DUMPSARENA

LTM Specialist: Maintain & Troubleshoot

F5 301b

Version Demo

Total Demo Questions: 15

Total Premium Questions: 210

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

QUESTION NO: 2

-- Exhibit –

```
Through LTM Device:
New TCP connection #1: 172.16.1.3(63936) <-> 172.16.20.21(443)
1 1  0.0013 (0.0013)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_AES_256_CBC_SHA256
        Unknown value 0xff
        compression methods
                NULL
1 2  0.0038 (0.0025)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          7c 00 d2 cf 81 f8 cd ab 6b 48 c0 9a cc 19 df f7
          12 5f f2 c8 2a a2 e8 ef 1e f1 10 41 61 99 6d 27
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
1 3  0.0038 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0038 (0.0000)  S>C  Handshake
      CertificateRequest
        certificate_types                   rsa_sign
        certificate_types                   dss_sign
        certificate_types                   unknown value
        certificate_authority
          30 81 90 31 0b 30 09 06 03 55 04 06 13 02 55 53
          31 0b 30 09 06 03 55 04 08 13 02 57 41 31 10 30
          0e 06 03 55 04 07 13 07 53 65 61 74 74 6c 65 31
          14 30 12 06 03 55 04 0a 13 0b 45 78 61 6d 70 6c
          65 2e 43 6f 6d 31 14 30 12 06 03 55 04 0b 13 0b
          45 6e 67 69 6e 65 65 72 69 6e 67 31 36 30 34 06
          03 55 04 03 13 2d 43 4e 3d 4a 6f 68 6e 20 55 73
          65 72 2c 4f 55 3d 45 6e 67 69 6e 65 65 72 69 6e
          67 2c 44 43 3d 65 78 61 6d 70 6c 65 2c 44 43 3d
          63 6f 6d
      ServerHelloDone
1 5  0.0040 (0.0002)  C>S  Handshake
      Certificate
1 6  0.0040 (0.0000)  C>S  Handshake
      ClientKeyExchange
1 7  0.0040 (0.0000)  C>S  ChangeCipherSpec
1 8  0.0044 (0.0003)  C>S  Handshake
1 9  0.0049 (0.0004)  S>C  Alert
     level           fatal
     value           handshake_failure
1    0.0049 (0.0000)  S>C  TCP FIN
1    0.0049 (0.0000)  C>S  TCP RST

Direct to application server:
New TCP connection #1: 1.1.2.150(64506) <-> 172.16.20.21(443)
1 1  0.0027 (0.0027)  C>S  Handshake
      ClientHello
        Version 3.1
        resume [32]=
          96 55 ee e0 53 90 e5 63 f8 46 3c 5c 19 59 8a fa
          c4 e6 2f 5f 6e 80 40 dd 08 05 5c 74 f7 3a d6 61
        cipher suites
        Unknown value 0xc00a
        Unknown value 0xc014
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
        TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
        Unknown value 0xc00f
        Unknown value 0xc005
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        Unknown value 0xc007
        Unknown value 0xc009
        Unknown value 0xc011
        Unknown value 0xc013
        Unknown value 0x45
        Unknown value 0x44
        TLS_DHE_DSS_WITH_RC4_128_SHA
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        TLS_DHE_DSS_WITH_AES_128_CBC_SHA
        Unknown value 0xc00c
        Unknown value 0xc00e
        Unknown value 0xc002
        Unknown value 0xc004
        Unknown value 0x96
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_RC4_128_MD5
        TLS_RSA_WITH_AES_128_CBC_SHA
        Unknown value 0xc008
        Unknown value 0xc012
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        Unknown value 0xc00d
        Unknown value 0xc003
        Unknown value 0xfeff
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                NULL
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has created a virtual server to load balance traffic to a pool of HTTPS servers. The servers use client certificates for user authentication. The virtual server has clientssl, serverssl, and http profiles enabled. Clients are unable to connect to the application through the virtual server. Clients are able to connect to the application servers directly.

What is the root cause of the problem?

A. The application server does NOT support 2048-bit keys.

B. The clientssl profile is NOT set to require a client certificate.

C. The LTM device does NOT trust the issuing CA of the client certificate.

D. The application server does NOT see the client certificate due to SSL offload.

ANSWER: D

QUESTION NO: 3

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

A. bigpipe platform show | grep -i pva

B. tmsh show /sys hardware pva status

C. tmsh show /sys hardware | grep -i pva

D. tmsh show /ltm hardware | grep -i pva

ANSWER: C

QUESTION NO: 4

-- Exhibit –

```
Client IP address:      10.0.0.1
Virtual Server:         11.0.0.1
Web Server:             12.0.0.1

Capture taken on Web server interface eth1:12.0.0.1
-------------------------------------------------

01:35:35.161396 IP 10.0.0.1.35285 > 12.0.0.1.http: S 3230388980:3230388980(0) win 8192 <mss 1416,nop,wscale 8,nop,nop,sackOK>
01:35:35.161466 IP 12.0.0.1.http > 10.0.0.1.35285: S 2242263384:2242263384(0) ack 3230388981 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 6>
01:35:35.177621 IP 10.0.0.1.26079 > 12.0.0.1.http: P 3570570638:3570571021(383) ack 1991745822 win 255
01:35:35.184475 IP 12.0.0.1.http > 10.0.0.1.26079: . 1:1417(1416) ack 383 win 700
01:35:35.184517 IP 12.0.0.1.http > 10.0.0.1.26079: . 1417:2833(1416) ack 383 win 700
01:35:35.184588 IP 12.0.0.1.http > 10.0.0.1.26079: P 2833:3905(1072) ack 383 win 700
01:35:35.297647 IP 10.0.0.1.35285 > 12.0.0.1.http: . ack 1 win 66
01:35:35.337992 IP 10.0.0.1.26079 > 12.0.0.1.http: . ack 2833 win 259
01:35:35.535349 IP 10.0.0.1.26079 > 12.0.0.1.http: . ack 3905 win 255
01:35:38.965404 IP 12.0.0.1.http > 10.0.0.1.35285: S 2242263384:2242263384(0) ack 3230388981 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 6>
01:35:39.096377 IP 10.0.0.1.35285 > 12.0.0.1.http: . ack 1 win 66 <nop,nop,sack 1 {0:1}>

Capture taken on LTM interface 0.0
-----------------------------------

17:32:30.828126 IP 10.0.0.1.10120 > 11.0.0.1.http: S 3414174673:3414174673(0) win 8192 <mss 1416,nop,wscale 2,nop,nop,sackOK> in slot1/tmm0 lis=
17:32:30.828172 IP 11.0.0.1.http > 10.0.0.1.10120: S 1751596785:1751596785(0) ack 3414174674 win 4248 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:30.951747 IP 10.0.0.1.10120 > 11.0.0.1.http: . ack 1 win 16638 in slot1/tmm0 lis=/Common/my_virtual
17:32:30.982820 IP 10.0.0.1.10120 > 11.0.0.1.http: P 1:560(559) ack 1 win 16638 in slot1/tmm0 lis=/Common/my_virtual
17:32:30.982871 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:30.952878 IP 11.0.0.1.http > 10.0.0.1.10120: . ack 560 win 4807 out slot1/tmm0 lis=/Common/my_virtual
17:32:33.982895 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:37.162627 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:40.352728 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,sackOK,eol> out slot1/tmm0 lis=/Common/my_virtual
17:32:43.582864 IP 11.0.0.1.http > 10.0.0.1.10120: R 1:55(54) ack 560 win 4807 out slot1/tmm0 lis=/Common/my_virtual
```

-- Exhibit --

Refer to the exhibit.

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

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

A. Configure SNAT on the pool.

B. Configure SNAT on the virtual server.

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

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

ANSWER: B D

QUESTION NO: 5

A stand-alone LTM device is to be paired with a second LTM device to create an active/standby pair. The current stand-alone LTM device is in production and has several VLANs with floating IP addresses configured. The appropriate device service clustering (DSC) configurations are in place on both LTM devices.

Which two non-specific DSC settings should the LTM Specialist configure on the second LTM device to ensure no errors are reported when attempting to synchronize for the first time? (Choose two.)

A. pools

B. VLANs

C. default route

D. self IP addresses

ANSWER: B D

QUESTION NO: 6

Which iRule statement demotes a virtual server from CMP?

A. set ::foo 123

B. set static::foo 123

C. persist source_addr 1800

D. [class match $HTTP_CONTENT contains my_data_class]

ANSWER: A

QUESTION NO: 7

An LTM Specialist has just manually failed the active LTM device over to the standby LTM device. The LTM Specialist notices the newly active LTM device is NOT currently receiving traffic. The LTM Specialist verifies the newly active device is responding to ARP but still no traffic is hitting the virtual servers. The LTM Specialist also notices that the virtual servers eventually start responding.

What should be added to the configuration to resolve the problem?

A. vlan failsafe

B. floating self IP

C. network failover

D. MAC masquerading

E. connection mirroring

ANSWER: D

QUESTION NO: 8

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. Add a ClientSSL profile to the virtual server.

C. Disable SNAT Automap on the virtual server.

D. Remove the HTTP profile from the virtual server.

ANSWER: D

QUESTION NO: 9

An active/standby pair of LTM devices deployed with network failover are working as desired. After external personnel perform maintenance on the network, the LTM devices are active/active rather than active/standby. No changes were made on the LTM devices during the network maintenance.

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

A. checking that the configurations are synchronized

B. checking the configuration of the VLAN used for failover

C. checking the configuration of the VLAN used for mirroring

D. checking the open ports in firewalls between the LTM devices

E. checking synchronization of system clocks among the network devices

ANSWER: B D

QUESTION NO: 10

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. tcp

B. http

C. oneconnect

D. snat automap

E. httpcompression

ANSWER: B C E

QUESTION NO: 11

Which two subsystems could the LTM Specialist utilize to access an LTM device with lost management interface connectivity? (Choose two.)

A. AOM

B. ILO

C. SCCP

D. ALOM

ANSWER: A C

QUESTION NO: 12

-- Exhibit –

```
Virtual Server details

Type                              Standard
Protocol                          TCP
Protocol Profile (Client)     tcp-wan-optimised
Protocol Profile (Server)     tcp-lan-optimised
OneConnect Profile                None
NTLM Conn Pool                    None
HTTP Profile                      None
FTP Profile                       None
Stream Profile                    None
XML Profile                       None
SSL Profile (Client)          None
SSL Profile (Server)          None
Authentication Profiles       None

RTSP Profile                      None
SMTP Profile                      None
Diameter Profile              None
SIP Profile                       None
Statistics Profile                None

SNAT Pool                         None
Rate Class                        None
Traffic Class                     None

Connection Limit              None
Connection Mirroring          None
Address Translation           Enabled
Port Translation              Enabled
Source Port                       Preserve
Clone Pool (Client)           None
Clone Pool (Server)           None
Last Hop Pool                     None

Pool details:

10.40.242.12: 443
10.40.242.13: 443
```

-- Exhibit --

Refer to the exhibit.

An LTM device is used to load balance web content over a secure channel.

The developers of the web content have done a trace using an HTTP profiler application. They believe that allowing the LTM device to compress traffic to the client will improve performance. The client can utilize GZIP or deflate compression algorithms.

An LTM Specialist must implement the compression.

The LTM Specialist has completed the following actions:

1. Create the relevant profile.

2. Apply the relevant profile to the virtual server (VS).

After applying the relevant profile, the LTM device is failing to compress the traffic. Instead, the traffic is being served with an error.

What is the problem?

A. The incorrect compression algorithm is applied to the compression profile.

B. The LTM device CANNOT SSL offload the traffic in order to read and compress it.

C. The Protocol Profile (Client) option of "Allow Compression" needs to be enabled.

D. The Protocol Profile (Server) option of "Allow Compression" needs to be enabled.

ANSWER: B

QUESTION NO: 13

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

QUESTION NO: 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
```

-- Exhibit --

Refer to the exhibit.

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

What is the problem?

A. The virtual server does NOT have persistence configured.

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

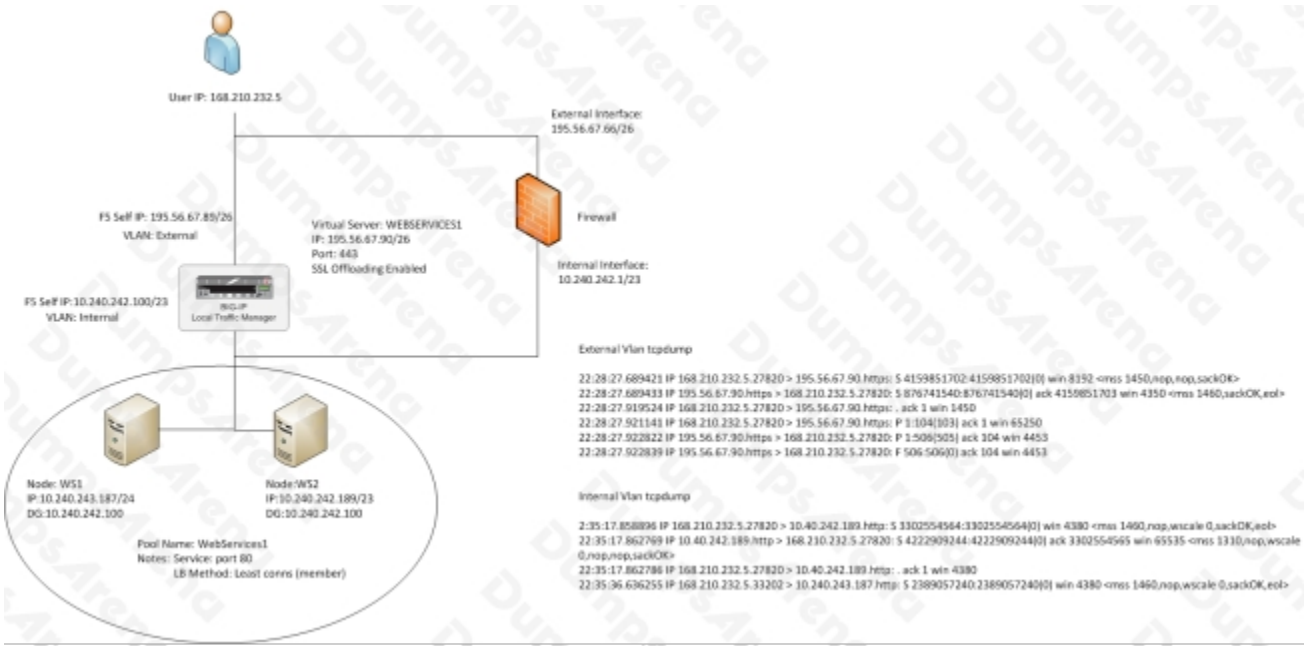
C. The cookie set by the LTM device does NOT have an "Expires" value.

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

ANSWER: C

QUESTION NO: 15

-- Exhibit –



-- Exhibit --

Refer to the exhibit.

An LTM Specialist has a virtual server set up on the LTM device as per the exhibit. The LTM Specialist receives reports of intermittent issues. Some clients are connecting fine while others are failing to connect.

The LTM Specialist does a tcpdump on the relevant interfaces, with the following results extracted:

What is causing the intermittent issues?

A. The firewall is dropping the packets from WS1.

B. The default gateway is inaccessible from WS1.

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

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

ANSWER: B