        0x0220:  2e32 2e34 204f 7065 6e53 534c 2f30 2e39  .2.4.OpenSSL/x.x
        0x0230:  2e38 6520 5365 7276 6572 2061 7420 2050  .8e.Server.at..P
        0x0240:  6f72 7420 3830 3c2f 6164 6472 6573 733e  ort.80</address>
        0x0250:  0a3c 2f62 6f64 793e 3c2f 6874 6d6c 3e0a  .</body></html>.
        0x0260:  0105 0101 0002 00                        .......
```

-- Exhibit --

Refer to the exhibit.

The decoded TCPDump capture is a trace of a failing health monitor. The health monitor is sending the string shown in the capture; however, the server response is NOT as expected. The receive string is set to 'SERVER IS UP'.

What is the solution?

A. The GET request Host header field requires a host name.

B. Incorrect syntax in send string. 'HTTP/1.1' should be 'HTTP1.1'.

C. The /test_page.html does NOT exist on the web server and should be added.

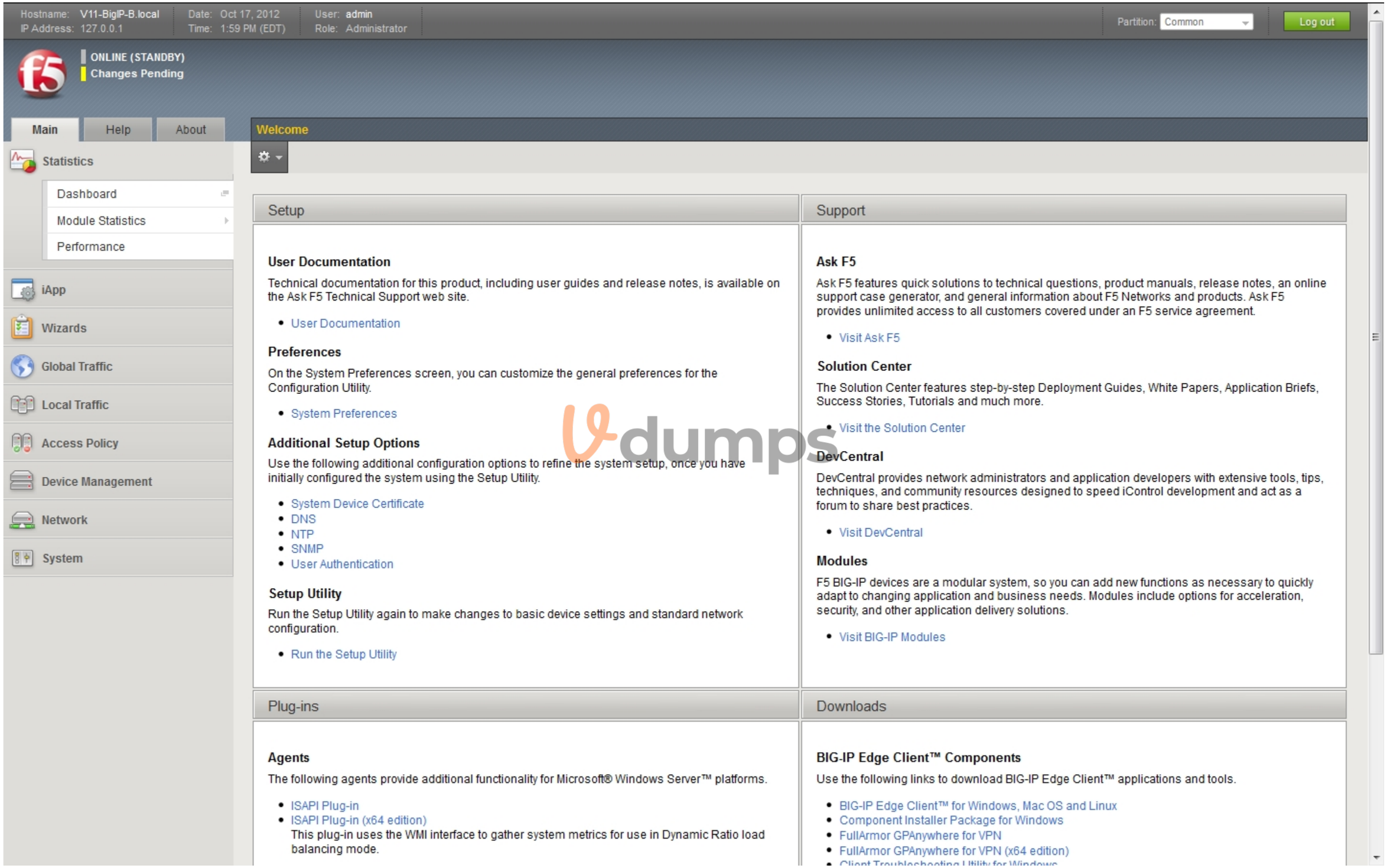
D. Incorrect syntax in send string. 'Connection: Close' should be 'Connection: Open'.

Correct Answer: C

Section:

QUESTION 82

-- Exhibit --



-- Exhibit --

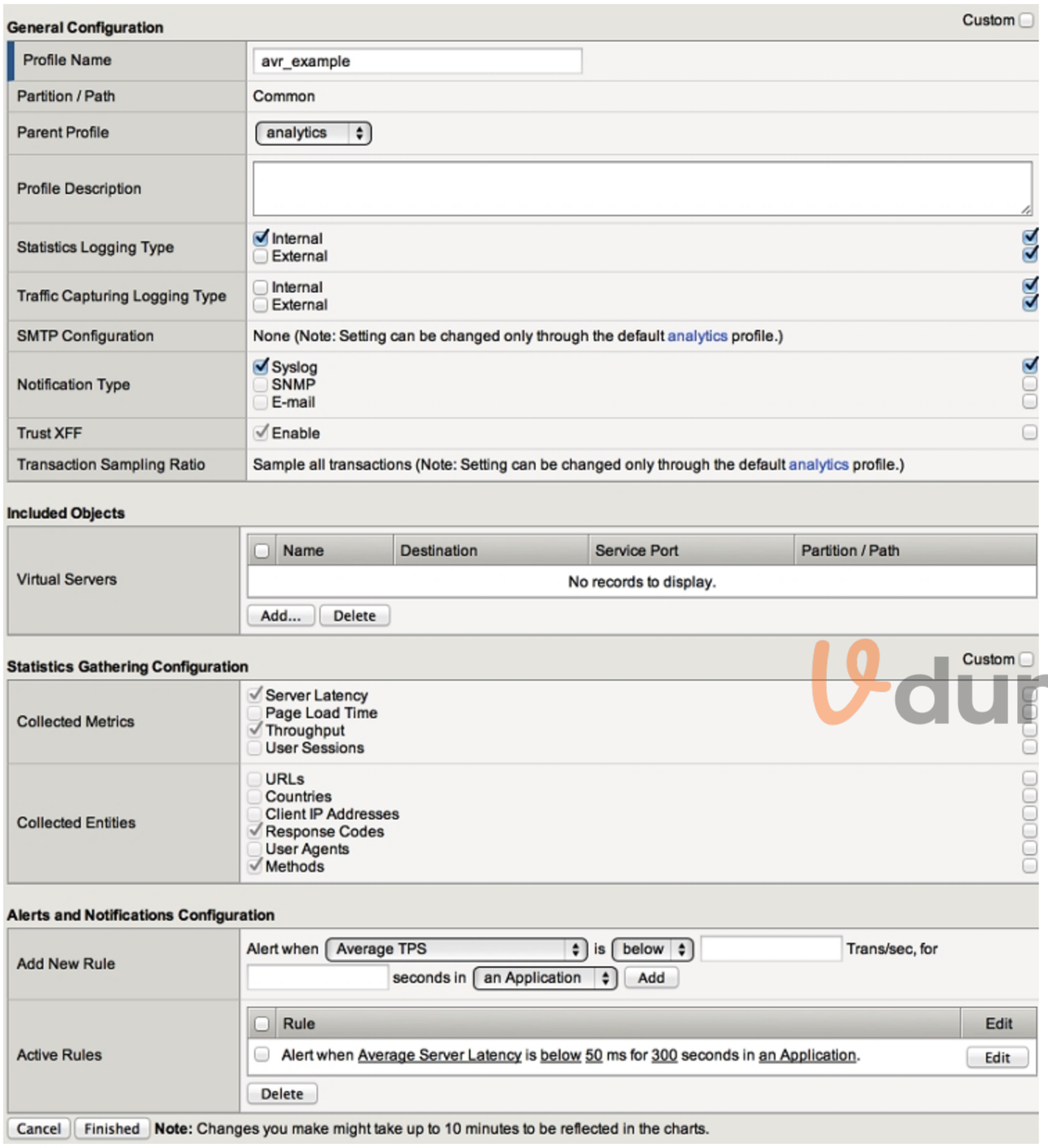
Refer to the exhibit.

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
Section:

QUESTION 83
-- 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?

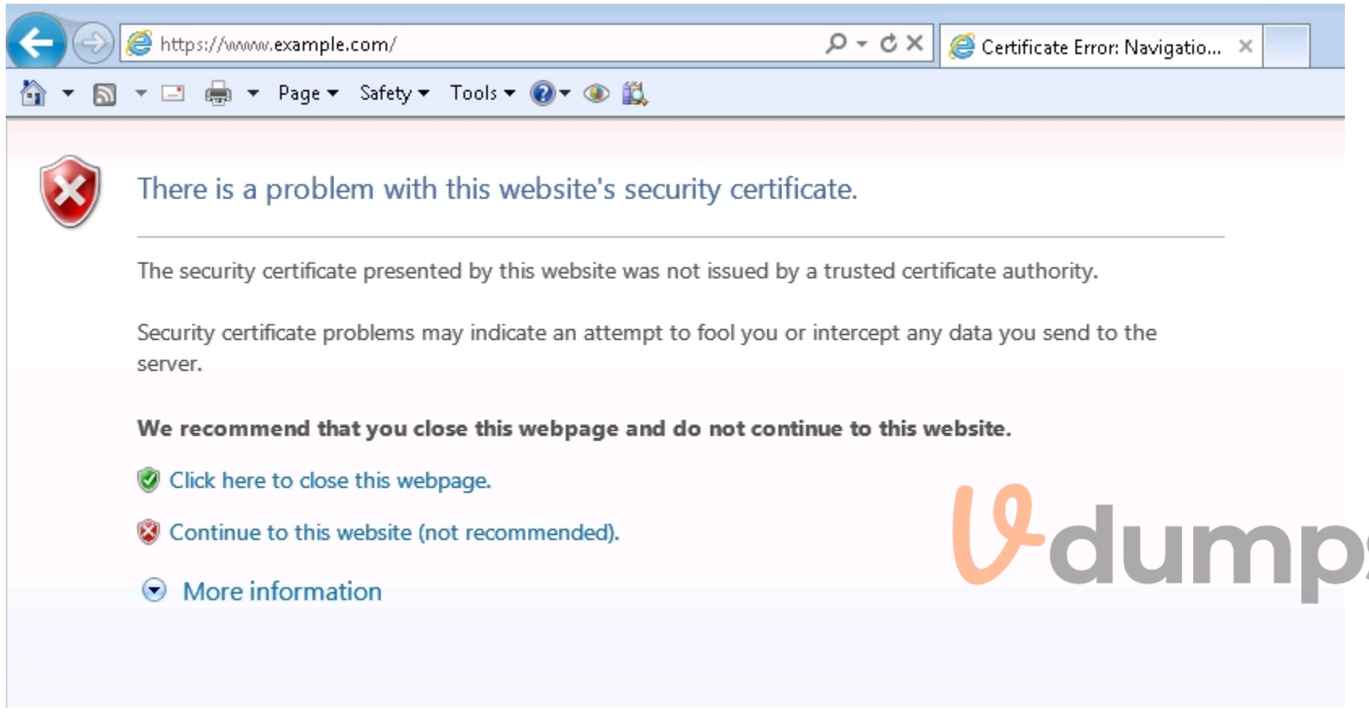
A. The rule should be adjusted to trigger when server latency is above 50ms.

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
Section:

QUESTION 84
-- Exhibit --



```
15:36:14.385939 IP 192.168.1.216.35137 > 192.168.1.1.80: S 379008507:379008507(0) win 14600 <mss 1460,sackOK,timestamp 2322043441 0,nop,wscale 7> out slot1/tmm0 lis=
E..<7f@.@..,.........A.P..5.......9............
.g.1.............
15:36:14.387168 IP 192.168.1.1.80 > 192.168.1.216.35137: S 2457418989:2457418989(0) ack 379008508 win 65535 <mss 1460,nop,wscale 3,sackOK,timestamp 2864934986 2322043441> in slot1/tmm0 lis=
E..<.I@.@..H.........P.A.y<...5.................
..pJ.g.1.......
15:36:14.387504 IP 192.168.1.216.35137 > 192.168.1.1.80: . ack 1 win 115 <nop,nop,timestamp 2322043443 2864934986> out slot1/tmm0 lis=
E..47g@.@..3.........A.P..5..y<....s.......
.g.3..pJ.......
15:36:14.387833 IP 192.168.1.216.35137 > 192.168.1.1.80: P 1:8(7) ack 1 win 115 <nop,nop,timestamp 2322043443 2864934986> out slot1/tmm0 lis=
E..;7h@.@..+.........A.P..5..y<....s@i.....
.g.3..pJGET /
.......
15:36:14.389329 IP 192.168.1.1.80 > 192.168.1.216.35137: P 1:1216(1215) ack 8 win 8326 <nop,nop,timestamp 2864934988 2322043443> in slot1/tmm0 lis=
E....M@.@............P.A.y<...6... .f......
..pL.g.3
<html><head><title>Load Balancing</title></head><body>
<h2>BIG-IP Load Balancing Test Page</h2>
<br><br>

<table cellpadding="4">
 <tr>
  <td width=35% align=right><b>Server Address:</b></td>
  <td align=left style="color:#347C17"><b>192.168.1.1:80</b></td>
 </tr>
 <tr>
  <td width=35% align=right><b>Client Address:</b></td>
  <td align=left style="color:#800000"><b>192.168.1.216:35137</b></td>
 </tr>
 </table>
 </body></html>
 .......
 15:36:14.389333 IP 192.168.1.1.80 > 192.168.1.216.35137: F 1216:1216(0) ack 8 win 8326 <nop,nop,timestamp 2864934989 2322043443> in slot1/tmm0 lis=
 .....N@.@..K.........P.A.yA...6... ..
 ..pM.g.3.......
 15:36:14.390225 IP 192.168.1.216.35137 > 192.168.1.1.80: . ack 1216 win 137 <nop,nop,timestamp 2322043445 2864934988> out slot1/tmm0 lis=
 E..47i@.@..1.........A.P..6..yA............
 .g.5..pL.......
 15:36:14.390230 IP 192.168.1.216.35137 > 192.168.1.1.80: F 8:8(0) ack 1217 win 137 <nop,nop,timestamp 2322043445 2864934989> out slot1/tmm0 lis=
 E..47j@.@..0.........A.P..6..yA............
 .g.5..pM.......
 15:36:14.391575 IP 192.168.1.1.80 > 192.168.1.216.35137: . ack 9 win 8325 <nop,nop,timestamp 2864934990 2322043445> in slot1/tmm0 lis=
 E..4.P@.@..I.........P.A.yA...6... ..
 .....
 ..pN.g.5.......
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is troubleshooting an HTTP monitor that is marking a pool member as down. Connecting to the pool member directly through a browser shows the application is up and functioning correctly.
ltm monitor http http_mon {
defaults-from http
destination *:*
interval 5
recv '200 OK'
send 'GET /\\r\\n'
time-until-up 0
timeout 16
}
What is the issue?

A. The HTTP headers are compressed.
B. The pool member is responding with a 404.
C. The pool member is responding without HTTP headers.
D. The request is NOT being received by the pool member.

Correct Answer: C
Section:

QUESTION 85
-- Exhibit --

```
[~]$ 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/xYyooMJVpXWZbzeKu04ro
euadY0KOwwa2zF9jaD0HDIJ3MtnVYaHMsHZvqoo1Q8EfohP85RfHrO4kMxtvAefm
s1qGE7MkmIxLtwYjjWXmwxW7sCFL19kt6pFOatzqeK3WxbdM5yF/RTHF4R/vyKQI
2lYf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBRG5CDKtOlkiiix7sc2JjoVHajd2zBm
BgNVHSMEXzBdgBRG5CDKtOlkiiix7sc2JjoVHajd26E6pDgwNjEWMBQGA1UEChMN
VHVybktleSBMaW51eDEcMBoGA1UECxMTU29mdHdhcmUgYXBwbGlhbmNlc4IJAImL
XVLJqYzBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEANo2TuXFVZKWG
n6KznFgueLGzn+qgyIz0ZVG5PF8RRzHPYDAIDRU0MEReQHhI4CRImMAwTAFdmhpl
RGH2+IqwglEPB7K6eudRy0D9GqzMHZrdMo9d3ewPB3BqjOrPhs5yRTgNrZHyasJr
ZAiCzekf24SwNpmhfHyyam88N2+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)
---
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting an issue with SSL and is receiving the error shown when connecting to the virtual server. When connecting directly to the pool member, clients do NOT receive this message, and the application functions correctly. The LTM Specialist exports the appropriate certificate and key from the pool member and imports them into the LTM device. The LTM Specialist then creates the Client SSL profile and associates it with the virtual server.

What is the issue?

A. The SSL certificate and key have expired.
B. The SSL certificate and key do NOT match.
C. The client CANNOT verify the certification path.
D. The common name on the SSL certificate does NOT match the hostname of the site.

Correct Answer: C
Section:

QUESTION 86
-- 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
Section:

QUESTION 87
-- Exhibit --

```
ltm pool srv1_https_pool {
    members {
        192.168.2.1:https {
            address 192.168.2.1
        }
    }
}
ltm virtual https_example_vs {
    destination 192.168.1.155:https
    ip-protocol tcp
    mask 255.255.255.255
    pool srv1_https_pool
    profiles {
        http { }
        tcp { }
    }
    snat automap
    vlans-disabled
}
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message 'The connection was reset' in the browser. Connections directly to the pool member show the application is functioning correctly.
What is the issue?

A. The pool member is failing the monitor check.
B. The pool member default gateway is set incorrectly.
C. The virtual server is configured with the incorrect SNAT address.
D. The virtual server is processing encrypted traffic as plain-text HTTP.

Correct Answer: D
Section:

QUESTION 88
-- Exhibit --

```
ltm node 192.168.2.1 {
    address 192.168.2.1
    session user-disabled
    state up
}
ltm pool srv1_http_pool {
    members {
        192.168.2.1:http {
            address 192.168.2.1
        }
    }
}
ltm profile http http-example {
    app-service none
    defaults-from http
    header-erase Accept-Encoding
    via-host-name ltm_prod.example.com
    via-request append
}
ltm virtual srv1_http_vs {
    destination 192.168.1.155:http
    ip-protocol tcp
    mask 255.255.255.255
    pool srv1_http_pool
    profiles {
        http-example { }
        tcp { }
    }
    vlans-disabled
}
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is troubleshooting a virtual server. Both the virtual server and the pool are showing blue squares for their statuses, and new clients report receiving 'The connection was reset' through their browsers.
Connections directly to the pool member are successful.
What is the issue?

A. The pool member is disabled.
B. The node is marked as disabled.
C. The HTTP profile has incorrect settings.
D. The virtual server is disabled on all VLANs.

Correct Answer: B
Section:

QUESTION 89
-- Exhibit --

```
21:48:50.118288 IP 10.0.0.2.49662 > 10.0.0.1.http: S 2982039927:2982039927(0) win 8192
21:48:50.118323 IP 10.0.0.1.http > 10.0.0.2.49662: S 4109615223:4109615223(0) ack 2982039928 win 4248
21:48:50.278582 IP 10.0.0.2.49662 > 10.0.0.1.http: . ack 1 win 16638 in slot1/tmm2 lis=/Common/test-vs
21:48:50.280165 IP 10.0.0.2.49662 > 10.0.0.1.http: P 1:560(559) ack 1 win 16638 in slot1/tmm2 lis=/Common/test-vs
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg
Accept-Language: en-GB
User-Agent: Mozilla/4.0
Accept-Encoding: gzip, deflate
Host: 10.0.0.1
Connection: Keep-Alive
21:48:50.280270 IP 10.0.0.1.http > 10.0.0.2.49662: . ack 560 win 4807 out slot1/tmm2 lis=/Common/test-vs
21:48:50.283344 IP 10.0.0.1.http > 10.0.0.2.49662: P 1:122(121) ack 560 win 4807 out slot1/tmm2 lis=/Common/test-vs
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm=""
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
21:48:50.642340 IP 10.0.0.2.49662 > 10.0.0.1.http: . ack 122 win 16607 in slot1/tmm2 lis=/Common/test-vs
21:48:54.676670 IP 10.0.0.2.49662 > 10.0.0.1.http: P 560:1158(598) ack 122 win 16607 in slot1/tmm2 lis=/Common/test-vs
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg
Accept-Language: en-GB
User-Agent: Mozilla/4.0
Accept-Encoding: gzip, deflate
Host: 10.0.0.1
Connection: Keep-Alive
Authorization: Basic YWRtaW46YWRtaW4=
21:48:54.676781 IP 10.0.0.1.http > 10.0.0.2.49662: . ack 1158 win 5405 out slot1/tmm2 lis=/Common/test-vs
21:48:54.679242 IP 10.0.0.1.http > 10.0.0.2.49662: P 122:243(121) ack 1158 win 5405 out slot1/tmm2 lis=/Common/test-vs
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm=""
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
21:48:55.031314 IP 10.0.0.2.49662 > 10.0.0.1.http: . ack 243 win 16577 in slot1/tmm2 lis=/Common/test-vs
```

-- Exhibit --
Refer to the exhibit.
A user is unable to access an application.
What is the root cause of the problem?

A. The User-Agent is incorrect.
B. The 'Content-Length' is zero.
C. The user failed authentication.
D. The GET request uses the wrong syntax.

Correct Answer: C
Section:

QUESTION 90
-- Exhibit --

```
ltm monitor http memberA_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\\r\\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberB_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\\r\\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberC_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\\r\\n"
    time-until-up 0
    timeout 16
}
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is troubleshooting an HTTP monitor that is marking a pool member as down. Connecting to the pool member directly through a browser shows the application is up and functioning correctly.
How should the send string be modified to correct this issue?

A. GET /\r\n\r\n
B. GET / HTTP/1.0\r\n\r\n
C. GET /\r\nHost: \r\n\r\n
D. GET /\r\nHTTP/1.0\r\n\r\n

Correct Answer: B
Section:

QUESTION 91
-- Exhibit --

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive


HTTP/1.1 302 Moved Temporarily
Content-Length: 0
Location: https://www.example.com
Date: Tue, 23 Oct 2012 18:05:57 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Accept-Ranges: bytes
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: sessionid=a4531785-7012-46aa-b5fe-a54be482b61a; path=/
```

-- Exhibit --
Refer to the exhibit.
An LTM Specialist is performing an HTTP trace on the client side of the LTM device and notices there are many undesired headers being sent by the server in the response. The LTM Specialist wants to remove all response headers except 'Set-Cookie' and 'Location.'
How should the LTM Specialist modify the HTTP profile to remove undesired headers from the HTTP response?

A. Enter the desired header names in the 'Request Header Insert' field.
B. Enter the undesired header names in the 'Request Header Erase' field.
C. Enter the undesired header names in the 'Response Header Erase' field.
D. Enter the desired header names in the 'Response Headers Allowed' field.

Correct Answer: D
Section:

QUESTION 92
-- Exhibit --

```
Client side of LTM Device:

GET / HTTP/1.1
User-Agent: curl/7.21.0 (i486-pc-linux-gnu) libcurl/7.21.0 OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.15 libssh2/1.2.6
Host: 172.16.80.80
Accept: */*

HTTP/1.1 200 OK
Date: Thu, 25 Oct 2012 16:17:21 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Tue, 23 Oct 2012 16:14:06 GMT
ETag: "17f655-1d-4ccbc425aaf80"
Accept-Ranges: bytes
Content-Length: 29
Vary: Accept-Encoding
Content-Type: text/html
X-Pad: avoid browser bug
Set-Cookie: BIGipServermy_http_pool=1679034890.20480.0000; path=/


Server side of LTM device:

GET / HTTP/1.1
User-Agent: curl/7.21.0 (i486-pc-linux-gnu) libcurl/7.21.0 OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.15 libssh2/1.2.6
Host: 172.16.80.80
Accept: */*

HTTP/1.1 200 OK
Date: Thu, 25 Oct 2012 16:17:21 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Tue, 23 Oct 2012 16:14:06 GMT
ETag: "17f655-1d-4ccbc425aaf80"
Accept-Ranges: bytes
Content-Length: 29
Vary: Accept-Encoding
Content-Type: text/html
X-Pad: avoid browser bug
```

-- Exhibit --
Refer to the exhibit.
A web application is configured to allow sessions to continue even after a user computer is shut down for the night. A new LTM device is configured to load balance the web application to several servers. The application owner reports that application users are logged out of the web application whenever their browser is restarted or computer is rebooted.
What is the problem?

A. The virtual server does NOT have persistence configured.
B. The virtual server does NOT have persistence mirroring configured.
C. The cookie set by the LTM device does NOT have an 'Expires' value.
D. The cookie set by the server is NOT being passed to client by the LTM device.

Correct Answer: C
Section:

QUESTION 93
-- 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
```

-- 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
Section:

QUESTION 94
-- 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: B, D
Section:

QUESTION 95
-- Exhibit --

Virtual Server	Destination	Service Port	Default Pool
intranet_it	10.1.1.10	8080	web_it
intranet_hr	10.1.1.10	443	web_hr
intranet_sales	10.1.1.10	8081	web_sales
intranet_finance	10.1.1.10	8083	web_finance
intranet_engineering	10.1.1.10	8085	web_engineering

Pool	Monitor	Pool Members
web_it	http_it	10.2.2.102, 10.2.2.105
web_hr	https_hr	10.2.2.101, 10.2.2.102
web_sales	http_sales	10.2.2.101, 10.2.2.102
web_finance	http_finance	10.2.2.101, 10.2.2.102
web_engineering	http_engineering	10.2.2.102, 10.2.2.105

-- Exhibit --
Refer to the exhibits.
Every monitor has the same Send String, Recv String, and an Alias of *:*. The LTM Specialist simplifies the configuration to minimize the number of monitors.
How many unique monitors remain?

A. 1

B. 2
C. 3
D. 4
E. 5

Correct Answer: B
Section:

QUESTION 96
-- Exhibit --

```
ltm monitor http memberA_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\\r\\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberB_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\\r\\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberC_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\\r\\n"
    time-until-up 0
    timeout 16
}
```

```
ltm pool member_pool {
    members {
        memberA:http {
            address 192.168.30.10
            monitor memberA_mon
            session monitor-enabled
            state down
        }
        memberB:http {
            address 192.168.30.20
            monitor memberB_mon
            session monitor-enabled
            state down
        }
        memberC:http {
            address 192.168.30.30
            monitor memberC_mon
            session monitor-enabled
            state down
        }
    }
}
```

-- Exhibit --
Refer to the exhibits.
How should the LTM Specialist minimize the configuration?

A. Remove the pool member level monitors.
B. The configuration is as minimized as possible.
C. Create a single monitor and apply it to each pool member.
D. Create a single monitor, apply it to the pool, and remove the pool member level monitors.

Correct Answer: D
Section:

QUESTION 97
Given the log entry:
011f0005:3: HTTP header (32800) exceeded maximum allowed size of 32768 (Client sidE. vip=/Common/VS_web profile=http pool=/Common/POOL_web client_ip=10.0.0.1)
Which HTTP profile setting can be modified temporarily to resolve the issue?

A. Increase Maximum Requests
B. Decrease Maximum Requests
C. Increase Maximum Header Count
D. Decrease Maximum Header Count
E. Increase Maximum Header size
F. Decrease Maximum Header size

Correct Answer: E
Section:

QUESTION 98

Which command should the LTM Specialist use to determine the current system time?

A. date
B. time
C. uname -a
D. ntpq -p

Correct Answer: A
Section:

QUESTION 99
An LTM Specialist connects to an LTM device via the serial console cable and receives unreadable output. The LTM Specialist is using the appropriate cable and connecting it to the correct serial port.
Which command should the LTM Specialist run through ssh to verify that the baud rate settings for the serial port are correct on the LTM device?

A. tmsh list /sys console
B. tmsh edit /sys console
C. tmsh show /sys console
D. tmsh show /ltm console

Correct Answer: C
Section:

QUESTION 100
The active LTM device in a high-availability (HA) pair performs a failover at the same time the network team reports an outage of a switch on the network.
Which two items could have caused the failover event? (Choose two.)

A. a VLAN fail-safe setting
B. a monitor on a pool in an HA group
C. the standby LTM that was rebooted
D. an Auditor role that has access to the GUI
E. the standby LTM that lost connectivity on the failover VLAN

Correct Answer: A, B
Section: