301b.exam.115q

Number: 301b
Passing Score: 800
Time Limit: 120 min

301b

LTM Specialist: Maintain & Troubleshoot

Exam A

QUESTION 1
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: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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: (none)
Explanation
Explanation/Reference:

QUESTION 3

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: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)

Explanation

Explanation/Reference:

QUESTION 5
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: (none)
Explanation

Explanation/Reference:

QUESTION 6
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: (none)
Explanation

Explanation/Reference:

QUESTION 7
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 ApplicationA. 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: (none)
Explanation

Explanation/Reference:

QUESTION 8
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: (none)
Explanation

Explanation/Reference:

QUESTION 9
A new VLAN vlan301 has been configured on a highly available LTM device in partition ApplicationA. 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: (none)
Explanation

Explanation/Reference:

QUESTION 10
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: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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: (none)
Explanation

Explanation/Reference:

QUESTION 12

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: (none)
Explanation

Explanation/Reference:

QUESTION 13

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

ssldump -Aed -ni vlan301 'port 443'

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

A. HTTP Version
B. User-Agent
C. ClientHello
D. ServerHello
E. Issuer

Correct Answer: CD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 14
Given this as the first packet displayed of an ssldump:

```
2 2 1296947622.6313 (0.0001) S>CV3.1(74) Handshake
      ServerHello
Version 3.1
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: (none)
Explanation

Explanation/Reference:

QUESTION 15
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: (none)
Explanation

Explanation/Reference:

QUESTION 16
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: (none)
Explanation

Explanation/Reference:

QUESTION 17
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: (none)
Explanation

Explanation/Reference:

QUESTION 18
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: (none)
Explanation

Explanation/Reference:

QUESTION 19
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: (none)
Explanation

Explanation/Reference:

QUESTION 20
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: (none)
Explanation

Explanation/Reference:

QUESTION 21

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: (none)
Explanation

Explanation/Reference:

QUESTION 22
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: (none)
Explanation
Explanation/Reference:

QUESTION 23
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: (none)
Explanation

Explanation/Reference:

QUESTION 24
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: (none)
Explanation

Explanation/Reference:

QUESTION 25
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: (none)
Explanation

Explanation/Reference:

QUESTION 26
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: (none)
Explanation

Explanation/Reference:

QUESTION 27
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: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29

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: (none)
Explanation

Explanation/Reference:

QUESTION 30
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: (none)
Explanation

Explanation/Reference:

QUESTION 31
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: (none)
Explanation

Explanation/Reference:

QUESTION 32
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: AB

Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
The LTM Specialist is writing a custom HTTP monitor for a web application and has viewed the content by accessing the site directly via their browser. The monitor continually fails. The monitor configuration is:

```
ltm monitor http /Common/exampleComMonitor {     defaults-
from /Common/http
   destination *:*
   interval 5
   recv "Recent Searches"     send "GET /app/feed/current\?uid=20145 HTTP/1.1\\r\\nHost: www.example.com\\r\\nAccept-EncodinG. gzip,
deflate\\r\\nConnection: close\\r\\n\\r\\n"     time-until-up 0
   timeout 16
}
```

A trace shows the following request and response:

Request:
GET /app/feed/current?uid=20145 HTTP/1.1
Host www.example.com
Accept-Encoding gzip, deflate
Connection: close

Response:
HTTP/1.1 302 Moved Temporarily
Date Wed, 17 Oct 2012 18:45:52 GMT
Server Apache
Location https://example.com/login.jsp Content-
Encoding gzip
Content-Type text/html;charset=UTF-8
Set-CookiE. JSESSIONID=261EFFBDA8EC3036FBCC22D991AC6835; Path=/app/feed/current?uid=20145

What is the problem?

A. The request does NOT include a User-Agent header.
B. The HTTP monitor does NOT support monitoring jsp pages.
C. The request does NOT include any cookies and the application is expecting a session cookie.
D. The request includes an Accept-Encoding so the server is responding with a gzipped result and LTM monitors CANNOT handle gzipped responses.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
An LTM Specialist configures an HTTP monitor as follows:

```
ltm monitor http stats_http_monitor {
   defaults-from http
destination *:*
   interval 5
   recv "Health check: OK"
   send "GET /stats/stats.html HTTP/1.1\\r\\nHost: www.example.com\\r\\nAccept-EncodinG. gzip, deflate\\r\\nConnection: close\\r\\n\\r\\n"     time-
until-up 0
   timeout 16
}
```

The monitor is marking all nodes as down. A trace of the HTTP conversation shows the following:

```
GET /stats/stats.html HTTP/1.1
Host: www.example.com
Accept-EncodinG. gzip, deflate
Connection: close

HTTP/1.1 401 Authorization Required
DatE. Tue, 23 Oct 2012 19:38:56 GMT
Server: Apache/2.2.15 (Unix)
WWW-AuthenticatE. Basic realm="Please enter your credentials"
Content-LengtH. 480
Connection: close
Content-TypE. text/html; charset=iso-8859-1
```

Which action will resolve the problem?

A. Add an NTLM profile to the virtual server.
B. Add a valid username and password to the monitor.
C. Use an HTTPS monitor with a valid certificate instead.
D. Add a backslash before the colon in the receive string.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
The following decoded TCPDump capture shows the trace of a failing health monitor.

```
00:00:13.245104 IP 10.29.29.60.51947 > 10.0.0.12.http: P 1:59(58) ack 1 win 46 <nop,nop,timestamp 2494782300 238063789> out slot1/tmm3
lis=        0x0000:  4500 006e 3b19 4000 4006 ce0c 0a1d 1d3c        E..n;.@.@......<        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.HTTP1.1.
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   0ffd 0800 4500 00c9 6f68 4000 8006 755d        ....E...oh@...u]        0x0010   0a29 0015 0a29 0103 0050 e0d6 4929
90eb        .)...)...P..I)..
        0x0020   6f12 d83c 8019 fab3 9b31 0000 0101 080a        o..<.....1......
        0x0030   0068 4e10 5240 6150 4854 5450 2f31 2e31        .hN.R@aPHTTP/1.1
        0x0040   2034 3030 2042 6164 2052 6571 7565 7374        .400.Bad.Request
0x0050   0d0a 436f 6e74 656e 742d 5479 7065 3a20        ..Content-Type:.
        0x0060   7465 7874 2f68 746d 6c0d 0a44 6174 653a        text/html..Date:
        0x0070   2054 6875 2c20 3231 204a 616e 2032 3031        .Mon,.01.Jan.201
0x0080   3020 3138 3a35 383a 3537 2047 4d54 0d0a        2.00:00:01.GMT..
        0x0090   436f 6e6e 6563 7469 6f6e 3a20 636c 6f73        Connection:.clos
        0x00a0   650d 0a43 6f6e 7465 6e74 2d4c 656e 6774        e..Content-Lengt
        0x00b0   683a 2032 300d 0a0d 0a3c 6831 3e42 6164        h:.20....<h1>Bad
        0x00c0   2052 6571 7565 7374 3c2f 6831 3e               .Request</h1>
```

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

What is the issue?

A. The /test_page.html does NOT exist on the web server.
B. Incorrect syntax in send string. 'HTTP1.1' should be 'HTTP/1.1'.
C. Incorrect syntax in send string. 'Connection: Close' should be 'Connection: Open'.
D. The wrong HTTP version is specified in the send string. Version 1.2 should be used instead of version 1.1.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 37
An LTM device is monitoring pool members on port 80. The LTM device is using an HTTP monitor with a send string of GET / and a blank receive string.

What would cause the pool members to be marked down?

A. A pool member responds with an HTTP 200 series response code. B. A pool member responds with an HTTP 300 series response code. C. A pool member responds with an HTTP 400 series response code.
D. A pool member responds with an HTTP 500 series response code.
E. A pool member does NOT acknowledge the connection SYN on port 80.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
An LTM device is monitoring three pool members. One pool member is being marked down.

What should the LTM Specialist enable to prevent the server from being flooded with connections once its monitor determines it is up?

A. manual resume
B. packet shaping
C. hold down timer
D. slow ramp timer
E. fastest load balance algorithm

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An LTM device is serving an FTP virtual server that has three pool members. The FTP pool members are monitored via TCP port 21. Customers are reporting that they are able to log in, but are sometimes unable to upload files to the server.

Which monitor should the LTM Specialist configure to verify that the servers can handle file uploads?

A. FTP
B. Inband
C. External
D. Scripted
E. Real Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
An LTM HTTP pool has an associated monitor that sends a string equal to 'GET /test.html'.

Which two configurations could an LTM Specialist implement to allow server administrators to disable their pool member servers without logging into the LTM device? (Choose two.)

A. Set monitor to transparent and ask the server team to set string ‘TRANSPARENT’ in test.html.
B. Set ‘receive string’ equal to 'SERVER UP and ask the server team to set string ‘SERVER DOWN’ in test.html.
C. Set ‘alias’ equal to 'SERVER DOWN’ and ask the server team to set string ‘SERVER DOWN’ in test.html.
D. Set ‘receive disable string’ equal to 'SERVER DOWN’ and ask the server team to set string ‘SERVER DOWN’ in test.html.
E. Set ‘disable pool member’ equal to 'SERVER UP’ and ask the server team to set string ‘SERVER DOWN’ in test.html.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
An LTM Specialist is receiving reports from customers about multiple applications failing to work properly. The LTM Specialist looks at the services running and notices that the bigd process has NOT started.

How are monitored LTM device objects marked when the bigd process is stopped?

A. red or offline
B. blue or unchecked

C. green or available
D. unchanged until bigd is restarted

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
An LTM Specialist is setting up a monitor for an HTTP 1.1 server. The response to a GET / is:

HTTP/1.1 302 Moved Temporarily
Location: http://www.example.com/new/location.html

Which send string settings should the LTM Specialist use to force a proper response?

A. GET / HTTP/1.0\r\nHost: host.domain.com\r\nConnection: Close\r\n\r\n
B. GET /new/location.html HTTP/1.1\r\nHost: www.example.com\r\nConnection: Close\r\n\r\n
C. GET / HTTP/1.1\r\nHost: www.example.com/new/location.html\r\nConnection: Close\r\n\r\n
D. GET /new/location.html HTTP/1.1\r\nHost: host.domain.com/new/locations.html\r\nConnection: Close\r\n\r\n

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 43
An LTM Specialist defines a receive string in the HTTP monitor and then assigns it to the HTTP pool. The monitor has an interval of 5 seconds and a timeout of 16 seconds.

If the receive string is NOT seen in the the HTTP payload after 20 seconds, how does the LTM device mark the monitor status?

A. offline
B. unknown
C. available
D. unavailable
E. forced offline

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
An LTM Specialist receives a request to monitor the network path through a member, but NOT the member itself.

Which monitor option should the LTM Specialist enable or configure?

A. Reverse
B. Up interval
C. Transparent
D. Alias address
E. Time until up

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 45
An LTM Specialist is creating a custom EAV monitor.

In which directory should the LTM Specialist upload the script?

A. /usr/monitor
B. /usr/monitors
C. /config/monitors
D. /usr/bin/monitors
E. /config/templates

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
An FTP monitor is NOT working correctly.

Which three pieces of information does the LTM Specialist need to provide to ensure a properly working FTP monitor? (Choose three.)

A. alias
B. File path
C. username
D. password
E. FTP server port
F. FTP server IP address

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which iRule statement demotes a virtual server from CMP?

A. set ::foo 123
B. set static::foo 123
C. persist source_addr 1800
D. [class match $HTTP_CONTENT contains my_data_class]

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
What is the effect of an iRule error such as referencing an undefined variable?

A. The iRule execution will continue with the next statement.
B. The execution of the current event within the iRule will be terminated.

C. The iRule execution will be terminated, and both the client and server side connections will be reset.
D. The connection will continue, but the iRule will NOT be executed again for the lifetime of the connection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
What does the following iRule do?

```
when CLIENT_ACCEPTED {
  if { [matchclass [IP::client_addr] equals WebClient1-Whitelist1] }{
#log local0.  "Valid client IP: [IP::client_addr] - forwarding traffic"
  #Pool WebClient1

  } else {
        log local0. "Invalid client IP: [IP::client_addr] - discarding"
discard
   }
}
```

A. The iRule compares a client IP to a list. If the client IP is on the list, discard and log the discard.
B. The iRule compares a client IP to a list. If the client IP is NOT on the list, discard and log the discard.
C. The iRule compares a client IP to a list. If the client IP is on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the discard.
D. The iRule compares a client IP to a list. If the client IP is NOT on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the discard.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
What do the following iRule commands do when they are used in the same iRule?

```
set hsl [HSL::open -proto UDP -pool syslog_server_pool]
```

HSL::send $hsl "<190> [HTTP::host] from [whereis [IP::client_addr] country continent state city zip] , IP: [IP::client_addr]"

A. The commands set up a high-speed logging connection and then send the geographical database to the server.
B. The commands set up a high-speed logging connection and then send the host header and client geographical detail to the connection.
C. The commands set up a high-speed logging connection and then send the host header, HTTP payload, and client geographical detail to the connection.
D. The commands set up a high-speed logging connection to the LTM device and then send the host header and client geographical detail to the connection.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
An LTM Specialist configures the following iRule on an LTM device:

```
when HTTP_REQUEST {
   if {[string tolower [HTTP::uri]] contains "/URI1/" } {
pool Pool1
   }
  elseif {[string tolower [HTTP::uri]] contains "/URI2/" } {
pool Pool2
   }
 elseif {[string tolower [HTTP::uri]] contains "/URI3/" } {
pool Pool3
   }
 else { pool Pool4}
}
```

Given the following request: http://www.example.comURI1/index.html?fu=bar&pass=1234

Which pool will be selected by the iRule?

A. Pool1
B. Pool2
C. Pool3
D. Pool4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Given the iRule:

```
when HTTP_REQUEST {
 if {([HTTP::username] ne "") and ([HTTP::password] ne "") } {    log local0. "client ip
[IP::remote_addr] credentials provided [HTTP::username] [HTTP::password]"}  else {
   pool old_application_pool
  }
}
```

The associated virtual server has a default pool named new_application_pool.

Which functionality does the iRule provide?

A. Allows clients with credentials to access the old_application_pool and logs the access of clients without credentials to the new_application_pool.
B. Allows clients without credentials to access the old_application_pool and logs the access of clients with credentials to the new_application_pool.
C. Allows clients with credentials to access the old_application_pool and logs the attempted access of clients with credentials to the new_application_pool.
D. Allows clients without credentials to access the old_application_pool and logs the attempted access of clients without credentials to the new_application_pool.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which three HTTP headers allow an application server to determine the client's language compatibility, browser, operating system type, and compression compatibility? (Choose three.)

A. Accept
B. Accept-Encoding
C. Accept-Language

D. Host
E. User-Agent

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A web application requires the client to provide the destination server and service identification.

Which HTTP header will supply this information?

A. Host
B. From
C. Expect
D. Connection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A web application is meant to log the URI of the resource that responded to the client's initial Request-URI.

Which HTTP header will supply this information?

A. Via
B. Server
C. Trailer
D. Referer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
The end users of a web application need to verify that their browsers received the complete message-body from the web server.

Which HTTP header will accomplish this?

A. Range
B. Expect
C. Accept-Ranges
D. Content-Length

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
An HTTP 1.1 application utilizes chunking.

Which header should be used to notify the client's browser that there are additional HTTP headers at the end of the message?

A. ETag
B. From
C. Trailer
D. Expect

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A web application sends information about message integrity and content life time to the client.

Which two HTTP headers should be used in sending the client information? (Choose two.)

A. ETag
B. Expect
C. Expires
D. Content-MD5
E. Content-Range
F. Content-Length

Correct Answer: CD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 59
A web developer has created a custom HTTP call to a backend application. The HTTP headers being sent by the HTTP call are:

```
GET / HTTP/1.1
User-Agent: MyCustomApp (v1.0)
Accept: text/html
Cache-Control: no-cache
Connection: keep-alive
CookiE. somecookie=1
```

The backend server is responding with the following:

```
HTTP/1.1 400 Bad Request
DatE. Wed, 20 Jul 2012 17:22:41 GMT
Connection: close
```

Why is the HTTP web server responding with a HTTP 400 Bad Request?

A. The client request does NOT include a Host header.
B. The User-Agent header contains an invalid character.
C. The web server is NOT expecting a keep-alive connection.
D. The web server is configured to accept HTTP 1.0 requests only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A client is attempting to log in to a web application that requires authentication. The following HTTP headers are sent by the client:

```
GET /owa/ HTTP/1.1
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
User-Agent: curl/7.26.0
Host: 10.0.0.14
Accept: */*
Accept-EncodinG. gzip,deflate
```

The web server is responding with the following HTTP headers:

```
HTTP/1.1 401 Unauthorized
Content-TypE. text/html
Server: Microsoft-IIS/7.5
WWW-AuthenticatE. NTLM
DatE. Wed, 16 Aug 1977 19:12:31 GMT    Content-
LengtH. 1293
```

The client has checked the login credentials and believes the correct details are being entered.

What is the reason the destination web server is sending an HTTP 401 response?

A. The username and password are incorrect.
B. The server has an incorrect date configured.
C. The client is using the wrong type of browser.
D. The wrong authentication mechanism is being used.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
The LTM device is configured to provide load balancing to a set of web servers that implement access control lists (ACL) based on the source IP address of the client. The ACL is at the network level and the web server is configured to send a TCP reset back to the client if it is NOT permitted to connect.

The virtual server is configured with the default OneConnect profile.

The ACL is defined on the web server as:

Permit: 192.168.136.0/24
Deny: 192.168.116.0/24

The packet capture is taken of two individual client flows to a virtual server with IP address 192.168.136.100.
Client A - Src IP 192.168.136.1 - Virtual Server 192.168.136.100:

Clientside:

09:35:11.073623 IP 192.168.136.1.55684 > 192.168.136.100.80: S 869998901:869998901(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
09:35:11.073931 IP 192.168.136.100.80 > 192.168.136.1.55684: S 2273668949:2273668949(0) ack 869998902 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:35:11.074928 IP 192.168.136.1.55684 > 192.168.136.100.80: . ack 1 win 16425
09:35:11.080936 IP 192.168.136.1.55684 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:35:11.081029 IP 192.168.136.100.80 > 192.168.136.1.55684: . ack 299 win 4678

Serverside:

09:35:11.081022 IP 192.168.136.1.55684 > 192.168.116.128.80: S 685865802:685865802(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:35:11.081928 IP 192.168.116.128.80 > 192.168.136.1.55684: S 4193259095:4193259095(0) ack 685865803 win 5840 <mss
1460,nop,nop,sackOK,nop,wscale
6>
09:35:11.081943 IP 192.168.136.1.55684 > 192.168.116.128.80: . ack 1 win 4380
09:35:11.081955 IP 192.168.136.1.55684 > 192.168.116.128.80: P 1:299(298) ack 1 win 4380
09:35:11.083765 IP 192.168.116.128.80 > 192.168.136.1.55684: . ack 299 win 108

Client B - Src IP 192.168.116.1 - Virtual Server 192.168.136.100:

Clientside:

09:36:11.244040 IP 192.168.116.1.55769 > 192.168.136.100.80: S 3320618938:3320618938(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
09:36:11.244152 IP 192.168.136.100.80 > 192.168.116.1.55769: S 3878120666:3878120666(0) ack 3320618939 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:36:11.244839 IP 192.168.116.1.55769 > 192.168.136.100.80: . ack 1 win 16425
09:36:11.245830 IP 192.168.116.1.55769 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:36:11.245922 IP 192.168.136.100.80 > 192.168.116.1.55769: . ack 299 win 4678

Serverside:

09:36:11.245940 IP 192.168.136.1.55684 > 192.168.116.128.80: P 599:897(298) ack 4525 win 8904
09:36:11.247847 IP 192.168.116.128.80 > 192.168.136.1.55684: P 4525:5001(476) ack 897 win 142

Why was the second client flow permitted by the web server?

A. A global SNAT is defined.
B. SNAT automap was enabled on the virtual server.
C. The idle TCP session from the first client was re-used.
D. A source address persistence profile is assigned to the virtual server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
An LTM Specialist is troubleshooting an HTTP monitor. The pool member is accessible directly through a browser, but the HTTP monitor is marking the pool member as down.

GET / HTTP/1.1

HTTP/1.1 400 Bad Request
DatE. Tue, 23 Oct 2012 21:39:07 GTM
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4
mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Content-LengtH. 226
Connection: close
Content-TypE. text/html; charset=iso-8859-1

Which issue is the pool member having?

A. The pool member has too many concurrent connections.

B. The pool member is rejecting the request because it is invalid.
C. The pool member lacks the object requested by the monitor.
D. The pool member is NOT accepting requests from the LTM device IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which command will identify the active LTM device currently handling client traffic?

A. b ha table show
B. tmsh list /sys ha-status
C. tmsh show /cm traffic-group D. tmsh run /sys failover standby
E. tmsh show /sys ha-status all-properties

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which command should an LTM Specialist use on the command line interface to show the health of RAID array hard drives?

A. tmsh show /sys raid disk
B. tmsh show /ltm raid disk
C. tmsh show /sys raid status
D. tmsh show /ltm disk status

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which command line interface command will check if the BIG-IP platform contains a packet velocity ASIC (PVA)?

A. bigpipe platform show | grep -i pva
B. tmsh show /sys hardware pva status
C. tmsh show /sys hardware | grep -i pva
D. tmsh show /ltm hardware | grep -i pva

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 66
Which two subsystems could the LTM Specialist utilize to access an LTM device with lost management interface connectivity? (Choose two.)

A. AOM
B. ILO
C. SCCP
D. ALOM

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A BIG-IP Operator has made a grave error and deleted a few virtual servers on the active LTM device fronting the web browsing proxies. The BIG-IP Operator has NOT yet performed a configuration sync.

Which command should the LTM Specialist execute on the active LTM device to force a failover to the standby node and restore web browsing?

A. tmsh /sys failover standby
B. tmsh run /sys failover standby
C. tmsh /sys failover status standby
D. tmsh run /sys failover status standby

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
The output of a tmsh command is: ---------- Net::Interface Name Status Bits Bits Errs Errs Drops Drops Colli In Out In Out In Out sions ---------- 1.1 down 0 0 0 0 0 0 0 1.2 up 191.4K 0 0 0 374 0 0 1.3 down 0 0 0 0 0 0 0 1.4 up 22.5K 0 0 0 44 0 0 2.1 miss 0 0 0 0 0 0 0 2.2 miss 0 0 0 0 0 0 0 mgmt up 43.2G 160.0G 0 0 0 0 0
Which command was executed on the LTM device to show the output?

A. tmsh show /net interface
B. tmsh /net show interface statusC. tmsh /net show interface
D. tmsh show /net interface status

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Given:

Filesystem Size Used Avail Use% Mounted on
/dev/md11 248M 248M 0 100% /
/dev/md13 3.0G 76M 2.8G 3% /config
/dev/md12 1.7G 1.1G 476M 71% /usr
/dev/md14 3.0G 214M 2.6G 8% /var
/dev/md0 30G 2.2G 26G 8% /shared /dev/md1
6.9G 288M 6.3G 5% /var/log none 3.9G
452K 3.9G 1% /dev/shm none 3.9G 19M
3.9G 1% /var/tmstat none 3.9G 1.2M 3.9G
1% /var/run prompt 4.0M 12K 4.0M 1%
/var/prompt /dev/md15 12G 8.3G 3.1G 74%

/var/lib/mysql Which command is used to produce this output?

A. df
B. du
C. lsof
D. ps
E. vmstat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An LTM Specialist realizes that a datacenter engineer has changed the console baud rate.

Which command determines the current baud rate via the command line interface?

A. tmsh show /ltm console
B. tmsh show /sys console
C. tmsh list /sys baud-rate
D. tmsh list /net baud-rate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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: (none)
Explanation

Explanation/Reference:

QUESTION 72
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: (none)
Explanation

Explanation/Reference:

QUESTION 73
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: (none)
Explanation

Explanation/Reference:
QUESTION 74
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: (none)
Explanation

Explanation/Reference:

QUESTION 75
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: (none)
Explanation

Explanation/Reference:
QUESTION 76
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: (none)
Explanation

Explanation/Reference:

QUESTION 77
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: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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: (none)
Explanation

Explanation/Reference:

QUESTION 80
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: (none)
Explanation

Explanation/Reference:

QUESTION 81
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: (none)
Explanation

Explanation/Reference:

QUESTION 82
-- Exhibit –

```
ltm profile httpclass acct_class {
    app-service none
    defaults-from httpclass
    paths { glob:/accounting }
    pool srv1_http_pool
    redirect none
}
ltm profile httpclass marketing_class {
    app-service none
    defaults-from httpclass
    paths { glob:/marketing }
    pool srv1_http_pool
    redirect none
}
ltm profile httpclass default_class {
    app-service none
    defaults-from httpclass
    pool srv2_http_pool
    redirect none
}
ltm virtual http_vs {
    destination 192.168.1.155:http
    http-class {
        acct_class
        marketing_class
        default_class
    }
    ip-protocol tcp
    mask 255.255.255.255
    pool srv2_http_pool
    profiles {
        http { }
        tcp { }
    }
    snat automap
    vlans-disabled
}
```

-- Exhibit -Refer to the exhibit.

An LTM Specialist is reviewing the virtual server configuration on an LTM device.

Which two actions should the LTM Specialist perform to minimize the virtual server configuration? (Choose two.)

A. Remove 'snat automap' from the virtual server.
B. Remove the 'http' profile from the virtual server.
C. Remove the 'default_class' from the virtual server.
D. Combine 'acct_class' and 'marketing_class' into one class and update associations on the virtual server.
E. Combine 'marketing_class' and 'default_class' into one class and update associations on the virtual server.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 84
-- 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: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
-- Exhibit –

Data Format: Normalized
Auto Refresh: Disabled | Refresh

Search

Status	Pool/Member	Partition / Path	Bits In	Bits Out	Packets In	Packets Out	Connections Current	Connections Maximum	Connections Total	Requests Total	Request Queue Depth	Request Queue 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?

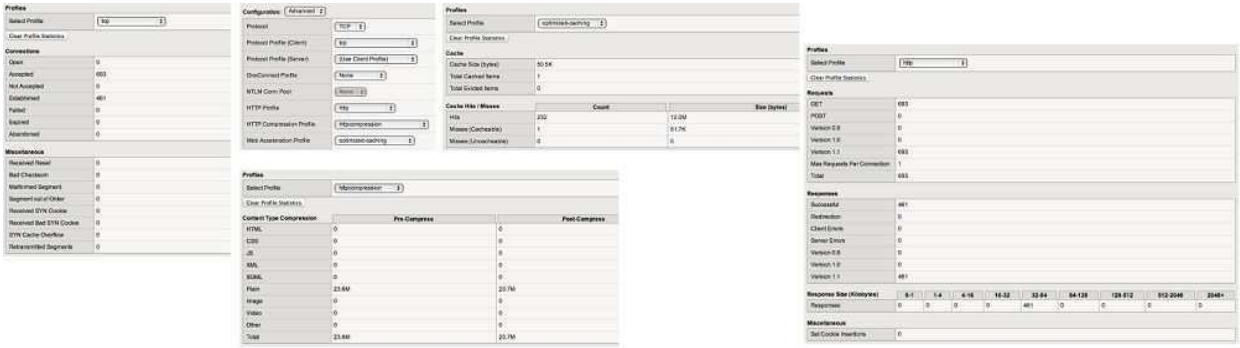
A. ftp_pool
B. http_pool
C. server1_80
D. server_pool

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86

-- 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?

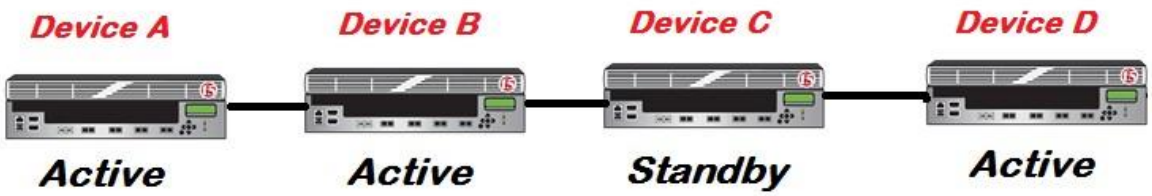
A. tcp
B. http
C. httpcompression
D. optimized-caching

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 88
-- Exhibit –

An SSH configuration error exposes a potential vulnerability - CVE-2012-1493

Recommended upgrade version	Solution Links	Heuristic Name	Was this helpful?
10.2.4 11.0.0.HF2 11.1.0.HF3 11.2.0	SOL13600	H386652	Yes No

Details

Related Changes
ID 379600

Description
An SSH configuration error in the default SSH configuration may allow unauthorized remote users to gain privileged access to the system.

Recommendation resolution
Upgrade to an unaffected version. For workaround information, refer to the linked Solution.

Additional Information
The current configuration appears to be vulnerable.

-- 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.

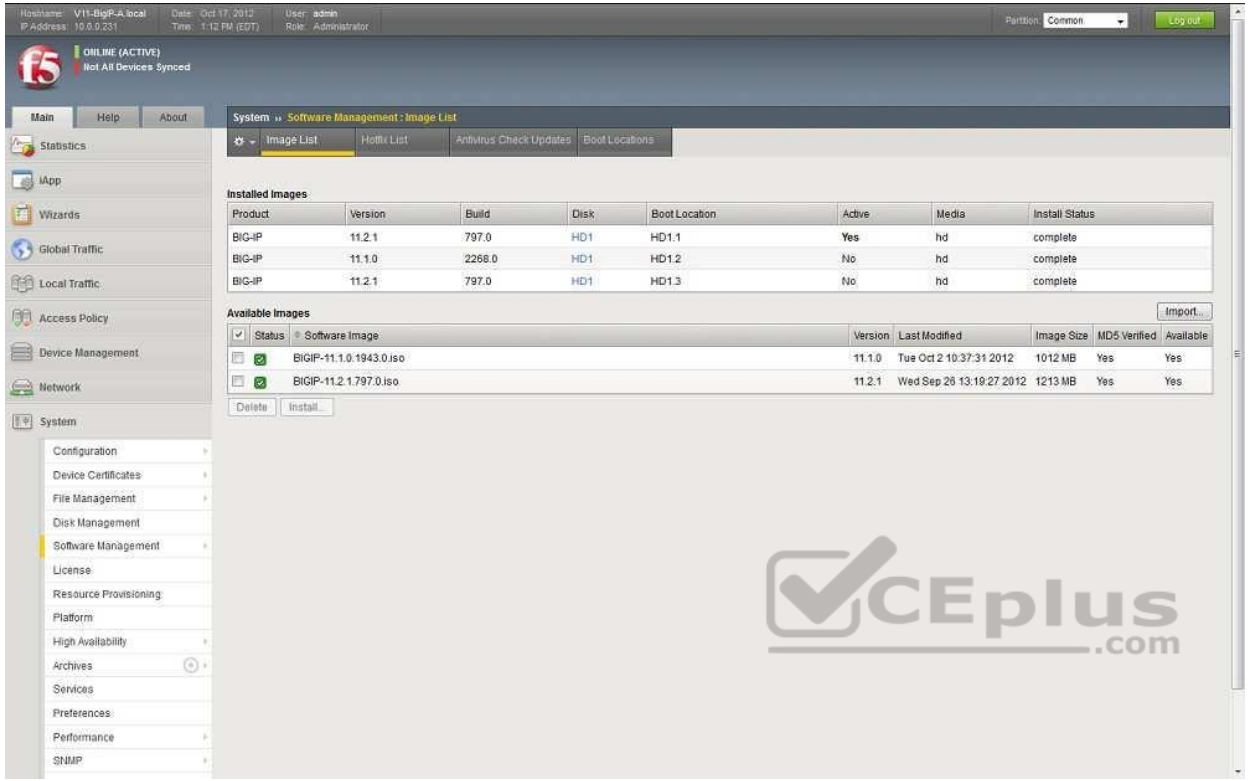
Which procedure resolves the problem?

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: (none)
Explanation

Explanation/Reference:
QUESTION 89

-- 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.

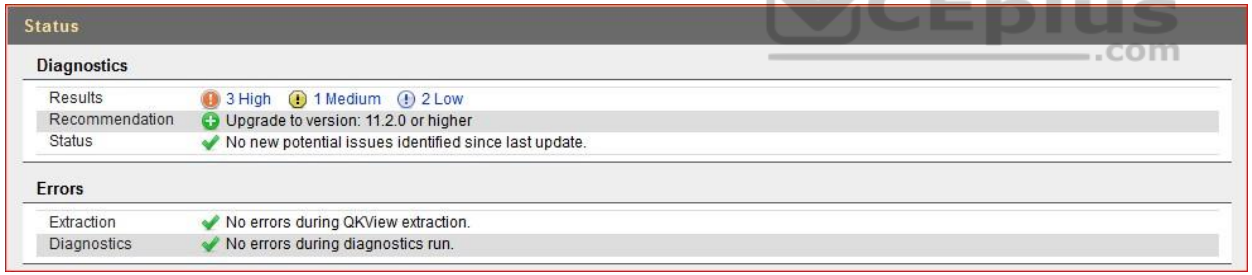
C. Obtain product version image from downloads.f5.com. Import product version image.
Install image onto BIG-IP platform.
Select product version image and click Install.
Select the available disk and volume set name.

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: (none)
Explanation

Explanation/Reference:

QUESTION 90
-- Exhibit –



-- Exhibit --

Refer to the exhibit.

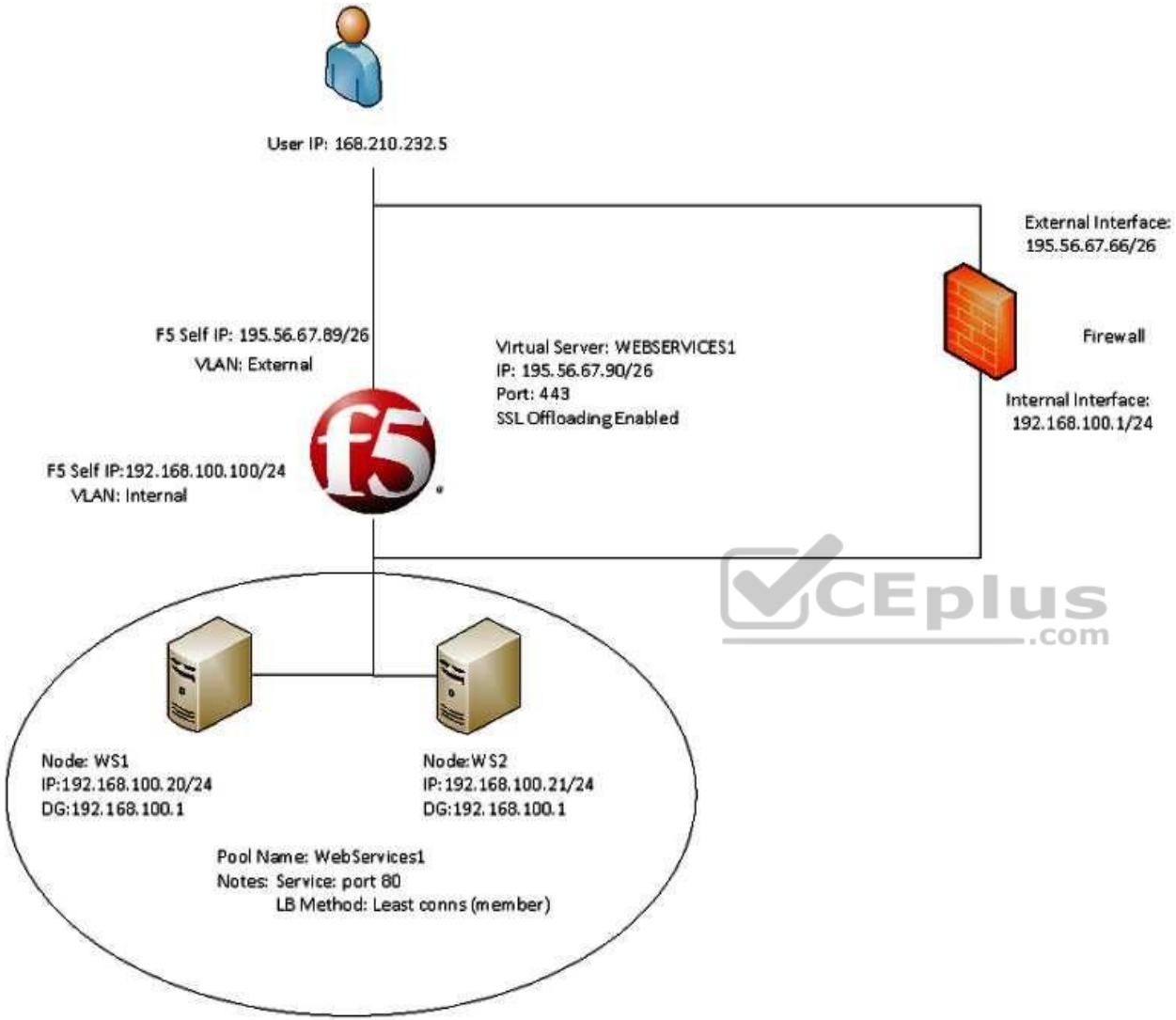
Which step should an LTM Specialist take next to finish upgrading to HD1.3?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 92
-- 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.

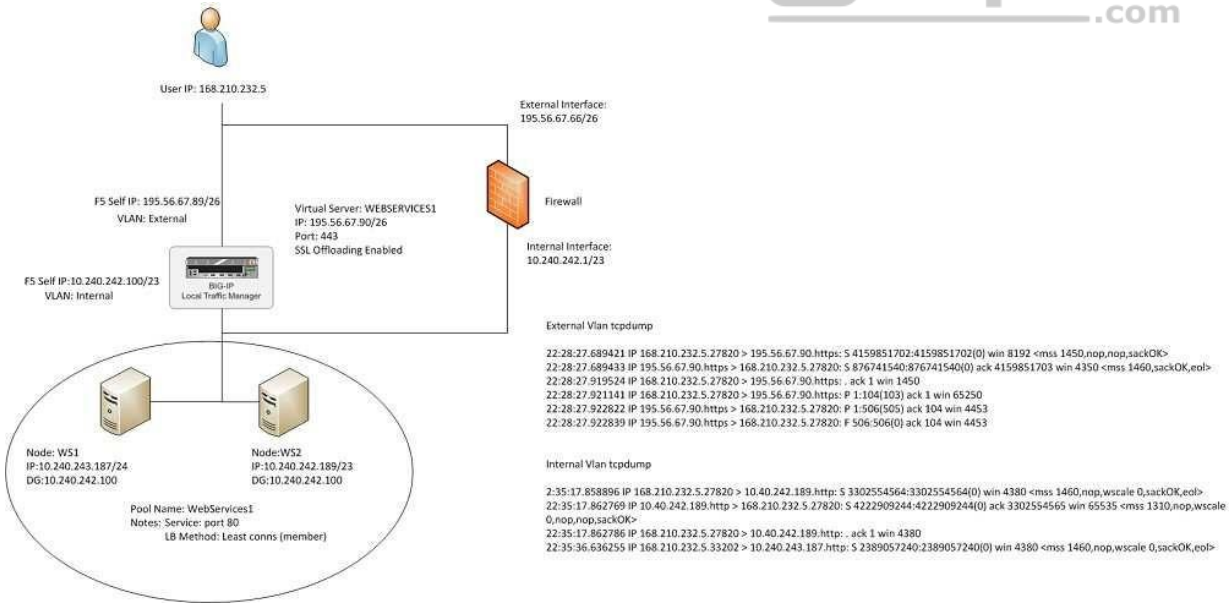
The LTM Specialist does an ssldump on the virtual server and receives the results as per the exhibit.
What is the problem?

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: (none)
Explanation

Explanation/Reference:

QUESTION 93
-- Exhibit –



-- 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: (none)
Explanation

Explanation/Reference:
QUESTION 94
-- 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.

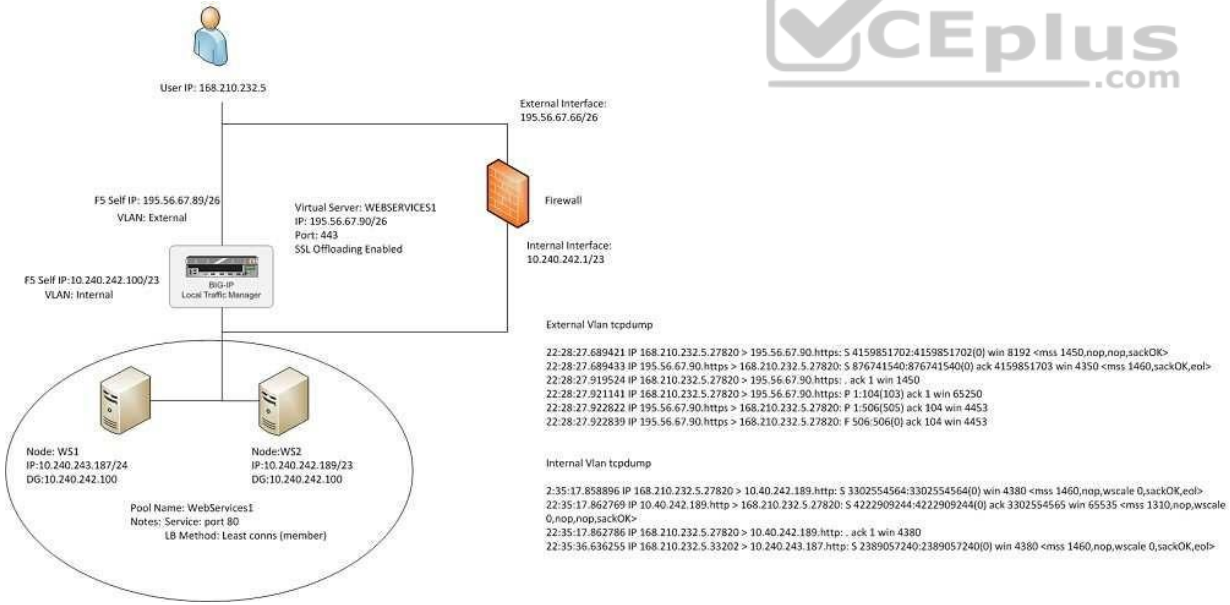
The LTM Specialist has the tcpdump extract and knows the client software has at least one connection to a VS on port 1990. However, when a tcpdump runs on the internal VLAN, there is no record of port 1990 in the tcpdump.

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: (none)
Explanation
Explanation/Reference:

QUESTION 95
- Exhibit --



-- 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.

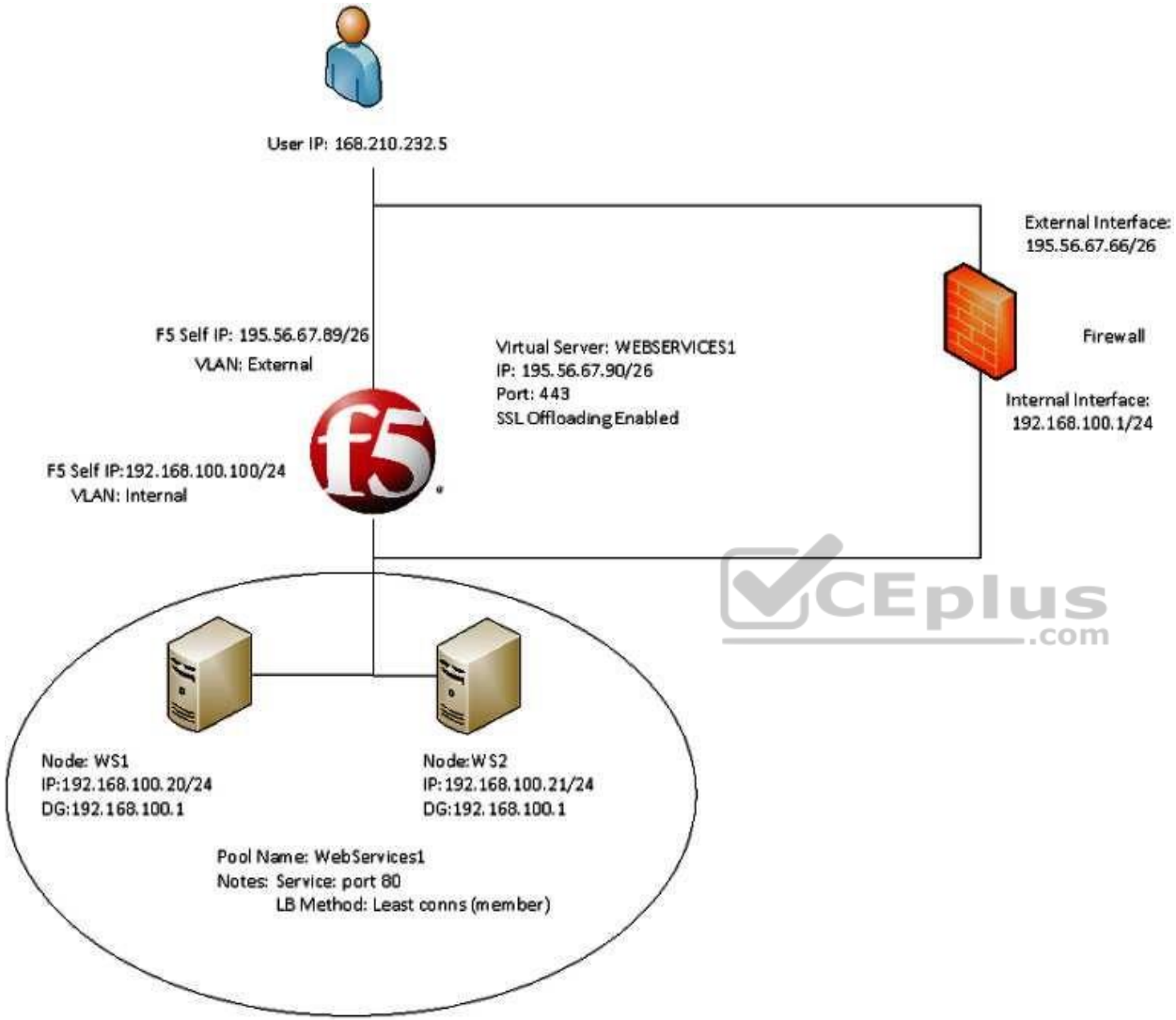
Assuming no wildcard virtual servers, how many distinct virtual servers does the client connect to on the LTM device?

A. 2 B.
3
C. 4
D. 6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 97
-- 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
```

-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 98
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 99
-- 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
```

-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 100
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 101
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 102
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 103
-- 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: (none)
Explanation

Explanation/Reference:
QUESTION 104

-- 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>
13:59:08.704146 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>
13:59:08.706366 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 4042 <nop,nop,timestamp 2395417933 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 4042 <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>
13:59:13.439692 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>
13:59:13.439958 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>
13:59:16.439821 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 2395785676 0,sackOK,eol>
13:59:16.439842 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 1533617 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.

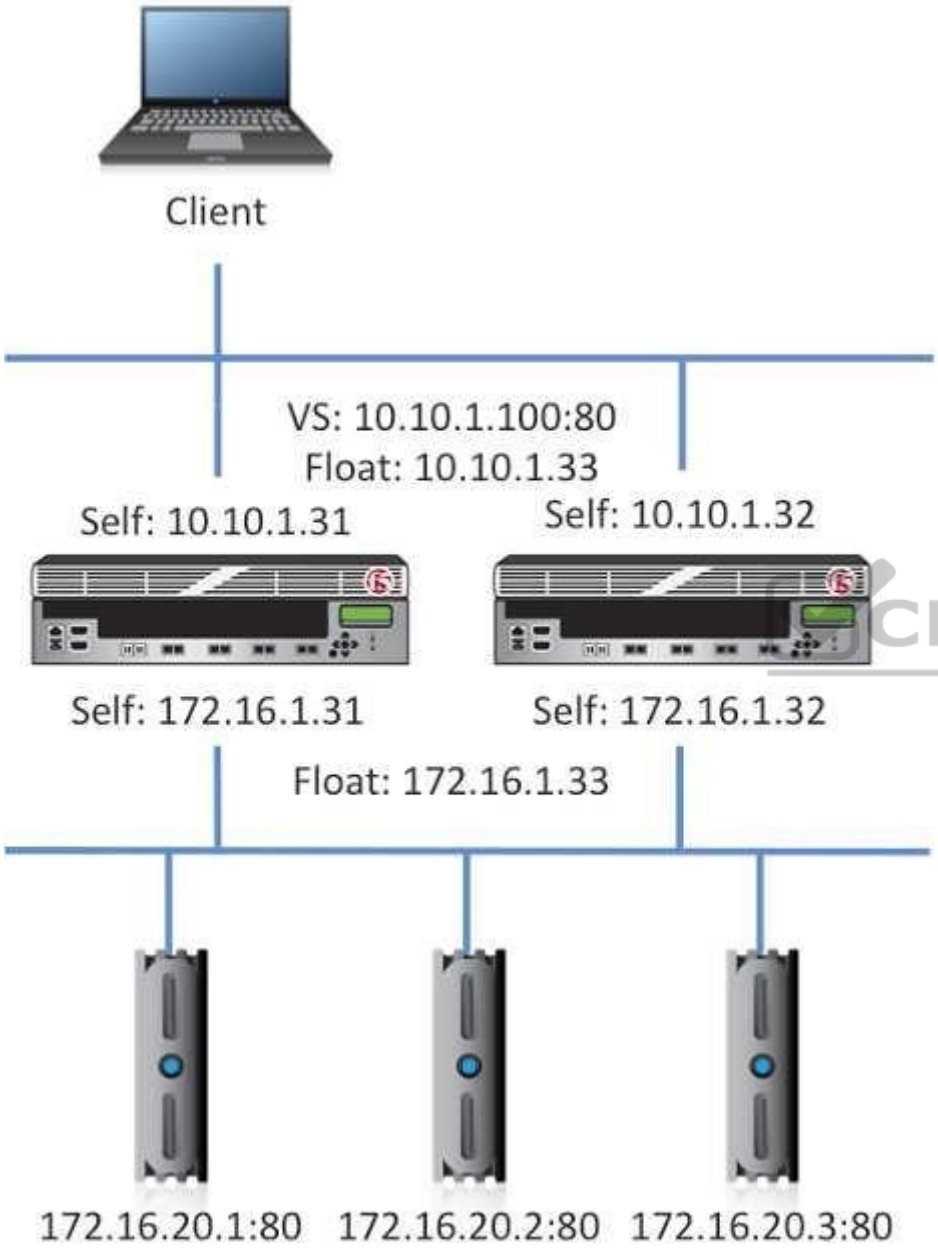
Which two actions will resolve the problem? (Choose two.)

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: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
-- 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 10.10.1.100C. 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: (none)
Explanation

Explanation/Reference:

QUESTION 106
-- 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'.

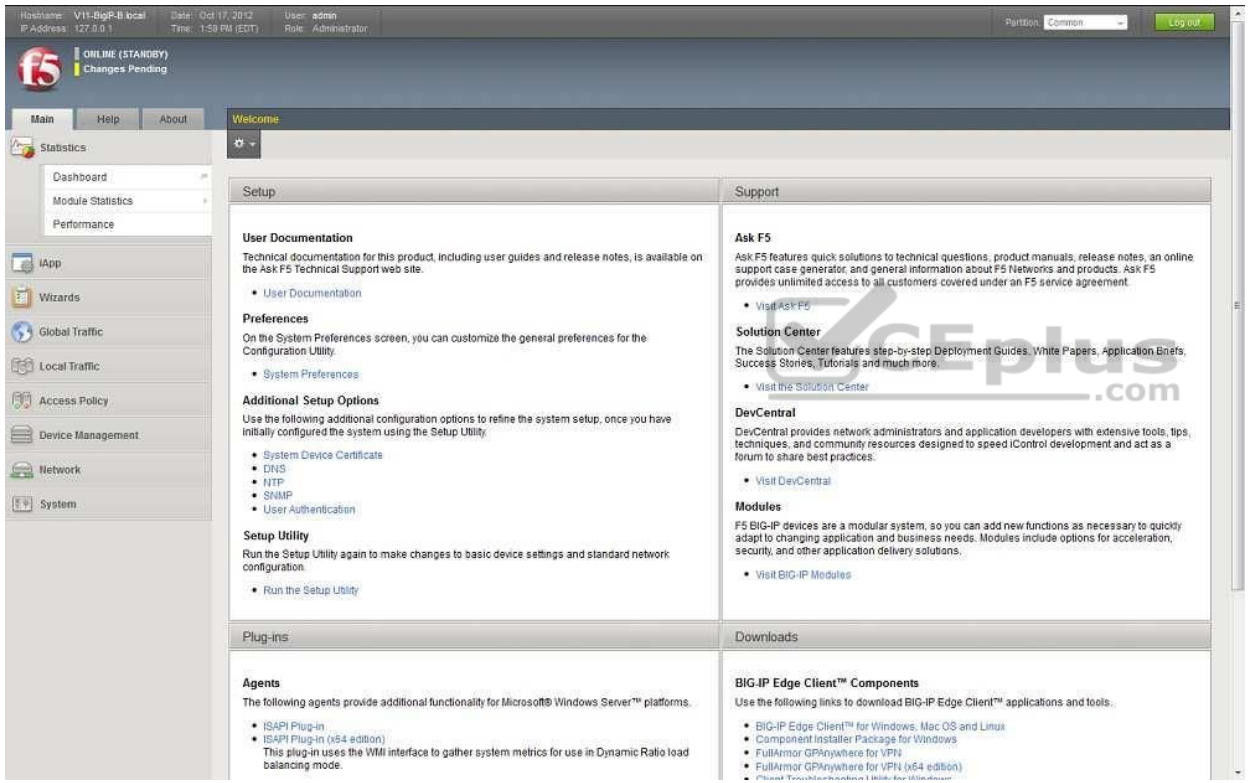
What is the solution?

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: (none)
Explanation

Explanation/Reference:

QUESTION 107
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 108
-- Exhibit –

General Configuration Custom

Profile Name	avr_example
Partition / Path	Common
Parent Profile	analytics
Profile Description	
Statistics Logging Type	☑ Internal ☐ External
Traffic Capturing Logging Type	☐ Internal ☐ External
SMTP Configuration	None (Note: Setting can be changed only through the default analytics profile.)
Notification Type	☑ Syslog ☐ SNMP ☐ E-mail
Trust XFF	✓ Enable
Transaction Sampling Ratio	Sample all transactions (Note: Setting can be changed only through the default analytics profile.)

Included Objects

Virtual Servers

Name	Destination	Service Port	Partition / Path
No records to display.			

Add... Delete

Statistics Gathering Configuration Custom

Collected Metrics	✓ Server Latency ☐ Page Load Time ✓ Throughput ☐ User Sessions
Collected Entities	☐ URLs ☐ Countries ☐ Client IP Addresses ✓ Response Codes ☐ User Agents ✓ Methods

Alerts and Notifications Configuration

Add New Rule

Alert when Average TPS is below Trans/sec, for seconds in an Application Add

Active Rules

Rule	Edit
Alert when Average Server Latency is below 50 ms for 300 seconds in an Application.	Edit

Delete

Cancel Finished **Note:** Changes you make might take up to 10 minutes to be reflected in the charts.

-- 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.

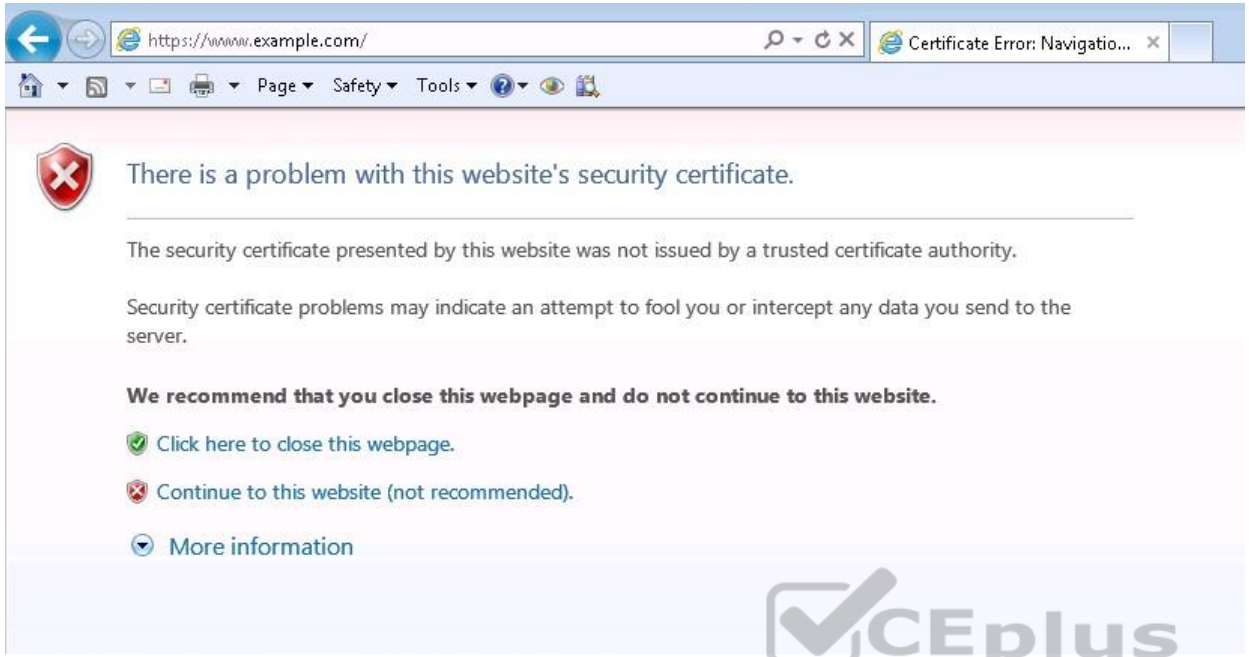
Which configuration should the LTM Specialist modify to achieve the expected results?

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: (none)
Explanation

Explanation/Reference:

QUESTION 109
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 110
-- 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
s1qGE7MkmIxLtwYjjWXmwxW7sCFLl9kt6pFOatzqeK3WxbdM5yF/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: (none)
Explanation

Explanation/Reference:

QUESTION 111
-- 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
```

-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 112
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 113
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 114
-- 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: (none)
Explanation

Explanation/Reference:

QUESTION 115
-- 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: (none)
Explanation

Explanation/Reference: