F5.301b.v2022-05-13.q134

Exam Code:	301b
Exam Name:	LTM Specialist: Maintain & Troubleshoot
Certification Provider:	F5
Free Question Number:	134
Version:	v2022-05-13
# of views:	1665
# of Questions views:	1340
https://www.dumpsdb.com/dumps/F5/301b/F5.301b.v2022-05-13.q134	

NEW QUESTION: 1
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 any cookies and the application is expecting a session cookie.
B. The request does NOT include a User-Agent header.
C. The HTTP monitor does NOT support monitoring jsp pages.
D. The request includes an Accept-Encoding so the server is responding with a gzipped result and LTM monitors CANNOT handle gzipped responses.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
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 vlan301 'host 192.168.0.251 or host 192.168.0.252'
B. tcpdump -ni vlan301 'host 192.168.0.253'
C. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.253'
D. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.251 or host 192.168.0.252'
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
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, although connections directly to the pool member show the application is functioning correctly.
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
}
How should the LTM Specialist resolve this issue?
A. Enable HTTP monitoring on the pool.
B. Disable SNAT Automap on the virtual server.
C. Remove the HTTP profile from the virtual server.
D. Add a ClientSSL profile to the virtual server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
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. Incorrect syntax in send string. 'Connection: Close' should be 'Connection: Open'.
B. Incorrect syntax in send string. 'HTTP1.1' should be 'HTTP/1.1'.
C. The /test_page.html does NOT exist on the web server.
D. The wrong HTTP version is specified in the send string. Version 1.2 should be used instead of version 1.1.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
-- Exhibit -

-- Exhibit --
Refer to the exhibit.
The virtual server is listening on port 443.
What is the solution to the problem?
A. Modify the virtual server HTTP Profile to 'Redirect RewritE. Matching'.
B. Modify the virtual server HTTP Profile to 'Redirect RewritE. All'.
C. Modify the virtual server TCP profile to disable Nagle's Algorithm.
D. Add an SSL Client profile to the existing virtual server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
An LTM device is load balancing telnet and ssh applications in a client/server environment experiencing significant packet delay.
Which setting in the TCP profile should reduce the amount of packet delay?
A. disable Bandwidth Delay
B. increase Maximum Segment Retransmissions
C. disable Nagle's Algorithm
D. enable Proxy Maximum Segment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
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 show /net interface status
C. tmsh /net show interface
D. tmsh /net show interface status
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
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 Header size
C. Increase Maximum Header size
D. Decrease Maximum Header Count
E. Decrease Maximum Requests
F. Increase Maximum Header Count
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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 any cookies and the application is expecting a session cookie.
B. The HTTP monitor does NOT support monitoring jsp pages.
C. The request does NOT include a User-Agent header.
D. The request includes an Accept-Encoding so the server is responding with a gzipped result and LTM monitors CANNOT handle gzipped responses.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
What is a benefit provided by F5 Enterprise Manager?
A. Enterprise Manager allows administrators to establish baseline application usage and generate an alert if an administratively set threshold for the application is exceeded.
B. Enterprise Manager allows administrators to identify application vulnerabilities. Virtual patches are then automatically generated and applied to remediate the detected application vulnerability.
C. 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.
D. Enterprise Manager allows administrators to analyze traffic flow and create custom application IPS signatures.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
Users are experiencing low throughput when downloading large files over a high-speed WAN connection.
Extensive packet loss was found to be an issue but CANNOT be eliminated.
Which two TCP profile settings should be modified to compensate for the packet loss in the network? (Choose two.)
A. slow start
B. proxy options
C. proxy buffer low
D. proxy buffer high
E. Nagle's algorithm
Answer: C,D (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 12
An LTM device has been configured to log the reasons for generating TCP RST packets.
The following log entry occurs:
"01230140:3: RST sent from 192.168.1.100:80 to 192.168.1.124:39272, [0x112d82a:1721] {peer} TCP RST from remote system."
Which condition will trigger this log entry?
A. The LTM device has reached the maximum number of allowed attempts to send the data segment to the affected TCP connection.
B. The LTM device reset the connection because no pool members are available.
C. A virtual server connection limit has been reached.
D. The host at the other end terminated the TCP connection.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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. tcpdump -s 64 -i internal -w /shared/ssl.pcap host 172.16.20.1
ssldump -r /shared/ssl.pcap
B. ssldump -i internal host 172.16.20.1
C. curl -d - -k https://172.16.20.1
D. tcpdump -i internal host 172.16.20.1 > /shared/ssl.pcap
ssldump < /shared/ssl.pcap
Answer: (SHOW ANSWER)

NEW QUESTION: 14
-- Exhibit -

```
Client side of LTM Device:

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

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


Server side of LTM device:

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

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

dumpsdb.com

-- Exhibit --

Refer to the exhibit.

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

What is the problem?

A. The cookie set by the LTM device does NOT have an "Expires" value.

B. The virtual server does NOT have persistence configured.

C. The virtual server does NOT have persistence mirroring configured.

D. The cookie set by the server is NOT being passed to client by the LTM device.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

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. external VLAN interface of the LTM device

C. management VLAN interface of the LTM device
D. network interface of client machine
E. internal VLAN interface of the LTM device
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 16
-- 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
}
```

dumpsdb.com

-- 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 'default_class' from the virtual server.
C. Remove the 'http' profile 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.
Answer: B,D (LEAVE A REPLY)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
-- Exhibit-

Capture through LTM device

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on External, link-type EN10MB (Ethernet), capture size 96 bytes

16:52:54.866907 IP 192.168.1.1.6789 > 192.168.1.211.443: S 2995599259:2995699259(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:52:54.866974 IP 192.168.1.211.443 > 192.168.1.1.6789: S 2305990363:2305990363(0) ack 2995699260 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:52:54.868417 IP 192.168.1.1.6789 > 192.168.1.211.443: . ack 1 win 16425
16:52:54.868422 IP 192.168.1.1.6789 > 192.168.1.211.443: P 1:105(104) ack 1 win 16425
16:52:54.868451 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:52:54.868457 IP 192.168.1.211.443 > 192.168.1.1.6789: . ack 105 win 4484
16:52:57.869207 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:53:01.068627 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:53:04.268911 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,sackOK,eol>
16:53:07.468781 IP 192.168.1.211.443 > 192.168.1.1.6789: R 1:1(0) ack 105 win 4484
```

Capture direct to application server

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes

09:46:03.428985 IP 192.168.1.1.31214 > 192.168.10.80.8443: S 1295563595:1295563595(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:46:03.430000 IP 192.168.10.80.8443 > 192.168.1.1.31214: S 2062014236:2062014236(0) ack 1295563596 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 3>
09:46:03.430041 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 1 win 4380
09:46:03.463946 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 1:137(136) ack 1 win 4380
09:46:03.465072 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 137 win 864
09:46:03.466127 IP 192.168.10.80.8443 > 192.168.1.1.31214: P 1:139(138) ack 137 win 864
09:46:03.466150 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 139 win 4518
09:46:03.720161 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 137:196(59) ack 139 win 4518
09:46:03.720183 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 196:542(346) ack 139 win 4518
09:46:03.721853 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 542 win 998
09:46:03.723009 IP 192.168.10.80.8443 > 192.168.1.1.31214: . 139:1599(1460) ack 542 win 998
09:46:03.723071 IP 192.168.10.80.8443 > 192.168.1.1.31214: P 1599:2693(1094) ack 542 win 998
09:46:03.723026 IP 192.168.10.80.8443 > 192.168.1.1.31214: F 2693:2693(0) ack 542 win 998
09:46:03.723060 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 2693 win 7072
09:46:03.723072 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 2694 win 7072
09:46:03.818084 IP 192.168.1.1.31214 > 192.168.10.80.8443: F 542:542(0) ack 2694 win 7072
09:46:03.819820 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 543 win 998
```

Trace direct to application server

Started	Time Chart	!	Time	Sent	Received	Method	Result	Type	URL
00:00:00.000	This page (index.html) is from Server 1								
+0.000		!	9.140	278	2480	GET	200		http://srv1.example.com/
+9.144		!	9.134	336	5079	GET	200		http://srv1.example.com/header.gif
+9.146		!	9.266	334	19307	GET	200		http://srv1.example.com/left.gif
+9.147		!	9.232	335	14644	GET	200		http://srv1.example.com/right.gif
+9.149		!	9.189	336	4192	GET	200		http://srv1.example.com/footer.jpg
	9.186 → 18.414 →	!	18.412	1619	45702	5 requests			

Trace through LTM device

Started	Time Chart	!	Time	Sent	Received	Method	Result	Type	URL
00:00:00.000	This page (index.html) is from SSL Server 1								
+0.000		!	0.428	346	2650	GET	200		https://www.exarple.com/
+0.435		!	9.110	300	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/header.gif
+0.435		!	9.322	298	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/left.gif
+0.435		!	9.322	299	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/right.gif
+0.435		!	9.322	300	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/footer.jpg
	← 0.452 9.759 →	!	9.757	1543	2650	5 requests			

dumpsQD.com

```
ltm virtual VS_HTTP {
    destination 10.10.17.100:http
    ip-protocol tcp
    mask 255.255.255.255
    pool Pool_HTTP
    profiles {
        customHTTP { }
        tcp { }
    }
    vlans-disabled
}
ltm pool Pool_HTTP {
    members {
        172.16.20.1:http {
            address 172.16.20.1
        }
    }
}
ltm profile http customHTTP {
    app-service none
    defaults-from http
    encrypt-cookies none
    fallback-host none
    fallback-status-codes none
    header-erase Host
    header-insert none
    insert-xforwarded-for disabled
    lws-separator none
    lws-width 80
    max-header-count 64
    max-header-size 32768
    max-requests 0
    oneconnect-transformations enabled
    pipelining enabled
    redirect-rewrite none
    request-chunking preserve
    response-chunking selective
    response-headers-permitted none
    security disabled
    via-request preserve
    via-response preserve
}
```

-- Exhibit -

Refer to the exhibits.

An LTM Specialist is troubleshooting an application configured on an LTM device on a one-armed configuration. The application is NOT working through the LTM device but does work when accessed directly via the application servers. The virtual server 192.168.1.211:443 is configured to SNAT using the address 192.168.1.144 and references a pool with the member 192.168.10.80:443. No Client or Server SSL profiles are associated. The LTM Specialist has collected two traffic captures to help determine the issue.

What is the problem with the configuration on the LTM device?

A. Pool member is configured to use wrong port.

B. Virtual server is configured without SSL Profiles.

C. Virtual server is configured to use wrong port.

D. Pool member is configured for SSL off-loading.

Answer: (SHOW ANSWER)

NEW QUESTION: 18

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 status
B. tmsh /net show interface status
C. tmsh show /net interface
D. tmsh /net show interface
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
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 attempted access of clients with credentials to the new_application_pool.
B. Allows clients with credentials to access the old_application_pool and logs the access of clients without credentials to the new_application_pool.
C. Allows clients without credentials to access the old_application_pool and logs the attempted access of clients without credentials to the new_application_pool.
D. Allows clients without credentials to access the old_application_pool and logs the access of clients with credentials to the new_application_pool.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
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 edit /sys console
B. tmsh show /ltm console
C. tmsh show /sys console
D. tmsh list /sys console

Answer: C (LEAVE A REPLY)

NEW QUESTION: 21

-- Exhibit -

-- Exhibit --

Refer to the exhibit.

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

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

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

B. Configure SNAT on the virtual server.

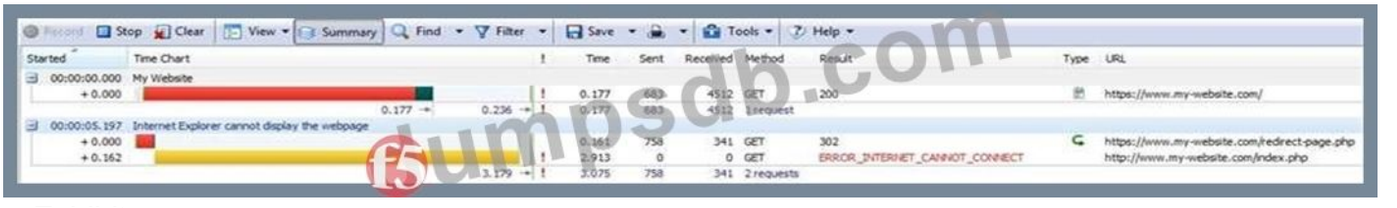
C. Change server default gateway to point at LTM internal floating IP.

D. Configure SNAT on the pool.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 22

-- Exhibit-



-- Exhibit --

Refer to the exhibit.

The virtual server is listening on port 443.

What is the solution to the problem?

A. Modify the virtual server HTTP Profile to 'Redirect RewritE.All'.

B. Modify the virtual server TCP profile to disable Nagle's Algorithm.

C. Modify the virtual server HTTP Profile to 'Redirect RewritE.Matching'.

D. Add an SSL Client profile to the existing virtual server.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
There are three servers in the pool: 172.16.20.1, 172.16.20.2, and 172.16.20.3, with the virtual IP address
10.0.20.88.
A user CANNOT connect to an HTTP application. To understand the problem and find a solution, the LTM Specialist runs two concurrent traces on the LTM device, with the following results:
Trace on client side:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on 0.0, link-type EN10MB (Ethernet), capture size 96 bytes
22:22:07.423759 IP 172.16.20.100.53875 > 10.0.20.88.80: S 998346084:998346084(0) win 5840 <mss
1460,sackOK,timestamp 67942058 0,nop,wscale 4>
22:22:07.424056 IP 10.0.20.88.80 > 172.16.20.100.53875: S 4671780:4671780(0) ack 998346085 win
4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2392362490 67942058,sackOK,eol>
22:22:07.424776 IP 172.16.20.100.53875 > 10.0.20.88.80: . ack 1 win 365 <nop,nop,timestamp 67942058
2392362490>
22:22:07.424790 IP 172.16.20.100.53875 > 10.0.20.88.80: P 1:149(148) ack 1 win 365
<nop,nop,timestamp 67942058 2392362490>
22:22:07.424891 IP 10.0.20.88.80 > 172.16.20.100.53875: . ack 149 win 4528
<nop,nop,timestamp
2392362491 67942058>
22:22:12.024850 IP 10.0.20.88.80 > 172.16.20.100.53875: R 1:1(0) ack 149 win 4528
6 packets captured
6 packets received by filter
0 packets dropped by kernel
Trace on server side:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on internal, link-type EN10MB (Ethernet), capture size 96 bytes
22:22:07.424881 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss
1460,nop,wscale 0,nop,nop,timestamp 2392362491 0,sackOK,eol>
22:22:08.424893 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss
1460,nop,wscale 0,nop,nop,timestamp 2392363491 0,sackOK,eol>
22:22:09.625082 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss

1460,nop,wscale 0,nop,nop,timestamp 2392364691 0,sackOK,eol>
22:22:10.825194 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380
<mss
1460,sackOK,eol>
4 packets captured
4 packets received by filter
0 packets dropped by kernel
What should the LTM Specialist do to solve the problem?
A. Enable the virtual server.
B. Configure the virtual server to use SNAT.
C. Modify the monitor of the pool.
D. Edit the packet filter rules.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
-- Exhibit -

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

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

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

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

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

f5 unpsdb.com

-- 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. 591 seconds
E. 590 seconds
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
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
How should the LTM Specialist resolve this issue?
A. Change the interval on the monitor from 5 seconds to 30 seconds.
B. Change the HTTP version in the send string from HTTP/1.1 to HTTP/1.0.
C. Add 'Connection: close\r\n' to the monitor's send string.
D. Add '200 OK' to the monitor's receive string.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
-- Exhibit- -- Exhibit -

```
18:25:47.354188 IP 192.168.1.100.55596 > 192.168.1.155.8080: S 3650835520:3650835520(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK> in slot1/tmm0 lis=
....E..4cE@..../...d.....,............ .......................
18:25:47.354218 IP 192.168.1.155.8080 > 192.168.1.100.55596: S 2357787[illegible]:2357[illegible](0) ack 3650835521 win 3780 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..4.O@....#.......d...,..............................".....//test/http_custom_redirect_vs
18:25:47.357679 IP 192.168.1.100.55596 > 192.168.1.155.8080: . ack 1 win 16695 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(cF@....:...d....,...........P.A7.....".....//test/http_custom_redirect_vs
18:25:47.365725 IP 192.168.1.100.55596 > 192.168.1.155.8080: P 1:294(293) ack 1 win 16695 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..McG@........d....,...........P.A7\
..GET / HTTP/1.1
Host: 192.168.1.155:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:16.0; Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive

."...../test/http_custom_redirect_vs
18:25:47.365805 IP 192.168.1.155.8080 > 192.168.1.100.55596: P 1:105(104) ack 294 win 3780 out slot1/tmm0 lis=/test/http_custom_redirect_vs
....E....S@............d...,.........P.......HTTP/1.0 302 Found
Location: https://192.168.1.155:8080/
Connection: Keep-Alive
Content-Length: 0

."...../test/http_custom_redirect_vs
18:25:47.382739 IP 192.168.1.100.55597 > 192.168.1.155.8080: S 2429178084:2429178084(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK> in slot1/tmm0 lis=
....E..4cH@....,...d.....-....P....... ..!......................
18:25:47.382752 IP 192.168.1.155.8080 > 192.168.1.100.55597: S 197089061:197089061(0) ack 2429178085 win 3780 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..4.V@............d...-..W%..P.......................".....//test/http_custom_redirect_vs
18:25:47.384086 IP 192.168.1.100.55597 > 192.168.1.155.8080: . ack 1 win 16695 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(cI@....7...d.....-....P...W&P.A7.....".....//test/http_custom_redirect_vs
18:25:47.384092 IP 192.168.1.100.55597 > 192.168.1.155.8080: P 1:89(88) ack 1 win 16695 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E...cJ@........d.....-....P...W&P.A7gN......S...O..P.......x...z&u.....i..!K..[v...?..(.......9.8...5.E.D.3.2...A...../.......
..."...../test/http_custom_redirect_vs
18:25:47.384106 IP 192.168.1.155.8080 > 192.168.1.100.55597: . ack 89 win 3868 out slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(.Z@....$.......d...-..W&..Q=P........".....//test/http_custom_redirect_vs
18:25:47.571574 IP 192.168.1.100.55596 > 192.168.1.155.8080: . ack 105 win 16669 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(cK@....(...d....,..........JP.A..n...".....//test/http_custom_redirect_vs
18:27:42.414390 IP 192.168.1.100.55596 > 192.168.1.155.8080: F 294:294(0) ack 105 win 16669 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(b)@........d....,..........JP.A..m...".....//test/http_custom_redirect_vs
18:27:42.414425 IP 192.168.1.155.8080 > 192.168.1.100.55596: . ack 295 win 4073 out slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(..@............d...,...J....P........".....//test/http_custom_redirect_vs
18:27:42.414431 IP 192.168.1.155.8080 > 192.168.1.100.55596: F 105:105(0) ack 295 win 4073 out slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(..@....-.......d...,...J....P........".....//test/http_custom_redirect_vs
18:27:42.415916 IP 192.168.1.100.55596 > 192.168.1.155.8080: . ack 106 win 16669 in slot1/tmm0 lis=/test/http_custom_redirect_vs
....E..(h-@........d....,..........KP.A..1...".....//test/http_custom_redirect_vs
```

dumpsdb.com

```
ltm profile httpclass /test/http_custom_redirect {
    app-service none
    defaults-from httpclass
    pool none
    redirect https://[HTTP::host][HTTP::uri]
}
ltm pool eCommerce_https_pool {
    members {
        10.1.1.1:https {
            address 10.1.1.1
        }
    }
    partition test
}
ltm virtual /test/http_custom_redirect_vs {
    destination 192.168.1.155:8080
    http-class {
        /test/http_custom_redirect
    }
    ip-protocol tcp
    mask 255.255.255.255
    partition test
    profiles {
        http { }
        tcp { }
    }
    vlans-disabled
}
ltm virtual https_vs {
    destination /Common/192.168.1.155:https
    ip-protocol tcp
    mask 255.255.255.255
    partition test
    pool eCommerce_https_pool
    profiles {
        /Common/example.com {
            context clientside
        }
        /Common/serverssl-insecure-compatible {
            context serverside
        }
        /Common/tcp { }
    }
    snat automap
    vlans-disabled
}
```

dumpsdb.com

Refer to the exhibits.

An LTM Specialist is reconfiguring a virtual server to redirect all clients to HTTPS. Testing reveals that the redirect is functioning incorrectly. As part of the troubleshooting process, the LTM Specialist performs a packet capture.
What is the issue?
A. The redirect is sending the client to the incorrect location.
B. The virtual server is incorrectly processing the HTTP request.
C. The redirect is causing an infinite loop.
D. The virtual server is missing a clientssl profile.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
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. available
B. forced offline
C. offline
D. unknown
E. unavailable
Answer: (SHOW ANSWER)

NEW QUESTION: 28
-- Exhibit -

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

dumpsdb.com

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

dumpsdb.com

-- Exhibit --

Refer to the exhibits.

Every monitor has the same Send String, Recv String, and an Alias of *:*. The LTM Specialist simplifies the configuration to minimize the number of monitors.

How many unique monitors remain?

A. 4

B. 1

C. 2

D. 5

E. 3

Answer: (SHOW ANSWER)

NEW QUESTION: 29

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. sssldump

B. tcpdump

C. telnet

D. curl

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 30

An LTM Specialist loads a UCS file generated on a different LTM device and receives the following error message:

"mcpd[2395]: 01070608:0: License is not operational (expired or digital signature does not match contents)"

Which command should the LTM Specialist use to prevent the error?

A. tmsh load /sys /ucs rma <path/to/UCS>

B. tmsh show /sys license
C. bigpipe config save /config.ucs
D. tmsh show /sys hardware
E. tmsh load /sys ucs <path/to/UCS> no-license
Answer: E (LEAVE A REPLY)

NEW QUESTION: 31
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 "Process Case-Insensitivity" option for the virtual server needs to be selected.
D. The pool members of both pools need to be set up as case-insensitive members.
Answer: (SHOW ANSWER)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 32
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
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 33
A OneConnect profile is applied to a virtual server. The LTM Specialist would like the client source IP addresses within the 10.10.10.0/25 range to reuse an existing server side connection. Which OneConnect profile source mask should the LTM Specialist use?
A. 255.255.255.224
B. 255.255.255.255
C. 255.255.255.128
D. 255.255.255.0
E. 0.0.0.0
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
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 Destination 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 IP is carried through from the External Vlan to the Internal Vlan
D. by checking to see if the Source port is carried through from the External Vlan to the Internal Vlan
Answer: (SHOW ANSWER)

NEW QUESTION: 35
-- Exhibit- -- Exhibit -

Refer to the exhibit.

An LTM Specialist is troubleshooting a new HTTP monitor on a pool. The pool member is functioning correctly when accessed directly through a browser, although the monitor is marking the member as down. As part of the troubleshooting, the LTM Specialist has captured the monitor traffic via tcpdump.

How should the LTM Specialist resolve this issue?

A. Add the 'icmp' monitor to the node.

B. Add the 'http' monitor to the pool.

C. Correct the firewall rules on the pool member.

D. Modify the receive string to valid content.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 36

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. bcm56xxd
B. mcpd
C. sod
D. lind
E. promptstatusd
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
-- Exhibit -

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

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

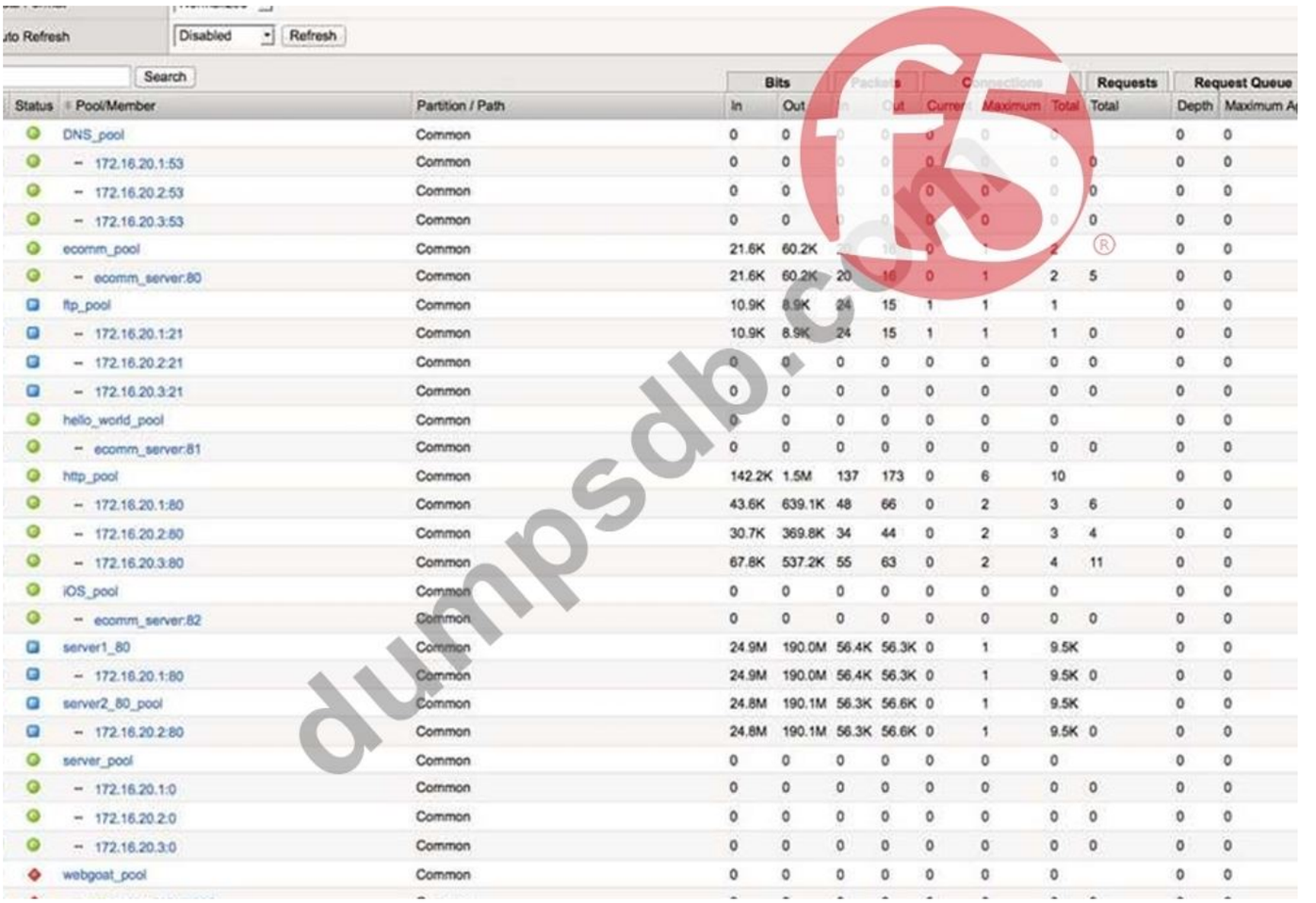
C. Incorrect syntax in send string. 'HTTP/1.1' should be 'HTTP1.1'.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

-- Exhibit-



Status	Pool/Member	Partition / Path	Bits In	Bits 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
	172.16.20.1:53	Common	0	0	0	0	0	0	0	0
	172.16.20.2:53	Common	0	0	0	0	0	0	0	0
	172.16.20.3:53	Common	0	0	0	0	0	0	0	0
	ecomm_pool	Common	21.6K	60.2K	0	1	2		0	0
	ecomm_server:80	Common	21.6K	60.2K	0	1	2	5	0	0
	ftp_pool	Common	10.9K	8.9K	1	1	1		0	0
	172.16.20.1:21	Common	10.9K	8.9K	1	1	1	0	0	0
	172.16.20.2:21	Common	0	0	0	0	0	0	0	0
	172.16.20.3:21	Common	0	0	0	0	0	0	0	0
	hello_world_pool	Common	0	0	0	0	0		0	0
	ecomm_server:81	Common	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

-- Exhibit --

Refer to the exhibit.

Which pool can be removed without affecting client traffic?

A. server_pool

B. server1_80

C. ftp_pool

D. http_pool

Answer: (SHOW ANSWER)

NEW QUESTION: 39

-- Exhibit -

-- Exhibit -Refer to the exhibit. A pair of LTM devices are configured for HA. The LTM Specialist observes from a capture that
there is a successful connection from a client directly to a web server and an unsuccessful connection from a client via the LTM device to the same web server.
Which two solutions will solve the configuration problem? (Choose two.)
A. Configure SNAT on the virtual server.
B. Change server default gateway to point at LTM internal floating IP.
C. Configure SNAT on the pool.
D. Change server default gateway to point at LTM internal self IP.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 40
Which two alerting capabilities can be enabled from within an application visibility reporting (AVR) analytics profile? (Choose two.)
A. sFlow
B. high speed logging (HSL)
C. SNMP
D. e-mail
E. LCD panel alert
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 41
-- Exhibit --

```
New TCP connection #3: 172.16.1.20(49379) <-> 172.16.20.1(443)
3 1  0.0006 (0.0006)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
3 2  0.0009 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          ed 15 16 5f c2 9d bf 5e e6 70 0e a4 86 59 bf 27
          e7 b5 fa 49 38 fd 24 d7 c3 1e c1 9f d2 67 e4 f7
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                     NULL
3 3  0.0009 (0.0000)  S>C  Handshake
      Certificate
3 4  0.0009 (0.0000)  S>C  Handshake
      ServerHelloDone
New TCP connection #4: 172.16.1.20(49380) <-> 172.16.20.1(443)
4 1  0.0004 (0.0004)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
4 2  0.0007 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          f5 eb fe e9 8e fc e9 7f c5 13 1b 40 69 15 08 72
          95 ef 43 e5 4e 10 f4 3b b2 3e 5c ec 5e ee 66 a8
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                     NULL
4 3  0.0007 (0.0000)  S>C  Handshake
      Certificate
4 4  0.0007 (0.0000)  S>C  Handshake
      ServerHelloDone
3    0.0015 (0.0006)  C>S  TCP RST
4    0.0010 (0.0003)  C>S  TCP RST
```

-- Exhibit --

Refer to the exhibit.

dumpsdb.com

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 device initiating the connection
C. the application server
D. the destination device of the initial connection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
Which command line interface command will check if the BIG-IP platform contains a packet velocity ASIC (PVA)?
A. tmsh show /sys hardware | grep -i pva
B. tmsh show /sys hardware pva status
C. tmsh show /ltm hardware | grep -i pva
D. bigpipe platform show | grep -i pva
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
-- Exhibit-

```
Monitor definition:

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

HTTP Headers from tcpdump:

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

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

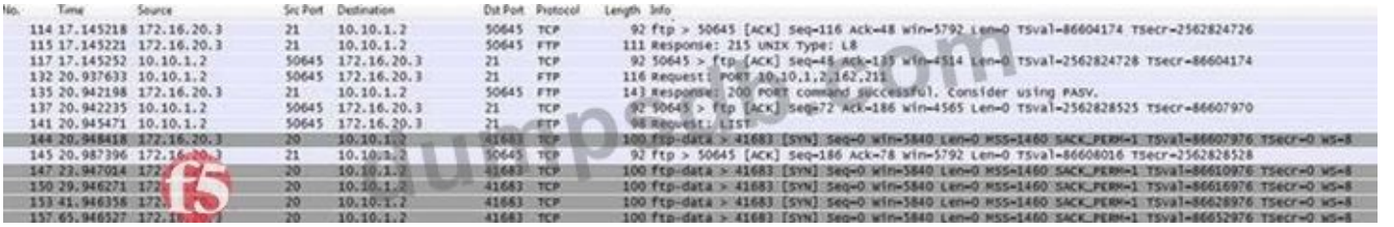
dumpsdb.com

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

A. The monitor is NOT configured to follow the redirect.
B. The send string is incorrect.
C. The response is compressed.
D. The monitor timeout is too short.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
-- Exhibit-
-- Exhibit -
Refer to the exhibit.
An LTM Specialist has created a virtual server to load balance traffic to a pool of HTTPS servers. The servers use client certificates for user authentication. The virtual server has clientssl, serverssl, and http profiles enabled. Clients are unable to connect to the application through the virtual server. Clients are able to connect to the application servers directly.
What is the root cause of the problem?
A. The clientssl profile is NOT set to require a client certificate.
B. The application server does NOT see the client certificate due to SSL offload.
C. The LTM device does NOT trust the issuing CA of the client certificate.
D. The application server does NOT support 2048-bit keys.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
-- 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	41.946356	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. command connection failing
C. PORT command disallowed
D. LIST command disallowed
Answer: (SHOW ANSWER)

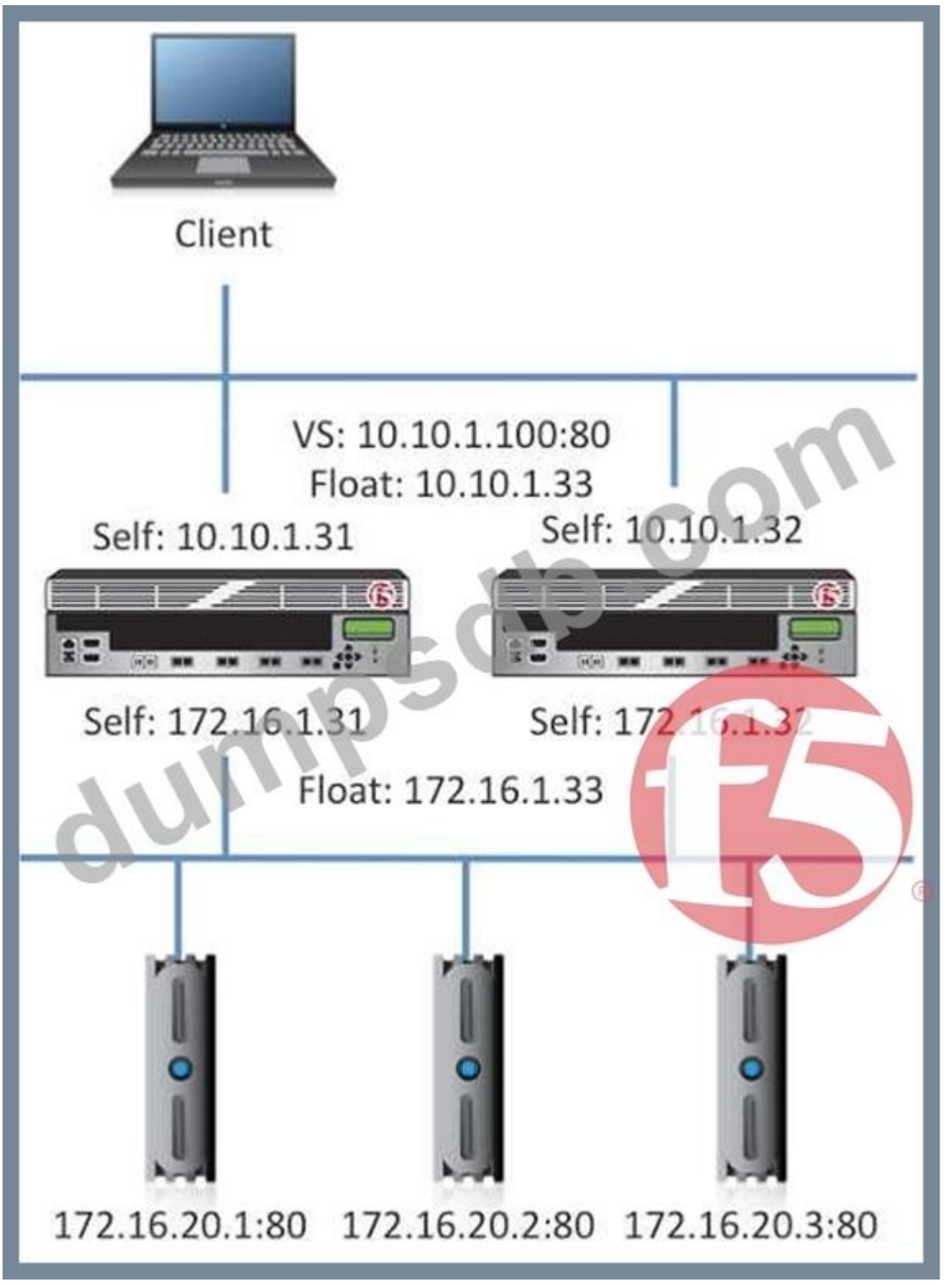
NEW QUESTION: 46

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

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 47
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 Active Directory authentication
B. the LTM device's external VLAN
C. the switch local to the user
D. a user's machine
E. the LTM device's internal VLAN
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 48
-- 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 172.16.20.1
C. tcpdump -i internal port 80 and host 172.16.1.33
D. tcpdump -i external port 80 and host 10.10.1.100
Answer: A (LEAVE A REPLY)

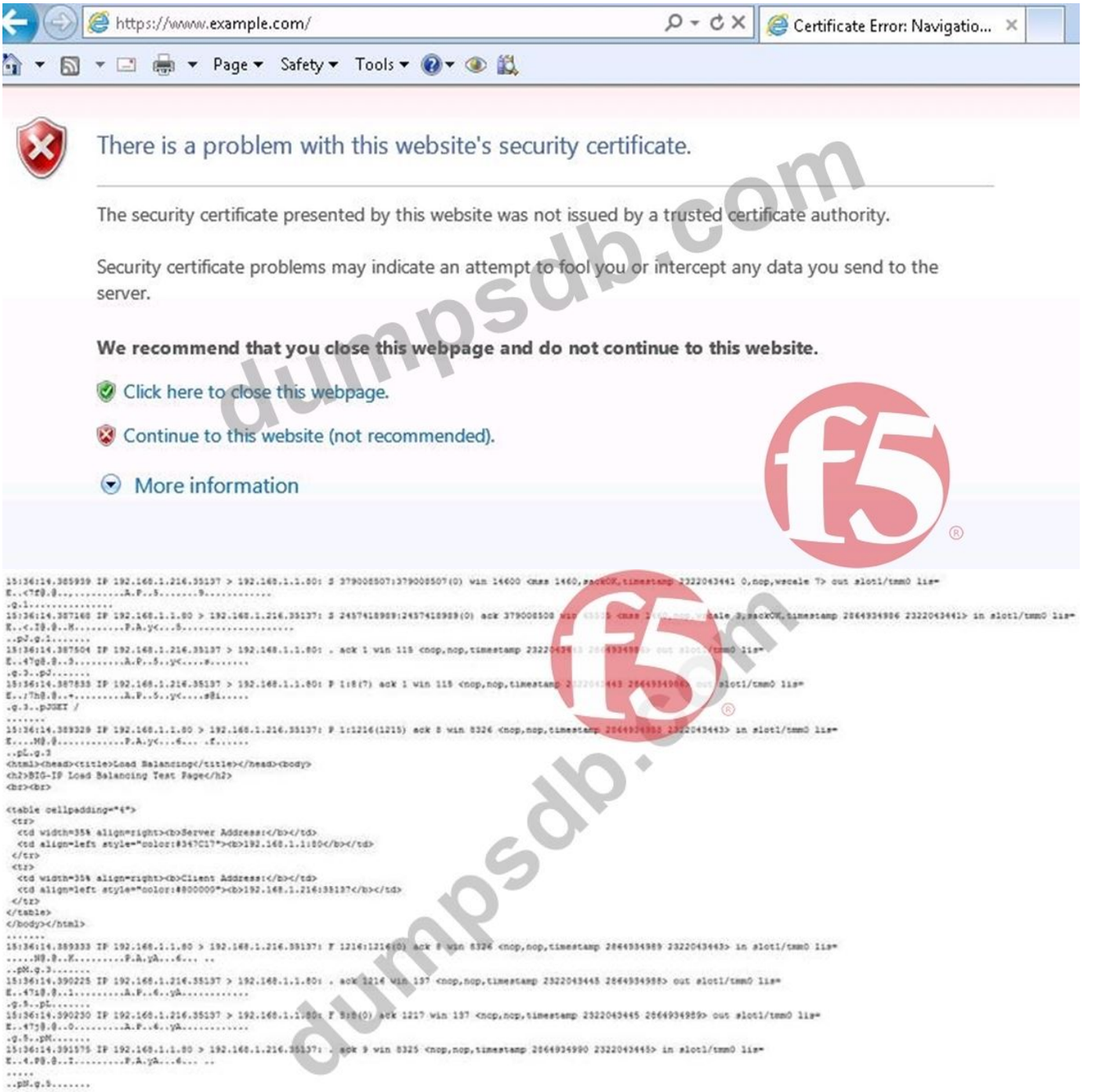
NEW QUESTION: 49
A web application requires the client to provide the destination server and service identification. Which HTTP header will supply this information?
A. Connection
B. Host
C. From
D. Expect
Answer: B (LEAVE A REPLY)

NEW QUESTION: 50
An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "Unable to connect" in the browser, although connections directly to the pool member show the application is functioning correctly. The LTM device configuration is:
ltm virtual /Common/vs_https {
destination /Common/10.10.1.110:443
ip-protocol udp
mask 255.255.255.255
pool /Common/pool_https
profiles {
/Common/udp { }
}
translate-address enabled
translate-port enabled
vlans-disabled
}
ltm pool /Common/pool_https {
members {
/Common/172.16.20.1:443 {
address 172.16.20.1
}
}
}
What issue is the LTM Specialist experiencing?
A. The pool member is marked down by a monitor.
B. The pool member is marked down administratively.

C. The virtual server is disabled on all VLANs.
D. The virtual server is configured for the incorrect protocol.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
An LTM Specialist troubleshooting an issue looks at the following /var/log/ltm entries:
Oct 2 04:52:42 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 05:37:16 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 05:57:32 slot1/tmm2 crit tmm2[21729]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 06:30:03 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 06:37:44 slot1/tmm2 crit tmm2[21729]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 06:47:05 slot1/tmm5 crit tmm5[21732]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Which configuration item should the LTM Specialist review to fix the issue?
A. Port Lockdown
B. Pool Member
C. SNAT Pool
D. Virtual Server Port Translation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
-- Exhibit -



dumpsdb.com

```
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...<?E@.@.....A.P..5.......9.....
.@.1.....
15:36:14.387168 IP 192.168.1.1.80 > 192.168.1.216.35137: S 2457418989:2457418989(0) ack 379008508 win 4380 <mss 1460,nop,wscale 3,sackOK,timestamp 2864934986 2322043441> in slot1/tmm0 lis=
E..<.I@.@..K.........P.A.y<...5.....
..pJ.@.1.....
15:36:14.387504 IP 192.168.1.216.35137 > 192.168.1.1.80: . ack 1 win 115 <nop,nop,timestamp 2322043443 2864934987> out slot1/tmm0 lis=
E..47g@.@..3.........A.P..5..y<....s.....
.@.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 2864934988> out slot1/tmm0 lis=
E..;7h@.@..+.........A.P..5..y<....s@i.....
.@.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 2864934989 2322043443> in slot1/tmm0 lis=
E....H@.@.............P.A.y<...6... .f.....
..pL.@.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=
.....H@.@..K.........P.A.yA...6... ..
..pM.@.3.....
15:36:14.390225 IP 192.168.1.216.35137 > 192.168.1.1.80: . ack 1216 win 137 <nop,nop,timestamp 2322043445 2864934989> out slot1/tmm0 lis=
E..47i@.@..1.........A.P..6..yA.....
.@.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.....
.@.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.@.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 pool member is responding with a 404.
B. The request is NOT being received by the pool member.
C. The pool member is responding without HTTP headers.
D. The HTTP headers are compressed.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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 is NOT accepting requests from the LTM device IP address.
B. The pool member has too many concurrent connections.
C. The pool member is rejecting the request because it is invalid.
D. The pool member lacks the object requested by the monitor.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
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. When the remote syslog sever fails, it returns to service before the timeout for the monitor has expired.
B. The -log option for tcpdump needs to be used.
C. The monitor type used is inappropriate.
D. The "verbose" logging option needs to be enabled for the pool.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
-- Exhibit -

-- 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 virtual test1_vs, delete pool test2_pool, delete node 10.1.1.1

B. delete pool test1_pool, delete node 10.1.1.2, delete node 10.1.1.1

C. delete pool test1_pool, delete pool test2_pool, delete node 10.1.1.3

D. delete node 10.1.1.2, delete pool test2_pool

E. delete pool test1_pool, delete node 10.1.1.2

Answer: E (LEAVE A REPLY)

NEW QUESTION: 56

Which file should be modified to create custom SNMP alerts?

A. /etc/alertd/alert.conf

B. /etc/alertd/user_alert.conf

C. /config/alert.conf

D. /config/user_alert.conf

Answer: D (LEAVE A REPLY)

NEW QUESTION: 57

-- Exhibit-

-- 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

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 58

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

NEW QUESTION: 59
An LTM Specialist needs to rewrite text within an HTML response from a web server. A client is sending the HTTP request below:
GET / HTTP/1.1
Host: www.f5.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-LanguagE. en-US,en;q=0.5 Accept-EncodinG. gzip, deflate Cache-Control: no-cache Connection: keep-alive CookiE. somecookie=1 Although a stream profile has been added to the virtual server, the content within the HTTP response is NOT being matched, and therefore NOT modified.
Which HTTP header should the LTM Specialist remove from the request to ensure the content can be matched and modified?
A. Cache-Control
B. Accept-Encoding
C. Accept
D. Connection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user's shopping cart is shown as empty.
The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.
How should the LTM Specialist resolve this issue?
A. Create a custom persistence profile and enable "Match Across Services."
B. Add an HTTP profile to both virtual servers.
C. Create a custom persistence profile and enable "Map Proxies."
D. Enable SNAT Automap on both virtual servers.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
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. Generate Initial Sequence Number
B. Loose Initiation
C. Loose Close
D. Reset on Timeout
Answer: B (LEAVE A REPLY)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 62
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. Trailer
B. Expect
C. ETag
D. From
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63

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 pool members of both pools need to be set up as case-insensitive members.

C. The 'switch' command in the iRule has been used incorrectly.

D. The "Process Case-Insensitivity" option for the virtual server needs to be selected.

Answer: (SHOW ANSWER)

NEW QUESTION: 64

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. unchanged until bigd is restarted

B. green or available

C. red or offline

D. blue or unchecked

Answer: A (LEAVE A REPLY)

NEW QUESTION: 65

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. lind
B. bcm56xxd
C. mcpd
D. promptstatusd
E. sod
Answer: (SHOW ANSWER)

NEW QUESTION: 66
An LTM Specialist needs to rewrite text within an HTML response from a web server. A client is sending the following HTTP request:
GET / HTTP/1.1 Host: www.example.com User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0 Accept: text/html,application/xhtml

+xml,application/xml;q=0.9,*/*;q=0.8 Accept-LanguagE.en-US,en;q=0.5 Accept-EncodinG.gzip, deflate Cache-Control: no-cache Connection: keep-alive CookiE.somecookie=1
HTTP/1.1 200 OK Server: Apache/2.2.15 (Unix) Last-ModifieD.Wed, 12 Aug 2009 00:00:30 GMT Accept-Ranges: bytes Content-LengtH.1063 X-Cnection: close Content-TypE.text/html; charset=UTF-8 Vary: Accept-Encoding Content-EncodinG.gzip Connection: Keep-Alive
Although a stream profile has been added to the virtual server, the content within the HTTP response is NOT being matched and therefore NOT modified.
Which header field is contributing to the issue?
A. HTTP Method
B. User-Agent Value
C. Accept-Encoding header
D. Cookie content
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
These log entries can have different root causes:
Jun 28 05:01:21 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: enabled
Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071431:5: Attempting to connect to CMI peer 1.1.1.2 port 6699
Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071432:5: CMI peer connection established to 1.1.1.2 port 6699
Jun 28 05:01:26 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: disabled, all peers are connected
Which two commands should be used to obtain additional information on these entries? (Choose two.)
A. tmsh show /sys mcpd
B. bigstart status mcpd
C. tmsh modify /sys db log.mcpd.level value debug
D. tmsh modify /sys db log.cmi.level value debug
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 68
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 list /sys baud-rate
C. tmsh show /sys console
D. tmsh list /net baud-rate
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69

An LTM device supports two power supplies. The value of the BigDB key "platform.powersupplymonitor" is equal to enable.
Where would the error message be visible if one of the power supplies fails or is NOT plugged in?
A. visible only via the console
B. in the /var/log/tmm log file
C. in the /var/log/kern.log file
D. in the /var/log/ltm log file
Answer: D (LEAVE A REPLY)

NEW 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
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 71
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. Scripted
B. FTP
C. External
D. Real Server
E. Inband
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
An LTM Specialist has just manually failed the active LTM device over to the standby LTM device. The LTM Specialist notices the newly active LTM device is NOT currently receiving traffic. The LTM Specialist verifies the newly active device is responding to ARP but still no traffic is hitting the virtual servers. The LTM Specialist also notices that the virtual servers eventually start responding.
What should be added to the configuration to resolve the problem?
A. MAC masquerading
B. vlan failsafe

C. floating self IP
D. network failover
E. connection mirroring
Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
An LTM Specialist configured a virtual server to load balance a custom application. The application works when it is tested from within the firewall but it fails when tested externally. The pool member address is
192.168.200.10:80. A capture from an external client shows:
GET /index.jsp HTTP/1.1
Host: 207.206.201.100
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:15.0) Gecko/20100101 Firefox/15.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Connection: keep-alive
HTTP/1.1 302 Found
DatE. Wed, 17 Oct 2012 23:09:55 GMT
Server: Apache/2.2.15 (CentOS)
Location: http://192.168.200.10/user/home.jsp
Content-LengtH. 304
Connection: close
What is the solution to this issue?
A. Configure a content filter on the backend web server.
B. Assign a SNAT pool to the virtual server.
C. Add a Web Acceleration Profile to the virtual server.
D. Configure redirect rewrite option in the HTTP profile.
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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. Accept-Ranges
B. Expect
C. Range
D. Content-Length
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
When re-licensing an LTM device from the command line interface, which tmsh command should the LTM Specialist use to generate the required information to provide on the F5 licensing portal?
A. tmsh install /sys license registration-key

B. tmsh generate /sys dossier
C. tmsh run /util get-dossier
D. tmsh list /sys registration-key
Answer: (SHOW ANSWER)

NEW QUESTION: 76
An IT administrator wants to log which server is being load balanced to by a user with IP address 10.10.10.25.
Which iRule should the LTM Specialist use to fulfill the request?
A. when SERVER_CONNECTED {
if { [IP::addr [IP::remote_addr]] equals 10.10.10.25]} {
log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }
}
B. when SERVER_CONNECTED {
if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25]} {
log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }
}
C. when CLIENT_ACCEPTED {
if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25]} {
log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }
}
D. when CLIENT_ACCEPTED {
if { [IP::addr [IP::remote_addr] equals 10.10.10.25]} {
log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }
}
Answer: B (LEAVE A REPLY)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 77
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. Scripted
B. External
C. Inband
D. FTP
E. Real Server
Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
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. green or available
B. blue or unchecked
C. unchanged until bigd is restarted
D. red or offline
Answer: (SHOW ANSWER)

NEW QUESTION: 79
-- Exhibit -

```
New TCP connection #3: 172.16.1.20(49379) <-> 172.16.20.1(443)
3 1  0.0006 (0.0006)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
3 2  0.0009 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          ed 15 16 5f c2 9d bf 5e e6 70 0e a4 86 59 bf 27
          e7 b5 fa 49 38 fd 24 d7 c3 1e c1 9f d2 67 e4 f7
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                     NULL
3 3  0.0009 (0.0000)  S>C  Handshake
      Certificate
3 4  0.0009 (0.0000)  S>C  Handshake
      ServerHelloDone
New TCP connection #4: 172.16.1.20(49380) <-> 172.16.20.1(443)
4 1  0.0004 (0.0004)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
4 2  0.0007 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          f5 eb fe e9 8e fc e9 7f c5 13 1b 40 69 15 08 72
          95 ef 43 e5 4e 10 f4 3b b2 3e 5c ec 5e ee 66 a8
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                     NULL
4 3  0.0007 (0.0000)  S>C  Handshake
      Certificate
4 4  0.0007 (0.0000)  S>C  Handshake
      ServerHelloDone
3    0.0015 (0.0006)  C>S  TCP RST
4    0.0010 (0.0003)  C>S  TCP RST
```

ITExamDump.com

```
[~]$ 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
SIb3DQEBAQUAA4GNADCBiQKBgQCV1genrRHsav6R+M/xYyooMJVpXWZbzeKu04ro
euadY0KOwwa2zF9jaD0HDIJ3MtnVYaHMsHZvqoo1Q8EfohP85RfHrO4kMxtvAefm
s1qGE7MkmIxLtwYjjWXmwxW7sCFL19kt6pFOatzqeK3WxbdM5yF/RTHF4R/vyKQI
2lYf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBRG5CDKtOlkiiix7sc2JjoVHajd2zBm
BgNVHSMEXzBdgBRG5CDKtOlkiiix7sc2JjoVHajd26E6pDgwNjEWMBQGA1UEChMN
VHVybktleSBMaW51eDEcMBoGA1UECxMTU29mdHdhcmUgYXBwbGlhbmNlczEW
XVLJqYzBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEA
n6KznFgueLGzn+qgyIz0ZVG5PF8RRzHPYDAIDRU0MERe
RGH2+IqwglEPB7K6eudRy0D9GqzMHZrdMo9d3ewPB3B
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 exhibits.

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

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

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

A. Enable ProxySSL option in the server SSL profile.

B. Change Secure Renegotiation to "Request."

C. Enable Strict Resume.

D. Change to different ciphers on the server SSL profile.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 80

-- Exhibit -

```
Direct to application server:
Request:
GET / HTTP/1.1
Host: 172.16.20.21
Connection: keep-alive
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

Response:
HTTP/1.1 200 OK
Date: Wed, 24 Oct 2012 19:11:46 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Fri, 08 Jun 2012 13:32:31 GMT
ETag: "a0b21-b1-4c1f608458836"
Accept-Ranges: bytes
Content-Length: 177
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Through LTM:
Request:
GET / 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

Response:
HTTP/1.1 301 Moved Permanently
Date: Wed, 24 Oct 2012 19:17:47 GMT
Server: Apache/2.2.22 (Ubuntu)
Location: https://www.example.com/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has created a virtual server to balance connections to a pool of application servers and offload SSL decryption. Clients connect to the application at https://www.example.com/. The virtual server is configured with a clientssl profile but no serverssl profile. The application servers are listening on ports
80 and 443. Users are unable to connect to the application through the virtual server but are able to connect directly to the application server.

What is the root cause of the error?

A. The LTM device is chunking responses.

B. The application servers are redirecting users to HTTPS.

C. The LTM device is redirecting users to HTTPS.

D. The pool members are configured with the wrong port.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 81

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 disk status

C. tmsh show /sys raid status

D. tmsh show /ltm raid disk

Answer: (SHOW ANSWER)

NEW QUESTION: 82

An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user's shopping cart is shown as empty. The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.

What is the issue?

A. The port 443 pool member is deleting the user's session cookie.

B. The port 80 pool member is deleting the user's session cookie.

C. The port 80 and port 443 connections are balanced to the same node.

D. The port 80 and port 443 connections are balanced to different nodes.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 83

-- Exhibit-

-- 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. Verify the default gateway on the application servers.

B. Verify that port lockdown is set to allow port 80.

C. Increase the TCP timeout value in the default TCP profile.

D. Enable SNAT automap on the virtual server.

E. Assign a custom HTTP monitor to the pool.

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 84

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 status

B. tmsh show /net interface

C. tmsh /net show interface

D. tmsh /net show interface status

Answer: B (LEAVE A REPLY)

NEW QUESTION: 85

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. tcpdump -i internal host 172.16.20.1 > /shared/ssl.pcap ssldump < /shared/ssl.pcap

B. ssldump -i internal host 172.16.20.1

C. curl -d - -k https://172.16.20.1

D. tcpdump -s 64 -i internal -w /shared/ssl.pcap host 172.16.20.1 ssldump -r /shared/ssl.pcap

Answer: B (LEAVE A REPLY)

NEW QUESTION: 86

-- Exhibit -

-- Exhibit -Refer to the exhibit.

An LTM Specialist is troubleshooting a new HTTP monitor on a pool. The pool member is functioning correctly when accessed directly through a browser. However, the monitor is marking the member as down. The LTM Specialist captures the monitor traffic via tcpdump.

What is the issue?

A. The 'time-until-up' setting on the monitor is incorrect.

B. The server is marking the connection as closed.

C. The pool member is rejecting the monitor request.

D. The monitor request is NOT returning the page body.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 87

-- Exhibit-

dumpsdb.com

-- Exhibit -

Refer to the exhibit.

An LTM Specialist is performing an HTTP trace on the client side of the LTM device and notices there are many undesired headers being sent by the server in the response. The LTM Specialist wants to remove all response headers except "Set-Cookie" and "Location."

How should the LTM Specialist modify the HTTP profile to remove undesired headers from the HTTP response?

A. Enter the desired header names in the 'Response Headers Allowed' field.

B. Enter the undesired header names in the 'Response Header Erase' field.

C. Enter the desired header names in the 'Request Header Insert' field.

D. Enter the undesired header names in the 'Request Header Erase' field.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 88

An LTM device is running BIG-IP v10.2.0 software. The LTM Specialist is tasked with upgrading the LTM device to BIG-IP v11.2.0 HF1. The LTM Specialist starts the upgrade process by selecting the uploaded Hotfix and installing to an unused volume. After 10 minutes, the LTM Specialist checks the status of the upgrade process and notices that the process is stalled at 0%.

What should the LTM Specialist verify?

A. the LTM device has an available Internet connection via the management interface

B. the base software version exists on the LTM device

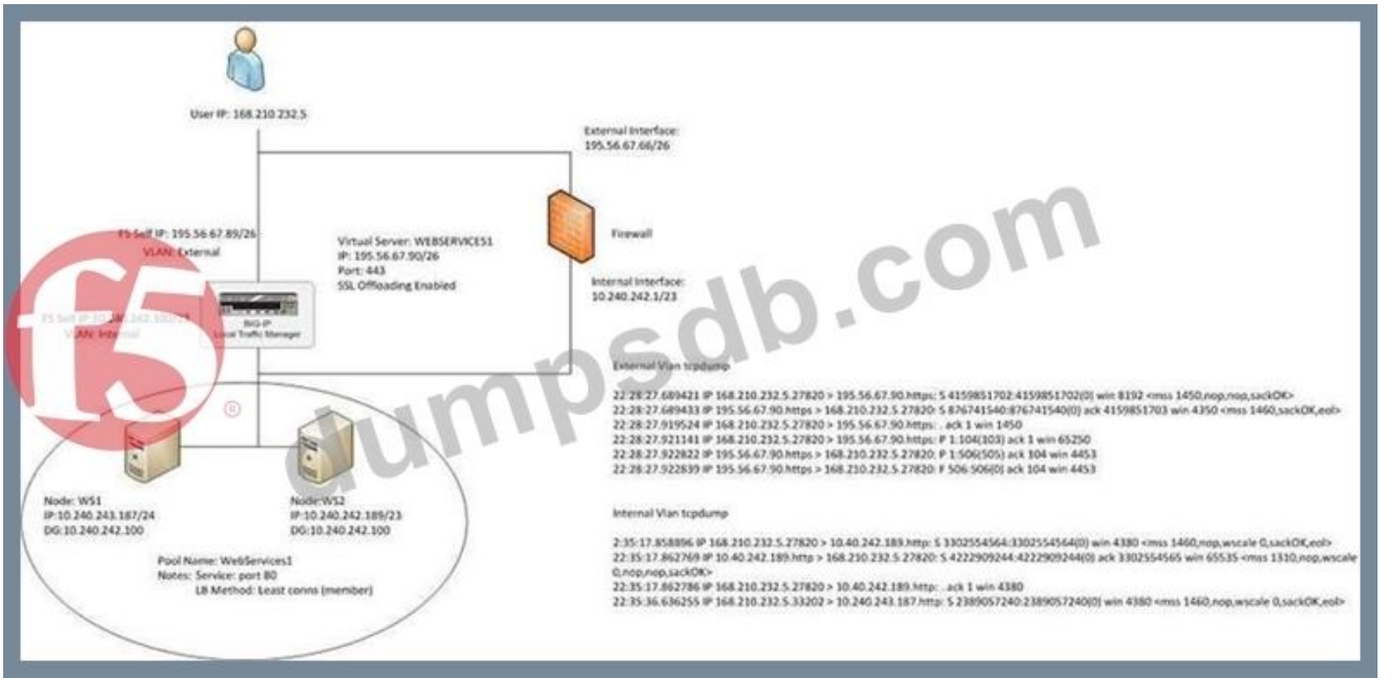
C. the LTM device has been restarted into maintenance mode

D. the selected volume has sufficient space available

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89

-- 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 pool members have been set up as an active/standby pair, with WS1 as the standby.

B. The firewall is dropping the packets from WS1.

C. The load balancing (LB) method is inappropriate.

D. The default gateway is inaccessible from WS1.

Answer: (SHOW ANSWER)

NEW QUESTION: 90

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. Create a universal persistence profile on the cartID cookie.
B. Enable source address persistence as a fallback persistence method.
C. Use an iRule to rewrite the cartID cookie domain.
D. Create a cookie persistence profile with "match across services" enabled.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 91
An LTM Specialist must perform a hot fix installation from the command line.
What is the correct procedure to ensure that the installation is successful?
A. import the hot fix to the /shared/images directory
check the integrity of the file with an md5 checksum
tmsh install sys software hotfix <hotfix_name>.iso volume <volume_name>
B. import the hot fix to the /var/shared/images directory
check the integrity of the file with an md5 checksum
tmsh install sys software hotfix <hotfix_name>.iso volume <volume_name>
C. import the hot fix to the /shared/images directory
check the integrity of the file with an md5 checksum
tmsh apply sys software hotfix volume <volume_name> <hotfix_name>.iso
D. import the hot fix to the /var/shared/images directory
check the integrity of the file with an md5 checksum
tmsh apply sys software hotfix volume <volume_name> <hotfix_name>.iso
Answer: (SHOW ANSWER)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest**

TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 92

-- 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
```

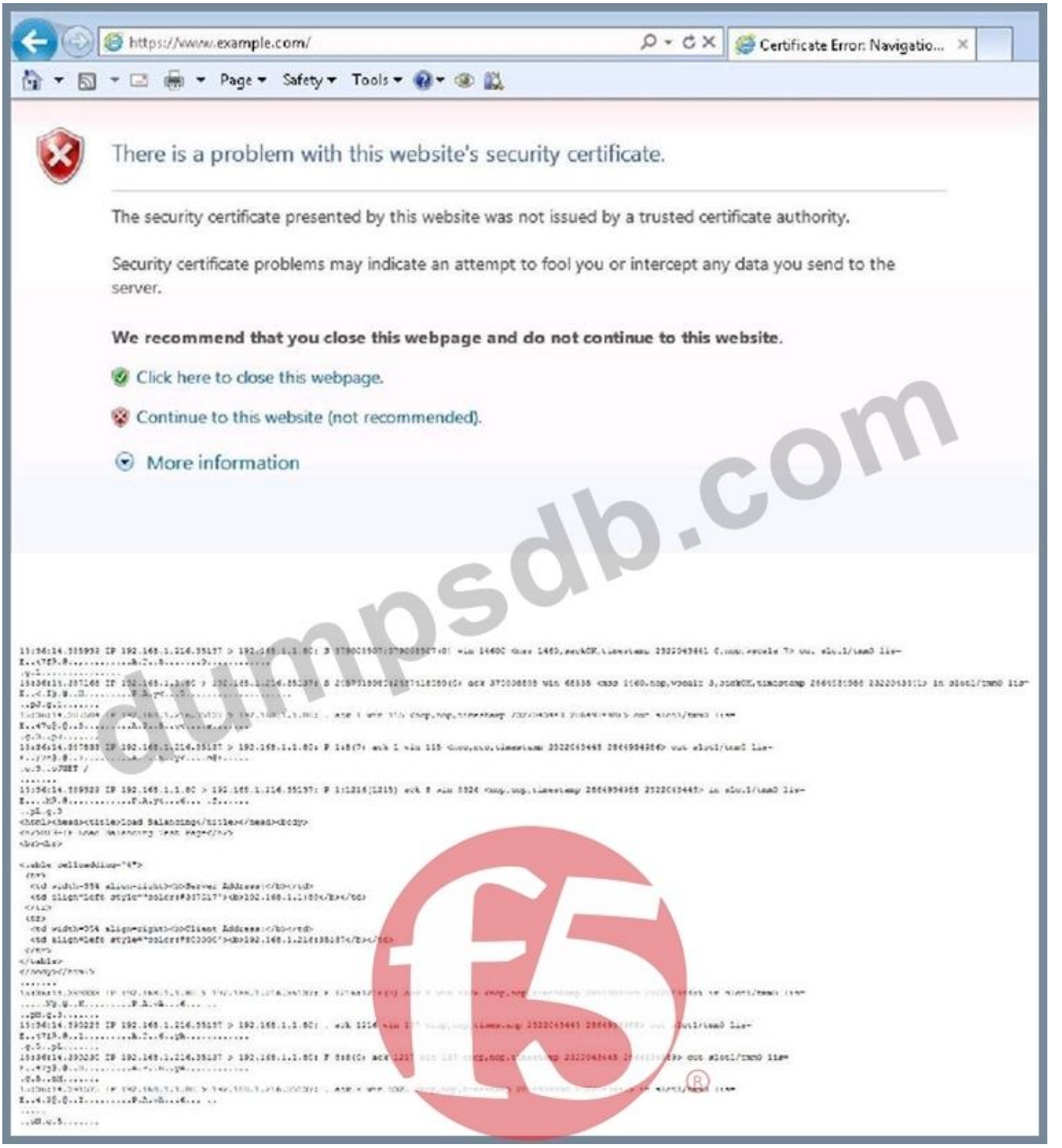
-- Exhibit --

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 LTM device CANNOT SSL offload the traffic in order to read and compress it.
B. The incorrect compression algorithm is applied to the compression profile.
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.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
-- Exhibit-



-- 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 request is NOT being received by the pool member.

B. The pool member is responding without HTTP headers.

C. The HTTP headers are compressed.

D. The pool member is responding with a 404.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 94

-- Exhibit-

```
Direct to application server:
Request:
GET / HTTP/1.1
Host: 172.16.20.21
Connection: keep-alive
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

Response:
HTTP/1.1 200 OK
Date: Wed, 24 Oct 2012 19:11:46 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Fri, 08 Jun 2012 13:32:31 GMT
ETag: "a0b21-b1-4c1f608458836"
Accept-Ranges: bytes
Content-Length: 177
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Through LTM:
Request:
GET / 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

Response:
HTTP/1.1 301 Moved Permanently
Date: Wed, 24 Oct 2012 19:17:47 GMT
Server: Apache/2.2.22 (Ubuntu)
Location: https://www.example.com/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
```

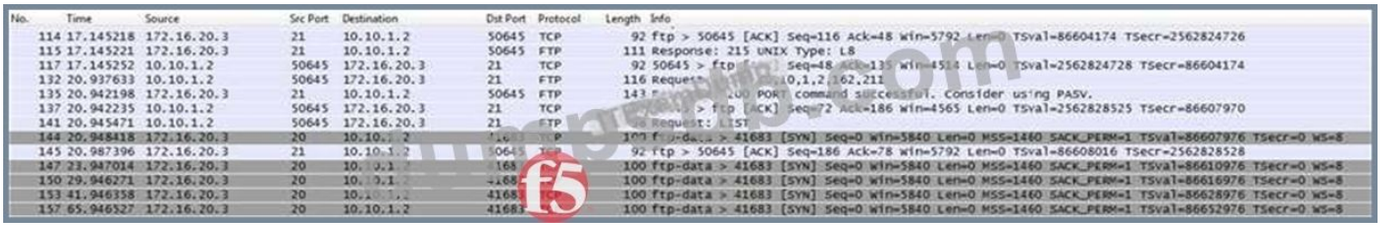
-- Exhibit -Refer to the exhibit. An LTM Specialist has created a virtual server to balance connections to a pool of
application servers and offload SSL decryption. Clients connect to the application at https://www.example.com/. The virtual server is configured with a clientssl profile but no serverssl profile. The application servers are listening on ports 80 and 443. Users are unable to connect to the application through the virtual server but are able to connect directly to the application server. What is the root cause of the error?

A. The LTM device is chunking responses.
B. The pool members are configured with the wrong port.
C. The LTM device is redirecting users to HTTPS.
D. The application servers are redirecting users to HTTPS.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
-- 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 load balancing (LB) method is inappropriate.
B. The pool members have been set up as an active/standby pair, with WS1 as the standby.
C. The firewall is dropping the packets from WS1.
D. The default gateway is inaccessible from WS1.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
-- 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 10,1,2,162,211
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. command connection failing

C. LIST command disallowed

D. PORT command disallowed

Answer: A (LEAVE A REPLY)

NEW QUESTION: 97

-- 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 virtual server is processing encrypted traffic as plain-text HTTP.

B. The pool member is failing the monitor check.

C. The pool member default gateway is set incorrectly.

D. The virtual server is configured with the incorrect SNAT address.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
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 server has an incorrect date configured.
B. The username and password are incorrect.
C. The client is using the wrong type of browser.
D. The wrong authentication mechanism is being used.
Answer: (SHOW ANSWER)

NEW QUESTION: 99
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
Answer: A,B (LEAVE A REPLY)
Explanation

NEW QUESTION: 100

-- Exhibit -

```
New TCP connection #3: 172.16.1.20(49379) <-> 172.16.20.1(443)
3 1  0.0006 (0.0006)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
3 2  0.0009 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          ed 15 16 5f c2 9d bf 5e e6 70 0e a4 86 59 bf 27
          e7 b5 fa 49 38 fd 24 d7 c3 1e c1 9f d2 67 e4 f7
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
3 3  0.0009 (0.0000)  S>C  Handshake
      Certificate
3 4  0.0009 (0.0000)  S>C  Handshake
      ServerHelloDone
New TCP connection #4: 172.16.1.20(49380) <-> 172.16.20.1(443)
4 1  0.0004 (0.0004)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
4 2  0.0007 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          f5 eb fe e9 8e fc e9 7f c5 13 1b 40 69 15 08 72
          95 ef 43 e5 4e 10 f4 3b b2 3e 5c ec 5e ee 66 a8
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
```

dumpsdb.com

```
          compressionMethod
4 3  0.0007 (0.0000)   S>C   Handshake
      Certificate
4 4  0.0007 (0.0000)   S>C   Handshake
      ServerHelloDone
3    0.0015 (0.0006)   C>S   TCP RST
4    0.0010 (0.0003)   C>S   TCP RST
```

-- Exhibit -

Refer to the exhibit.

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

Where is the reset originating?

A. the device initiating the connection

B. the application server

C. the destination device of the initial connection

D. the local switch

Answer: A (LEAVE A REPLY)

NEW QUESTION: 101

-- Exhibit -

```
ltm pool /Common/my_admin_pool {
    members {
        /Common/10.0.0.1:80 {
            address 10.0.0.1
        }
        /Common/10.0.0.2:80 {
            address 10.0.0.2
        }
    }
}
ltm pool /Common/my_default_pool {
    members {
        /Common/10.0.0.4:80 {
            address 10.0.0.4
        }
        /Common/10.0.0.5:80 {
            address 10.0.0.5
        }
    }
}

ltm virtual /Common/my_virtual_server {
```

```
    destination /Common/10.0.0.1:80
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/my_default_pool
    profiles {
        /Common/http { }
        /Common/tcp { }
    }
    rules {
        /Common/my_iRule
    }
    snat automap
}
sys ha-group my_ha_group {
    active-bonus 10
    pools {
        /Common/my_default_pool {
            threshold 2
            weight 20
        }
    }
    trunks {
        my_trunk {
            threshold 1
            weight 20
        }
    }
```

-- Exhibit -

Refer to the exhibit.

A pair of LTM devices is configured for HA.

What happens if the pool member server with IP address 10.0.0.4 becomes totally unresponsive to the active LTM device, but is still responsive to the standby LTM device?

A. The HA-group will initiate a fail-over because the HA-Group score will be zero.

B. The HA-group will disable the trunk my_trunk.

C. The HTTP application will be unavailable via the LTM device.

D. The HA-group will initiate a fail-over because the threshold is set to 2.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 102

-- Exhibit -

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting a sync-failover group of three BIG-IP LTM devices. The command used is "tmsh run cm watch-devicegroup-device."

What does the output mean?

A. Configuration is synchronized between all the devices.

B. Configuration is not synchronized. Some modifications have been done on bigipA.

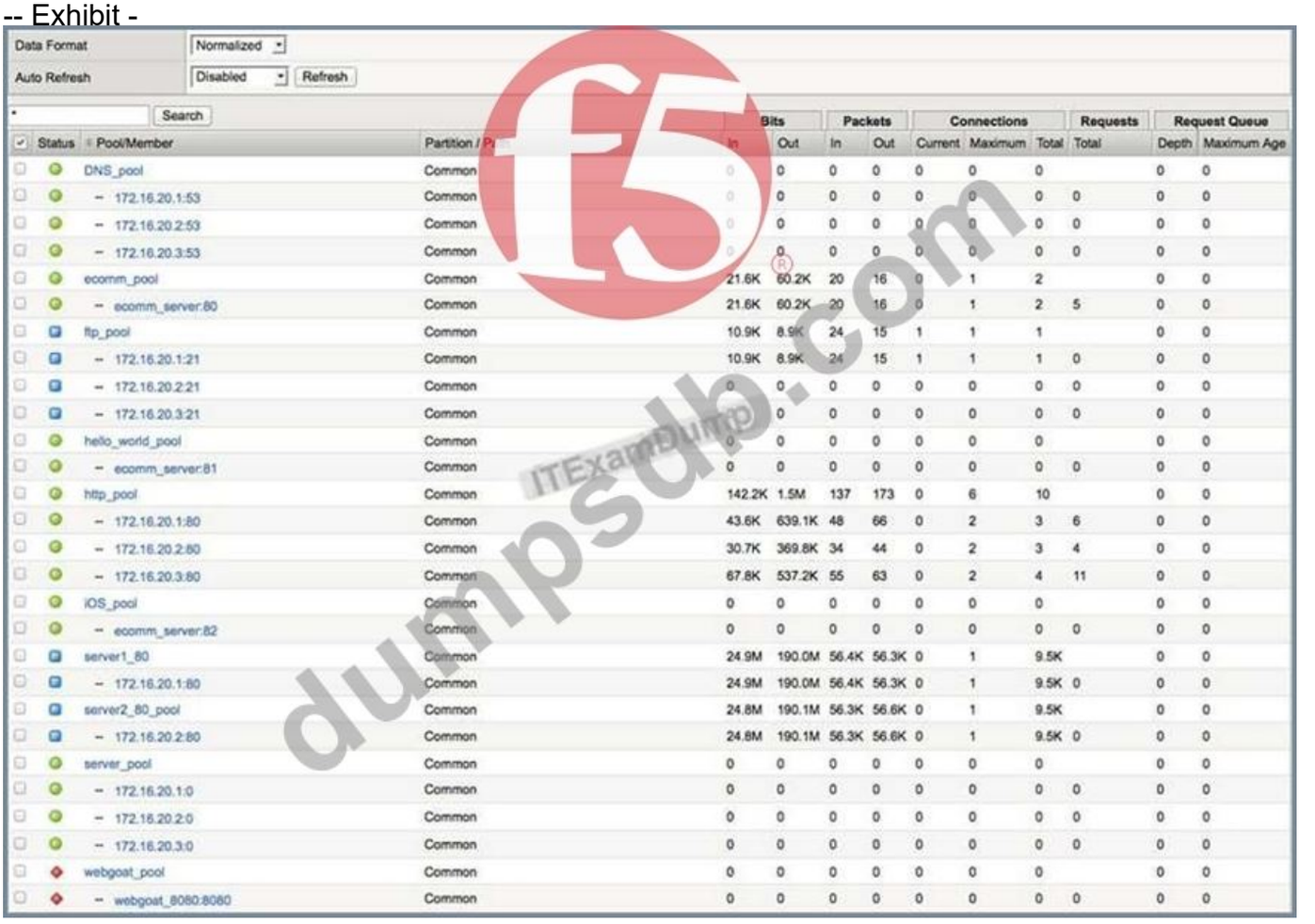
C. Configuration is not synchronized. Some modifications have been done on bigipC.

D. Configuration is not synchronized. Some modifications have been done on bigipB.

Answer: (SHOW ANSWER)

NEW QUESTION: 103

-- Exhibit -



-- Exhibit -

Refer to the exhibit.

Which pool can be removed without affecting client traffic?

A. server1_80

B. ftp_pool
C. http_pool
D. server_pool
Answer: (SHOW ANSWER)

NEW QUESTION: 104
-- Exhibit -

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

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

dumpsdb.com

-- Exhibit -Refer to the exhibits.
Every monitor has the same Send String, Recv String, and an Alias of *:*. The LTM Specialist simplifies the configuration to minimize the number of monitors.
How many unique monitors remain?
A. 1
B. 5
C. 2
D. 4
E. 3
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
-- Exhibit -

```
Oct 25 09:24:04 bigip1 notice syslog-ng[2983]: syslog-ng starting up; version=\'2.0.8\'
Oct 25 09:24:36 bigip1 notice audispd: audispd initialized with q_depth=80 and 1 active plugins
Oct 25 09:24:38 bigip1 notice syslog-ng[2983]: Configuration reload request received, reloading configuration;
Oct 25 09:25:55 bigip1 notice syslog-ng[2983]: Configuration reload request received, reloading configuration;
Oct 25 09:35:44 bigip1 notice shutdown[8888]: Thu Oct 25 09:35:44 2012 : shutting down for system reboot on behalf of root
2012-10-25T09:37:17-07:00 bigip1 notice boot_marker : ---===[ HD1.4 - BIG-IP 11.2.0 Build 2557.0 ]===---
Oct 25 09:37:19 bigip1 notice syslog-ng[2970]: syslog-ng starting up; version=\'2.0.8\'
Oct 25 09:37:51 bigip1 notice audispd: audispd initialized with q_depth=80 and 1 active plugins
Oct 25 09:37:53 bigip1 notice syslog-ng[2970]: Configuration reload request received, reloading configuration;
Oct 25 09:39:02 bigip1 notice syslog-ng[2970]: Configuration reload request received, reloading configuration;
```

```
Oct 25 09:29:05 tmm1 err tmm1[7355]: 01010028:3: No members available for pool /Common/http_pool
Oct 25 09:29:05 tmm1 err tmm1[7355]: 01010028:3: No members available for pool /Common/https_pool
Oct 25 09:29:05 tmm1 err tmm1[7355]: 01010028:3: No members available for pool /Common/ssh_pool
Oct 25 09:35:44 bigip1 notice overdog[4791]: 01140104:5: Watchdog touch disabled.
Oct 25 09:35:44 bigip1 info overdog[4791]: 01140101:6: Overdog daemon shutdown.
Oct 25 09:35:44 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id %promptstatusd
Oct 25 09:35:44 bigip1 info promptstatusd[4790]: 01460007:6: Resuming log processing at this invocation; held 1 messages.
Oct 25 09:35:45 bigip1 notice logger: /bin/bash /etc/rc6.d/K03bigstart stop  ==> /usr/bin/bigstart stop
Oct 25 09:35:46 bigip1 notice alertd[5636]: 01100043:5: logcheck Notice: Disconnect mcpd 0
Oct 25 09:35:46 bigip1 warning alertd[5636]: 01100002:4: alertd is going down.
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id csyncd
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id cluster_file_operations
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id BIGD_subscriber
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id eventd
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id %LACPD
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id lind
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id %istatsd
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id logstatsd
Oct 25 09:35:48 bigip1 info mcpd[5206]: 01070410:6: Per-invocation log rate exceeded; throttling.
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id cbrd
Oct 25 09:35:48 bigip1 notice scriptd[5641]: 014f0002:5: exiting
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id shell_publish
Oct 25 09:35:48 bigip1 info mcpd[5206]: 01070406:6: Per-invocation log rate exceeded; throttling.
Oct 25 09:35:48 bigip1 err mcpd[5206]: 01070069:3: Subscription not found in mcpd for subscriber Id stpd4860-0.
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id stpd4860-0
Oct 25 09:35:48 bigip1 notice sod[5970]: 010e0050:5: Sod requests links down.
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id ha_table_publish
Oct 25 09:35:48 tmm crit tmm[7354]: 01010019:2: Caught signal 15, exiting
Oct 25 09:35:48 tmm1 crit tmm1[7355]: 01010019:2: Caught signal 15, exiting
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Received signal: SIGTERM (15)
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: 4.1 rx[OK 582 Bad 0] tx[OK 594 Bad 0]
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good rx at: 1351182947.482888
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good tx at: 1351182947.050705
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last 64 rx hist: 0x0000000000000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last 64 tx hist: 0x0000000000000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last four bad rx at: 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: :                    0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last four bad tx at: 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: :                    0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: 4.2 rx[OK 582 Bad 0] tx[OK 595 Bad 0]
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good rx at: 1351182947.482885
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good tx at: 1351182947.050816
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last 64 rx hist: 0x0000000000000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last 64 tx hist: 0x0000000000000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last four bad rx at: 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: :                    0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last four bad tx at: 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: :                    0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0014:6: Exiting...
Oct 25 09:35:48 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus datastor
Oct 25 09:35:48 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus dedup_admin
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus tmrouted
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus dpid
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus wamd
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus websso
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart restart apd
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus acctd
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus eam
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus rba
Oct 25 09:35:49 bigip1 notice logger: /bin/sh ./finish 1 0  ==> /usr/bin/bigstart singlestatus logd
Oct 25 09:35:51 bigip1 info mcpd[5206]: 01070410:6: Resuming log processing at this invocation; held 6 messages.
Oct 25 09:35:51 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id named
Oct 25 09:35:53 bigip1 info mcpd[5206]: 01070406:6: Resuming log processing at this invocation; held 5 messages.
Oct 25 09:35:53 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id BCM56xxPublisher
Oct 25 09:35:55 bigip1 notice mcpd[5206]: 01070007:5: Received shutdown signal 15.
Oct 25 09:35:55 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id chmand_publisher
Oct 25 09:35:55 bigip1 info mcpd[5206]: 01070356:6: Resuming log processing at this invocation; held 3 messages.
Oct 25 09:35:58 bigip1 notice chmand[5451]: 012a0005:5: Stop chmand
2012-10-25T09:37:17-07:00 bigip1 notice boot_marker : ---===[ HD1.4 - BIG-IP 11.2.0 Build 2557.0 ]===---
Oct 25 09:37:22 bigip1 info mprov:3037:: Invoked as: /usr/bin/mprov.pl (pid=3037) --logicaldisk --boot --quiet
Oct 25 09:37:22 bigip1 info mprov:3037:: Checking for and completing any disk management transactions:
Oct 25 09:37:23 bigip1 info mprov:3044:: Invoked as: /usr/bin/mprov.pl (pid=3044) --diskmgmt --boot --quiet
```

-- Exhibit -

Refer to the exhibits.

An LTM Specialist uses the information in the logs to determine the cause of a failover event in a high-availability (HA) pair.

What caused the failover?

A. The system was administratively rebooted.

B. The configuration reload request caused the config to reload and the device to failover.

C. The process bcm56xxd received SIGTERM from the watchdog process.
D. The overdog process crashed.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
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. an Auditor role that has access to the GUI
B. the standby LTM that lost connectivity on the failover VLAN
C. the standby LTM that was rebooted
D. a VLAN fail-safe setting
E. a monitor on a pool in an HA group
Answer: D,E (LEAVE A REPLY)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 107
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
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 108
Windows PC clients are connecting to a virtual server over a high-speed, low-latency network with no packet loss.
Which built-in client-side TCP profile provides the highest throughput for HTTP downloads?
A. tcp
B. tcp-legacy
C. tcp-wan-optimized

D. tcp-lan-optimized

Answer: D (LEAVE A REPLY)

NEW QUESTION: 109

A device on the network is configured with the same IP address as the management address of the active LTM device, causing the management GUI to be inaccessible.

Which two methods should the LTM Specialist use to access the LTM device in order to change the management IP address? (Choose two.)

A. Connect to the LTM device via serial connection.

B. Connect via ssh to the management address.

C. Connect a monitor and keyboard to the LTM device.

D. Connect via ssh to the standby unit and connect via ssh across the serial link between the devices.

E. Connect via ssh to the AOM IP address.

Answer: (SHOW ANSWER)

NEW QUESTION: 110

-- Exhibit -

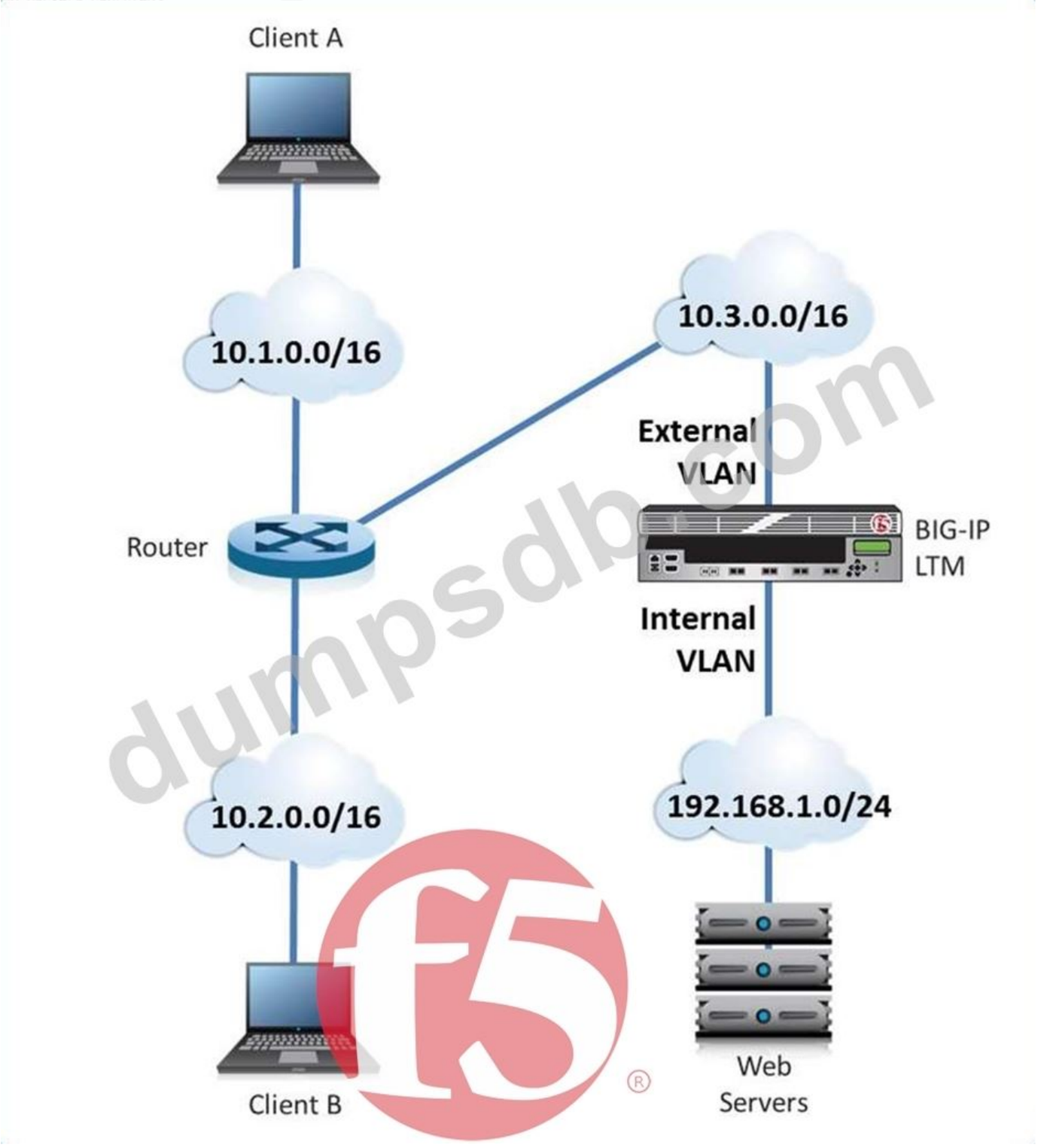
```
CTERNAL VLAN
5:01:29.356966 IP 10.1.5.100.49885 > 10.3.20.20.80: S 2686165014:2686165014(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
5:01:29.357743 IP 10.3.20.20.80 > 10.1.5.100.49885: S 1853772182:1853772182(0) ack 2686165015 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
5:01:29.359987 IP 10.1.5.100.49885 > 10.3.20.20.80: . ack 1 win 16425
5:01:29.361309 IP 10.1.5.100.49885 > 10.3.20.20.80: P 1:339(338) ack 1 win 16425
5:01:29.361327 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 339 win 4718
5:01:29.367040 IP 10.3.20.20.80 > 10.1.5.100.49885: P 1:342(341) ack 339 win 4718
5:01:29.523013 IP 10.1.5.100.49885 > 10.3.20.20.80: P 339:658(319) ack 342 win 16339
5:01:29.523067 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 658 win 5037
5:01:29.526066 IP 10.3.20.20.80 > 10.1.5.100.49885: P 342:1747(1405) ack 658 win 5037
5:01:29.544197 IP 10.1.5.100.49886 > 10.3.20.20.80: S 2661471084:2661471084(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
5:01:29.544330 IP 10.3.20.20.80 > 10.1.5.100.49886: S 4091779980:4091779980(0) ack 2661471085 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
5:01:29.544319 IP 10.1.5.100.49885 > 10.3.20.20.80: P 658:1007(349) ack 1747 win 16425
5:01:29.544329 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 1007 win 5386
5:01:29.547133 IP 10.1.5.100.49886 > 10.3.20.20.80: . ack 1 win 16425
5:01:29.547026 IP 10.3.20.20.80 > 10.1.5.100.49885: P 1747:3152(1405) ack 1007 win 5386
5:01:29.575235 IP 10.1.5.100.49885 > 10.3.20.20.80: P 1007:1356(349) ack 3152 win 16073
5:01:29.575262 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 1356 win 5735
5:01:29.576974 IP 10.3.20.20.80 > 10.1.5.100.49885: P 3152:4557(1405) ack 1356 win 5735
5:01:29.797914 IP 10.1.5.100.49885 > 10.3.20.20.80: . ack 4557 win 16425


CTERNAL VLAN
5:01:29.360061 IP 192.168.1.5.49885 > 192.168.1.100.80: S 895389186:895389186(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
5:01:29.364886 IP 192.168.1.100.80 > 192.168.1.5.49885: S 1666047010:1666047010(0) ack 895389187 win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
5:01:29.365020 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 1 win 4380
5:01:29.365031 IP 192.168.1.5.49885 > 192.168.1.100.80: P 1:339(338) ack 1 win 4380
5:01:29.366981 IP 192.168.1.100.80 > 192.168.1.5.49885: P 1:342(341) ack 339 win 256
5:01:29.367073 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 342 win 4721
5:01:29.523051 IP 192.168.1.5.49885 > 192.168.1.100.80: P 339:658(319) ack 342 win 4721
5:01:29.526009 IP 192.168.1.100.80 > 192.168.1.5.49885: P 342:1747(1405) ack 658 win 255
5:01:29.526074 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 1747 win 6126
5:01:29.544329 IP 192.168.1.5.49885 > 192.168.1.100.80: P 658:1007(349) ack 1747 win 6126
5:01:29.547230 IP 192.168.1.5.49886 > 192.168.1.100.80: S 1454462415:1454462415(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
5:01:29.546991 IP 192.168.1.100.80 > 192.168.1.5.49885: P 1747:3152(1405) ack 1007 win 254
5:01:29.547056 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 3152 win 7531
5:01:29.549134 IP 192.168.1.100.80 > 192.168.1.5.49886: S 786849220:786849220(0) ack 1454462416 win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
5:01:29.549159 IP 192.168.1.5.49886 > 192.168.1.100.80: . ack 1 win 4380
5:01:29.575259 IP 192.168.1.5.49885 > 192.168.1.100.80: P 1007:1356(349) ack 3152 win 7531
5:01:29.576958 IP 192.168.1.100.80 > 192.168.1.5.49885: P 3152:4557(1405) ack 1356 win 252
5:01:29.576978 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 4557 win 8936
5:01:34.564453 IP 192.168.1.5.49886 > 192.168.1.100.80: F 1:1(0) ack 1 win 4380
```

lumpsdb.com

```
XTERNAL VLAN
6:02:26.047441 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
6:02:26.285979 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
6:02:29.048674 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
6:02:29.283160 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
6:02:35.065086 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,nop,sackOK>
6:02:35.298372 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,nop,sackOK>

NTERNAL VLAN
```



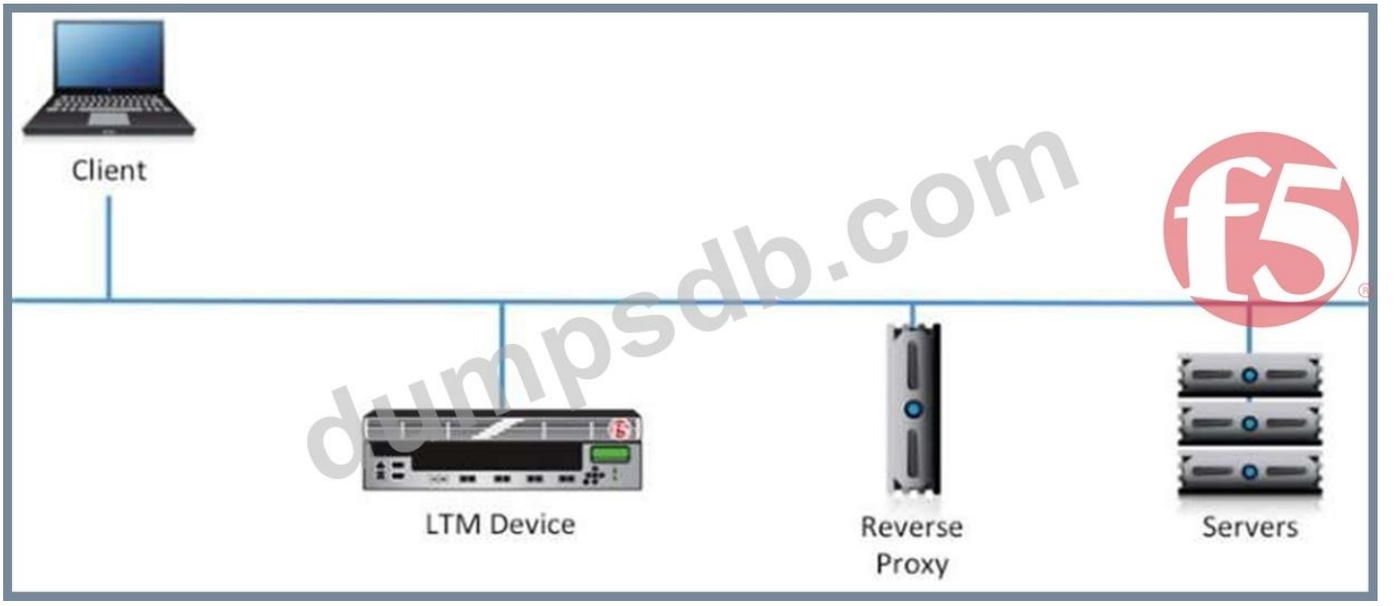
-- Exhibit --

Refer to the exhibits.

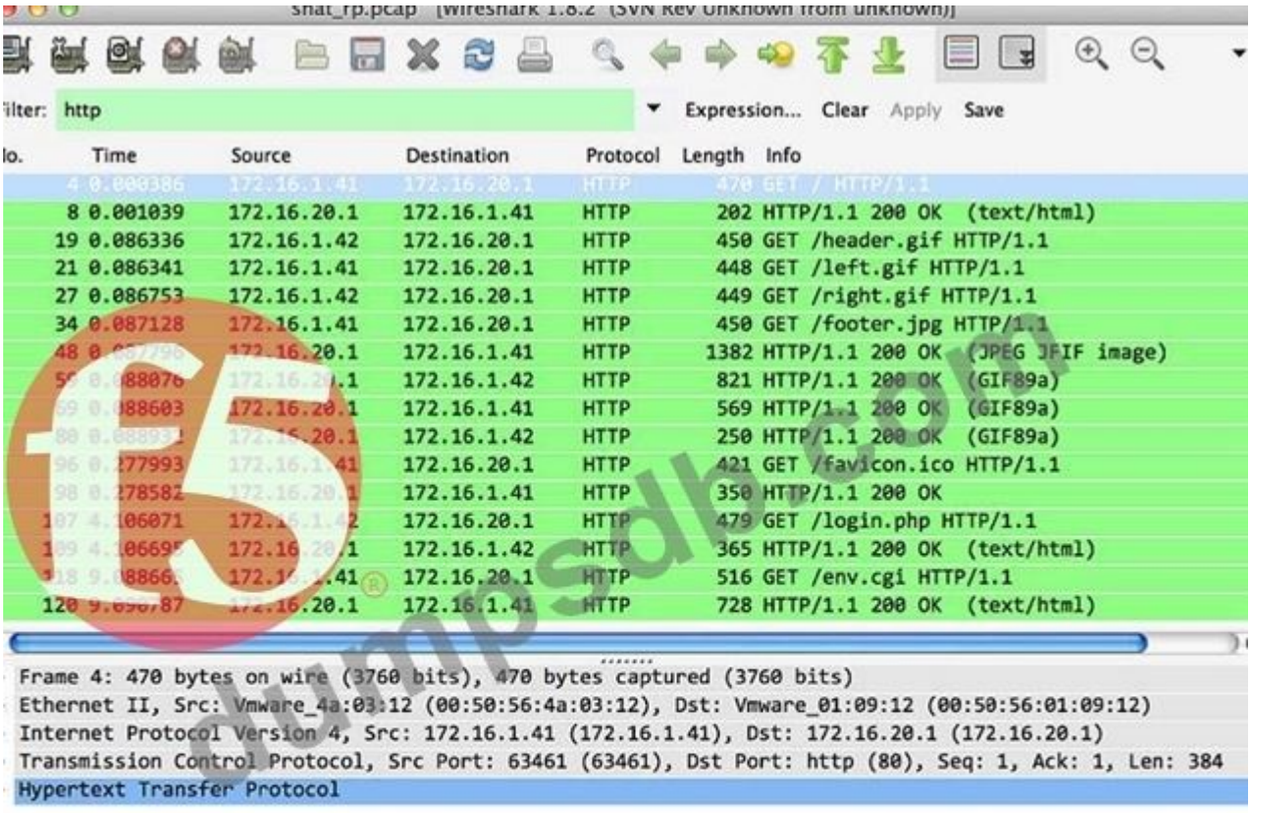
Users are able to access the application when connecting to the virtual server but are

unsuccessful when connecting directly to the application servers. The LTM Specialist wants to allow direct access to the application servers.
Which configuration change resolves this problem?
A. Enable port 443 on the virtual server.
B. Configure a SNAT pool on the LTM device.
C. Disable address translation on the virtual server.
D. Configure an IP Forwarding virtual server on the LTM device.
E. Configure a route to the web server subnet on the network router.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 111
-- Exhibit -



dumpsdb.com



-- Exhibit --

Refer to the exhibits.

A virtual server has been configured for SSL offload on a single-arm network. On average, the virtual server will be handling 100,000 connections, with a peak of 130,000 connections. Between the virtual server and the web servers there is a single reverse proxy to provide site caching. The proxy is configured to perform source IP persistence before contacting the web servers. The site is logging users out immediately after logging them in.

What should the LTM Specialist do to resolve this issue?

A. Change the virtual server server-side TCP profile to tcp-lan-optimized.

B. Add a source address persistence profile to the virtual server.

C. Configure the virtual server HTTP profile to insert an X-Forwarded-For header.

D. Create an iRule to add client IP persistence to a SNAT pool member.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 112

-- Exhibit-

PACKET CAPTURE AT LTM DEVICE – CONNECTING TO VIRTUAL SERVER

EXTERNAL VLAN

```
16:01:29.356966 IP 10.1.5.100.49885 > 10.3.20.20.80: S 2686165014:2686165014(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:01:29.357743 IP 10.3.20.20.80 > 10.1.5.100.49885: S 1853772182:1853772182(0) ack 2686165015 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:01:29.359987 IP 10.1.5.100.49885 > 10.3.20.20.80: . ack 1 win 16425
16:01:29.361809 IP 10.1.5.100.49885 > 10.3.20.20.80: P 1:339(338) ack 1 win 16425
16:01:29.361327 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 339 win 4718
16:01:29.367040 IP 10.3.20.20.80 > 10.1.5.100.49885: P 1:342(341) ack 339 win 4718
16:01:29.523013 IP 10.1.5.100.49885 > 10.3.20.20.80: P 339:658(319) ack 342 win 16339
16:01:29.523067 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 658 win 5037
16:01:29.526066 IP 10.3.20.20.80 > 10.1.5.100.49885: P 342:1747(1405) ack 658 win 5037
16:01:29.544197 IP 10.1.5.100.49886 > 10.3.20.20.80: S 2661471084:2661471084(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:01:29.544330 IP 10.3.20.20.80 > 10.1.5.100.49886: S 4091779980:4091779980(0) ack 2661471085 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:01:29.544319 IP 10.1.5.100.49885 > 10.3.20.20.80: P 658:1007(349) ack 1747 win 16425
16:01:29.544329 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 1007 win 5386
16:01:29.547133 IP 10.1.5.100.49886 > 10.3.20.20.80: . ack 1 win 16425
16:01:29.547026 IP 10.3.20.20.80 > 10.1.5.100.49885: P 1747:3152(1405) ack 1007 win 5386
16:01:29.575235 IP 10.1.5.100.49885 > 10.3.20.20.80: P 1007:1356(349) ack 3152 win 16073
16:01:29.575262 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 1356 win 5735
16:01:29.576979 IP 10.3.20.20.80 > 10.1.5.100.49885: P 3152:4557(1405) ack 1356 win 5735
16:01:29.797[illegible] IP 10.1.5.100.49885 > 10.3.20.20.80: . ack 4557 win 16425
```

INTERNAL VLAN

```
16:01:29.360001 IP 192.[illegible].1.5.49885 > 192.168.1.100.80: S 895389186:895389186(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:01:29.360856 IP 192.168.1.100.80 > 192.168.1.5.49885: S 1666047010:1666047010(0) ack 895389187 win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
16:01:29.365001 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 1 win 4380
16:01:29.365001 IP 192.168.1.5.49885 > 192.168.1.100.80: P 1:339(338) ack 1 win 4380
16:01:29.366901 IP 192.168.1.100.80 > 192.168.1.5.49885: P 1:342(341) ack 339 win 256
16:01:29.367073 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 342 win 4721
16:01:29.523001 IP 192.168.1.5.49885 > 192.168.1.100.80: P 339:658(319) ack 342 win 4721
16:01:29.526009 IP 192.168.1.100.80 > 192.168.1.5.49885: P 342:1747(1405) ack 658 win 255
16:01:29.526074 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 1747 win 6126
16:01:29.544309 IP 192.168.1.5.49886 > 192.168.1.100.80: P 658:1007(349) ack 1747 win 6126
16:01:29.547259 IP 192.168.1.100.80 > 192.168.1.100.80: S 1454462415:1454462415(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:01:29.546991 IP 192.168.1.100.80 > 192.168.1.5.49885: P 1747:3152(1405) ack 1007 win 254
16:01:29.547056 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 3152 win 7531
16:01:29.549134 IP 192.168.1.100.80 > 192.168.1.5.49886: S 786849220:786849220(0) ack 1454462416 win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
16:01:29.549159 IP 192.168.1.5.49886 > 192.168.1.100.80: . ack 1 win 4380
16:01:29.575259 IP 192.168.1.5.49885 > 192.168.1.100.80: P 1007:1356(349) ack 3152 win 7531
16:01:29.576956 IP 192.168.1.100.80 > 192.168.1.5.49885: P 3152:4557(1405) ack 1356 win 252
16:01:29.576978 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 4557 win 8936
16:01:34.564453 IP 192.168.1.5.49886 > 192.168.1.100.80: F 1:1(0) ack 1 win 4380
16:01:34.567472 IP 192.168.1.100.80 > 192.168.1.5.49886: R 1:1(0) ack 2 win 0
```

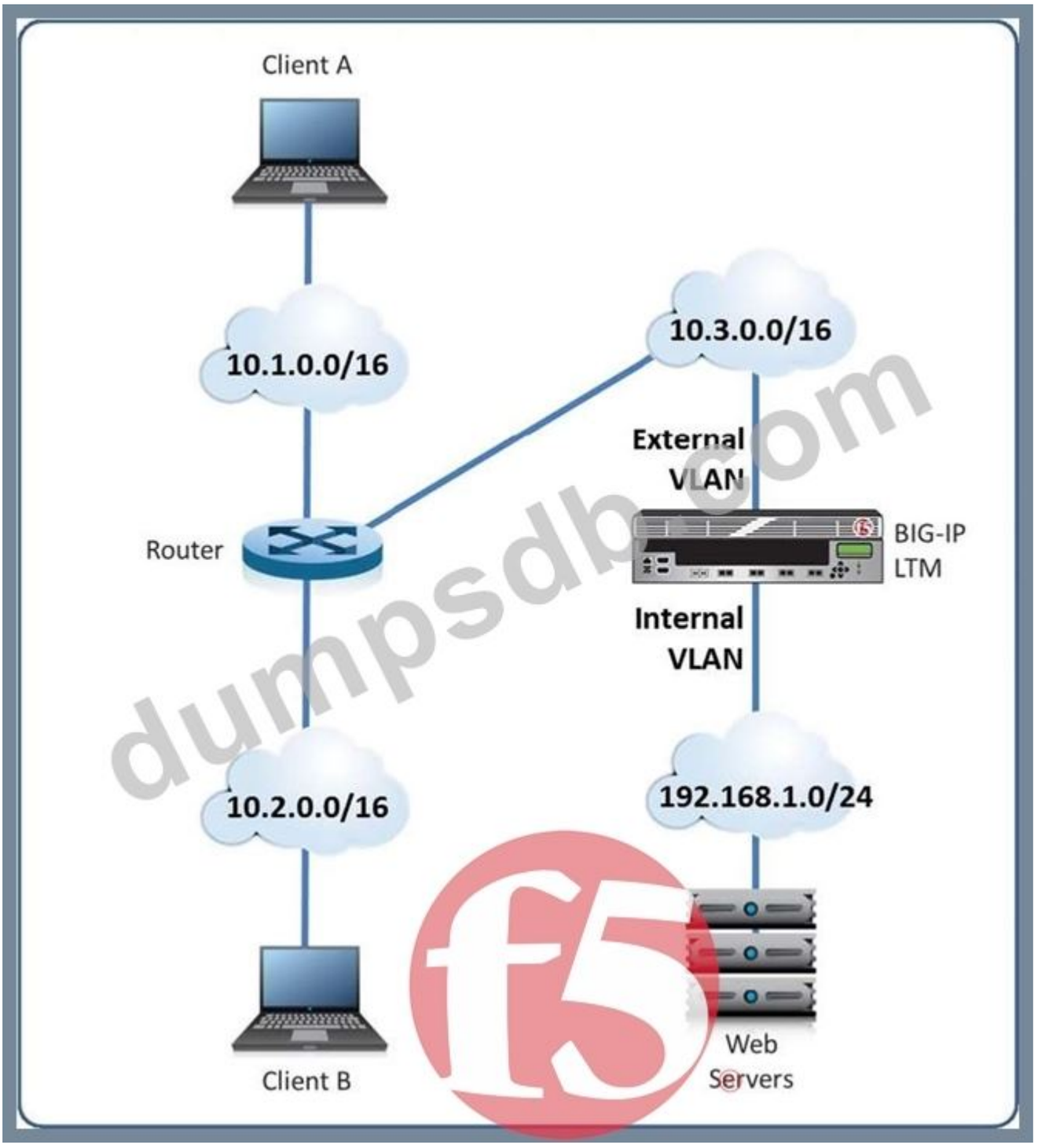
PACKET CAPTURE AT LTM DEVICE – TRYING TO CONNECT DIRECTLY TO SERVER

EXTERNAL VLAN

```
16:02:26.047441 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:02:26.285979 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:02:29.048674 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:02:29.283160 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:02:35.065086 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,nop,sackOK>
16:02:35.298372 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,nop,sackOK>
```

INTERNAL VLAN

<no packets captured>



dumpsdb.com

-- Exhibit -

Refer to the exhibits.

Users are able to access the application when connecting to the virtual server but are unsuccessful when connecting directly to the application servers. The LTM Specialist wants to allow direct access to the application servers.

Which configuration change resolves this problem?

A. Configure a route to the web server subnet on the network router.

B. Configure an IP Forwarding virtual server on the LTM device.

C. Enable port 443 on the virtual server.

D. Disable address translation on the virtual server.

E. Configure a SNAT pool on the LTM device.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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. ClientHello
B. Issuer
C. HTTP Version
D. User-Agent
E. ServerHello
Answer: (SHOW ANSWER)

NEW QUESTION: 114
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
Answer: C (LEAVE A REPLY)

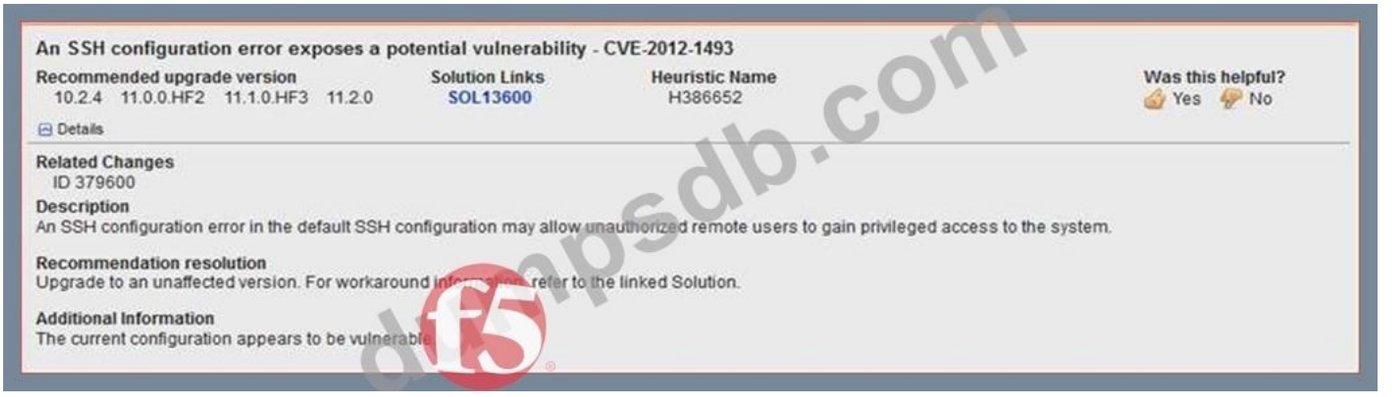
NEW QUESTION: 115

A new web application is hosted at www.example.net, but some clients are still pointing to the legacy web application at www.example.com.
Which iRule will allow clients referencing www.example.com to access the new application?
A. when HTTP_REQUEST {
if {[HTTP::host] equals "www.example.com" }{
HTTP::redirect "http://www.example.net" }
}
B. when HTTP_REQUEST {
if {[HTTP::host] equals "www.example.*" }{
HTTP::redirect "http://www.example.net" }
}
C. when HTTP_DATA {
if {[HTTP::host] equals "www.example.*" }{
HTTP::redirect "http://www.example.net" }
}
D. when HTTP_RESPONSE {
if {[HTTP::host] equals "www.example.com" }{
HTTP::redirect "http://www.example.net" }
}
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
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 attempted access of clients without credentials to the new_application_pool.
C. Allows clients without credentials to access the old_application_pool and logs the access of clients with credentials to the new_application_pool.
D. Allows clients with credentials to access the old_application_pool and logs the attempted access of clients with credentials to the new_application_pool.
Answer: (SHOW ANSWER)
NEW QUESTION: 117

A web application requires knowledge of the client's true IP address for logging and analysis purposes. Instances of the application that can decode X-Forwarded-For HTTP headers reside in pool_a, while pool_b instances assume the source IP is the true address of the client.
Which iRule provides the proper functionality?
A. when HTTP_DATA { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b } }
B. when HTTP_RESPONSE { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b } }
C. when HTTP_OPEN { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b } }
D. when HTTP_REQUEST { if {[HTTP::header exists X-Forwarded-For]}{ pool pool_a } else { pool pool_b } }
Answer: D (LEAVE A REPLY)

NEW QUESTION: 118
-- Exhibit -



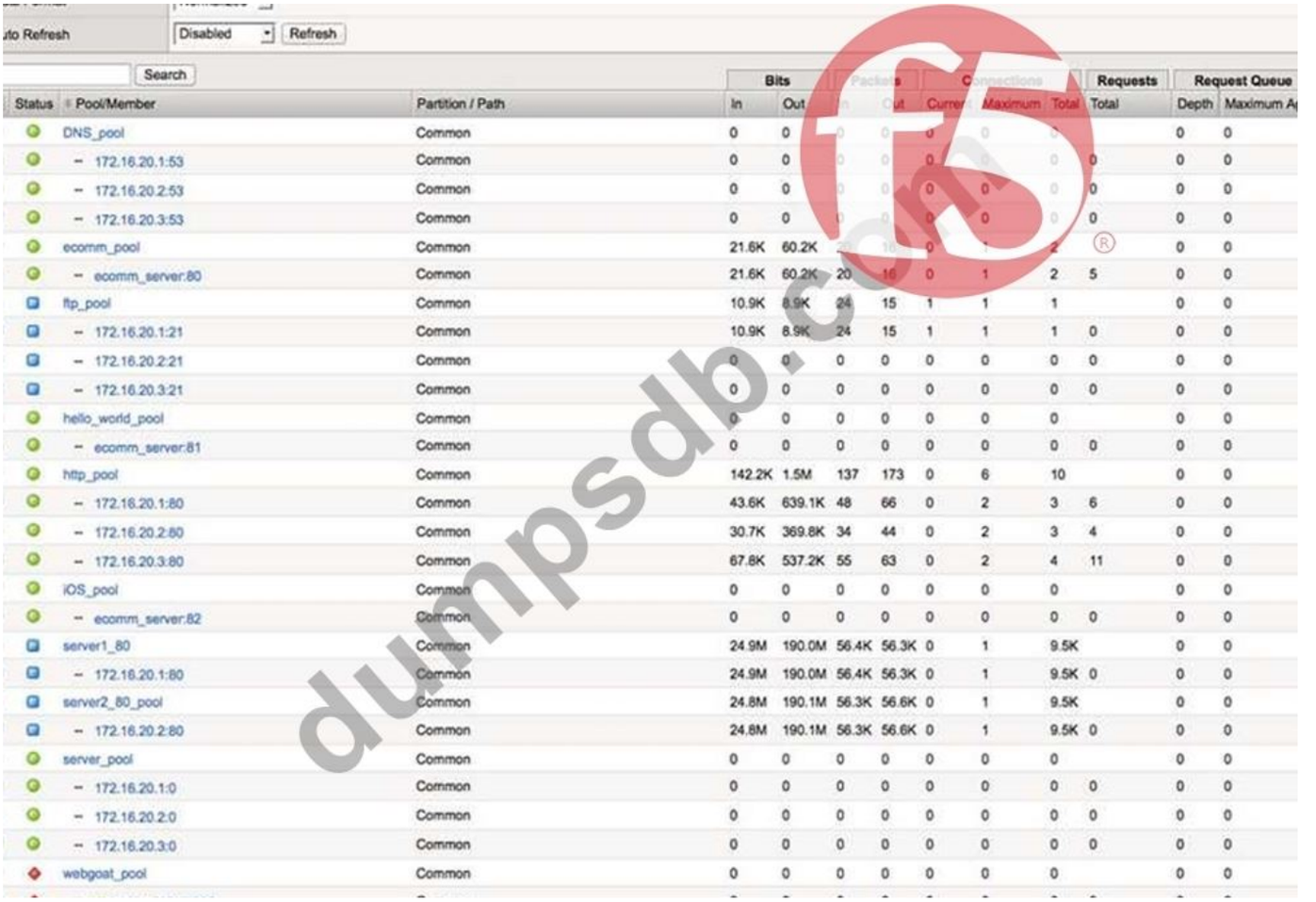
-- Exhibit --
Refer to the exhibit.
An LTM Specialist is working on an LTM 11.0.0 installation and has identified a security vulnerability as shown in the exhibit. The LTM Specialist is tasked with applying the latest available hotfix to resolve the problem.
Which procedure resolves the problem?
A. Browse to System > Software Management > Image List.
Import 11.1.0.HF3 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 TMOS 11.2.0 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 > Hotfix List.
Import 11.1.0.HF3 to the available hotfix images.

Select the imported hotfix image and installation location and click Install.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 119

-- Exhibit-



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			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

-- Exhibit -Refer to the exhibit.

An administrator created a monitor to a pool member web server, which resulted in a pool member that is marked red. The administrator knows the web server is working when it is accessed from another computer.

What should the administrator do to correct the problem?

A. Change the username and/or password on the monitor.

B. Change the default gateway on the server.

C. Create a SNAT in the LTM device configuration.

D. Change the route to the client in the LTM configuration.

Answer: (SHOW ANSWER)

NEW QUESTION: 120

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?

dumpsdb.com

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

NEW QUESTION: 121
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 '(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
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 'host 10.0.0.1' -w /var/tmp/trace.cap
Answer: B (LEAVE A REPLY)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 122
An LTM device pair is configured for failover and connection mirroring. The LTM devices are configured with virtual servers for HTTP, HTTPS with SSL offload, and SSH. An event occurs that causes a failover.
HTTP and SSH sessions active at the time of failover remain active, but HTTPS sessions are dropped.

What is the root cause of this problem?

A. The SSL certificates on the LTM devices do NOT match.

B. Connection mirroring was NOT enabled for the HTTPS virtual servers.

C. SNAT automap was NOT enabled for the HTTPS virtual servers.

D. Connection mirroring is incompatible with clientssl profiles.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 123

The pool members are serving up simple static web content.

The current virtual server configuration is given as follows:

```
tmsh list ltm virtual simple
ltm virtual simple {
destination 10.10.10.10:80
ip-protocol tcp
mask 255.255.255.255
profiles {
http { }
httpcompression { }
oneconnect { }
tcp { }
}
snat automap
vlans-disabled
}
tmsh list ltm pool simple_pool
ltm pool simple_pool {
members {
10.10.10.11:80 {
address 10.10.10.11 }
10.10.10.12:80 {
address 10.10.10.12 }
10.10.10.12:80 {
address 10.10.10.13 }
}
}
```

Which three objects in the virtual server configuration can be removed without disrupting functionality of the virtual server? (Choose three.)

A. http

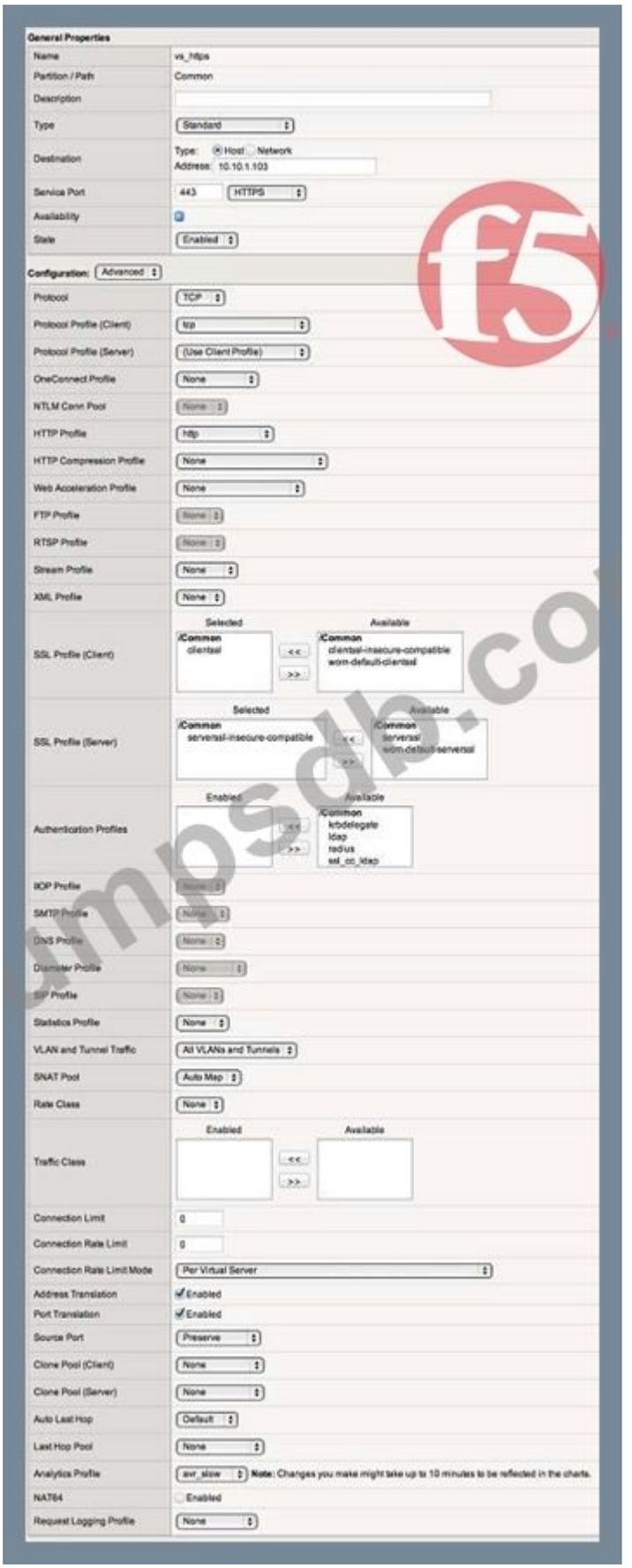
B. tcp

C. httpcompression

D. snat automap

E. oneconnect
Answer: (SHOW ANSWER)

NEW QUESTION: 124
-- Exhibit -



-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting an issue with an application configured on an LTM device.

The application works properly when accessed directly via the servers; however, it does not work when accessed via the LTM device. The virtual server, 192.168.1.211:443, is configured to SNAT using the address 192.168.1.144 and references a pool with the member 192.168.10.80:443. The virtual server has no Client or Server SSL profiles associated.
Which configuration change will allow the application to function through the virtual server?
A. Change pool member port to 8443.
B. Add Client and Server SSL profiles to the virtual server.
C. Change virtual server port to 8443.
D. Add SSL off-loading to the pool member.
Answer: (SHOW ANSWER)

NEW QUESTION: 125
A customer needs to intercept all of the redirects its application is sending to clients. When a redirect is matched, the customer needs to log a message including the client IP address.
Which iRule should be used?
A. when HTTP_RESPONSE {
if { [HTTP::is_redirect] } {
log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"
}
}
B. when HTTP_REQUEST {
if { [HTTP::is_301] } {
log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"
}
}
C. when HTTP_REQUEST {
if { [HTTP::is_redirect] } {
log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"
}
}
D. when HTTP_RESPONSE {
if { [HTTP::is_3xx] } {
log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"
}
}
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
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 NOT on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the discard.
B. The iRule compares a client IP to a list. If the client IP is 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, discard and log the discard.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
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 a backslash before the colon in the receive string.
B. Add a valid username and password to the monitor.
C. Add an NTLM profile to the virtual server.
D. Use an HTTPS monitor with a valid certificate instead.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 128
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. Server must support HTTP/0.9.
B. Client must support HTTP keep-alive.
C. Server must support HTTP keep-alive.
D. Client must support HTTP/1.0.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
-- 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. Upgrade the client to support the appropriate SSL cipher suite.

B. Adjust the SSL key length in the SSL profile to match the minimum required by the client.

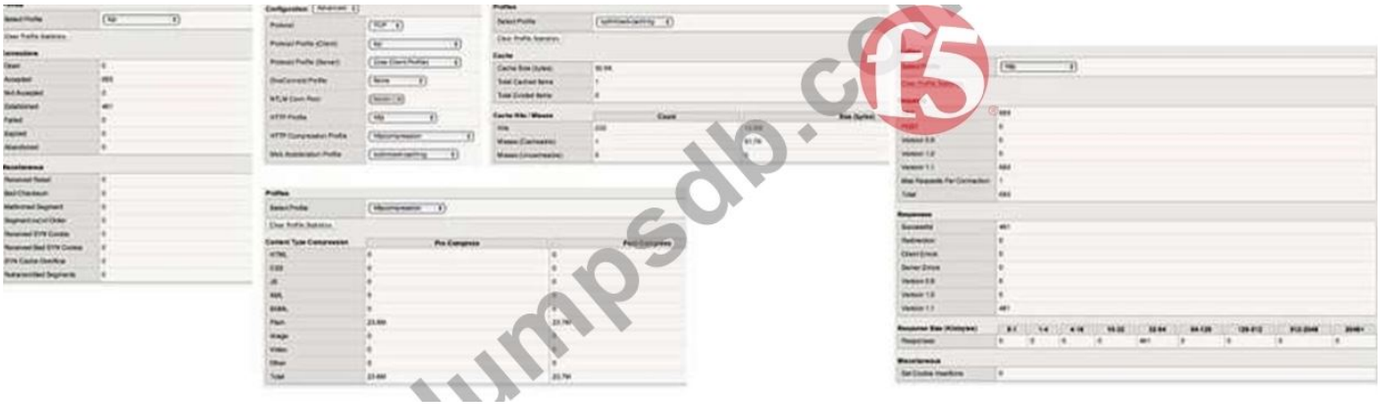
C. Set the virtual server to listen on port 443 (HTTPS).

D. Select the appropriate "SSL Profile (Client)" in the virtual server settings.

Answer: (SHOW ANSWER)

NEW QUESTION: 130

-- 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. http

B. optimized-caching

C. tcp

D. httpcompression

Answer: D (LEAVE A REPLY)

NEW QUESTION: 131

An LTM device is load balancing SIP traffic. An LTM Specialist notices that sometimes the SIP request is being load balanced to the same server as the initial connection.

Which setting in the UDP profile will make the LTM device more evenly distribute the SIP traffic?

A. Set Timeout to Indefinite

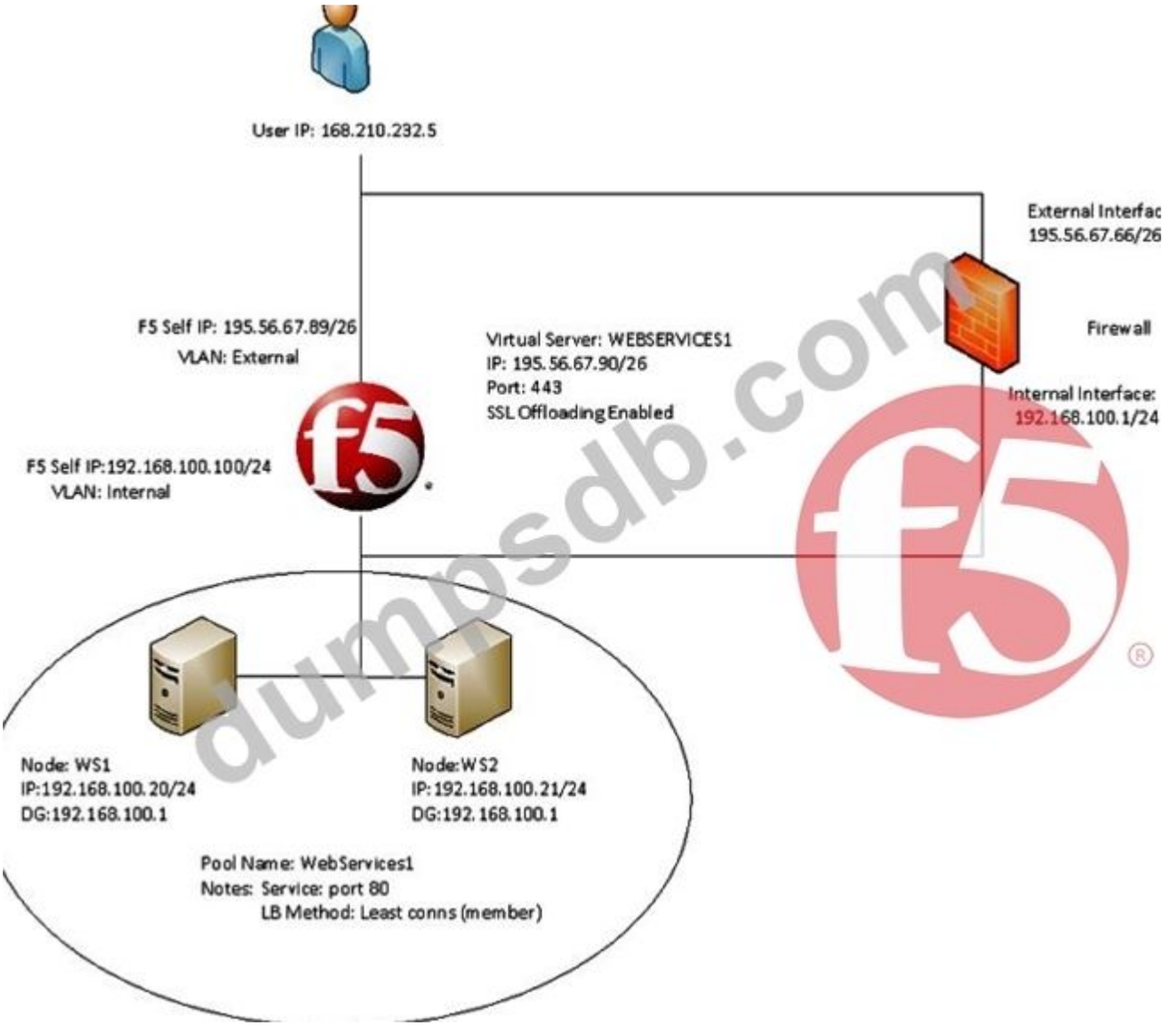
B. Enable Datagram LB

C. Disable Datagram LB

D. Set Timeout to Immediate

Answer: B (LEAVE A REPLY)

NEW QUESTION: 132



-- 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 Secure Network Address Translation (SNAT) pool on the virtual server is activated.

B. The individual's data stream is being routed to the LTM device by a means other than the default route.

C. Network Address Translation (NAT) has occurred in the path between the client and the LTM device.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 133

-- Exhibit -

```
Monitor definition:

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

HTTP Headers from tcpdump:

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

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

-- Exhibit --

Refer to the exhibit.

An HTTP monitor always marks the nodes in the pool as down. The monitor's definition and the HTTP headers from the monitor request and response are provided.

What is the issue?

A. The response is compressed.

B. The send string is incorrect.

C. The monitor timeout is too short.

D. The monitor is NOT configured to follow the redirect.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 134

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 web server is configured to accept HTTP 1.0 requests only.

B. The client request does NOT include a Host header.

C. The web server is NOT expecting a keep-alive connection.
D. The User-Agent header contains an invalid character.
Answer: B (LEAVE A REPLY)

Valid 301b Dumps shared by TrainingQuiz.com for Helping Passing 301b Exam! TrainingQuiz.com now offer the **newest 301b exam dumps**, the TrainingQuiz.com 301b exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 301b dumps with Test Engine here: https://www.trainingquiz.com/301b-practice-quiz.html (**210** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)