DUMPSBOSS.COM

BIG-IP Local Traffic Manager (LTM) Specialist: Maintain & Troubleshoot

F5 301b

Version Demo

Total Demo Questions: 15

Total Premium Questions: 210

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

dumpsboss.com

QUESTION NO: 1

An LTM Specialist wants to allow access to the Always On Management (AOM) from the network.

Which two methods should the LTM Specialist use to configure the AOM interface? (Choose two.)

A. Configure the AOM IP from the front panel buttons and LCD.

B. Choose the network configurator in the AOM menu on the serial port.

C. Configure the AOM network address in the GUI under System>Platform.

D. Log in to the Host via ssh, "ssh aom", and modify the network configuration file.

ANSWER: B D

QUESTION NO: 2

-- Exhibit --

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

-- Exhibit --

Refer to the exhibit.

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

Where is the reset originating?

A. the local switch

B. the application server

C. the device initiating the connection

D. the destination device of the initial connection

ANSWER: C

QUESTION NO: 3

Users in a branch office are reporting a website is always slow. No other users are experiencing the problem. The LTM Specialist tests the website from the external VLAN along with testing the servers directly. All tests indicate normal behavior. The environment is a single HTTP virtual server on the external VLAN with a single pool containing three HTTP pool members on the internal VLAN.

Which two locations are most appropriate to collect additional protocol analyzer data? (Choose two.)

A. a user's machine

B. the switch local to the user

C. the LTM device's internal VLAN

D. the LTM device's external VLAN

E. a user's Active Directory authentication

ANSWER: A B

QUESTION NO: 4

A failover event is recorded in the following log messages:

Jan 01 00:56:56 BIG-IP notice mcpd[5318]: 01070727:5: Pool /Common/my-pool member /Common/10.0.0.10:80 monitor status down.

Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0045:5: Leaving active, group score 10 peer group score 20.

Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0052:5: Standby for traffic group /Common/traffic-group-1.

Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0018:5: Standby

Jan 01 00:57:06 BIG-IP notice logger: /usr/bin/tmipsecd --tmmcount 4 ==> /usr/bin/bigstart stop racoon

What is the cause of the failover?

A. The HA group score changed.

B. No traffic is seen on traffic-group-1.

C. The peer device left the traffic group.

D. The racoon service stopped responding.

ANSWER: A

QUESTION NO: 5

Given this as the first packet displayed of an ssldump:

2 2 1296947622.6313 (0.0001) S>CV3.1(74) Handshake

ServerHello

Version 3.1

random[32]=

19 21 d7 55 c1 14 65 63 54 23 62 b7 c4 30 a2 f0

b8 c4 20 06 86 ed 9c 1f 9e 46 0f 42 79 45 8a 29

session_id[32]=

c4 44 ea 86 e2 ba f5 40 4b 44 b4 c2 3a d8 b4 ad

4c dc 13 0d 6c 48 f2 70 19 c3 05 f4 06 e5 ab a9

cipherSuite TLS_RSA_WITH_RC4_128_SHA

compressionMethod NULL

In reviewing the rest of the ssldump, the application data is NOT being decrypted.

Why is ssldump failing to decrypt the application data?

A. The application data is encrypted with SSLv3.

B. The application data is encrypted with TLSv1.

C. The data is contained within a resumed TLS session.

D. The BigDB Key Log.Tcpdump.Level needs to be adjusted.

ANSWER: C

QUESTION NO: 6

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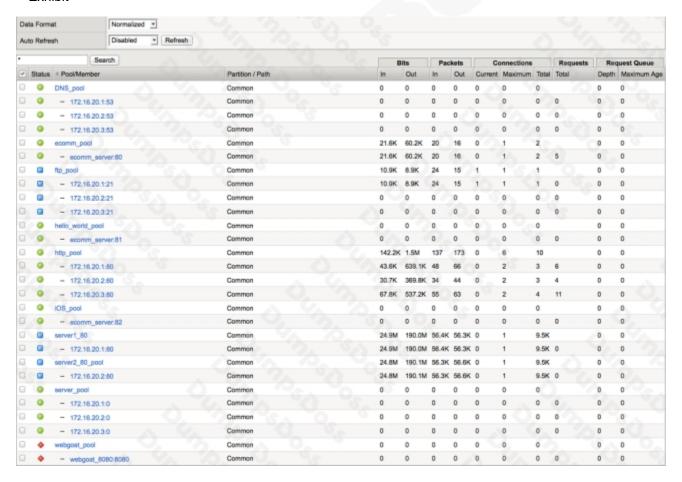
Which two actions would help determine the cause of the malfunction? (Choose two.)

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: 7

-- 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	20	16	0	1	2		0	0
	🟢	– ecomm_server:80	Common	21.6K	60.2K	20	16	0	1	2	5	0	0
	🔵	ftp_pool	Common	10.9K	8.9K	24	15	1	1	1		0	0
	🔵	– 172.16.20.1:21	Common	10.9K	8.9K	24	15	1	1	1	0	0	0
	🔵	– 172.16.20.2:21	Common	0	0	0	0	0	0	0	0	0	0
	🔵	– 172.16.20.3:21	Common	0	0	0	0	0	0	0	0	0	0
	🟢	hello_world_pool	Common	0	0	0	0	0	0	0		0	0
	🟢	– ecomm_server:81	Common	0	0	0	0	0	0	0	0	0	0
	🟢	http_pool	Common	142.2K	1.5M	137	173	0	6	10		0	0
	🟢	– 172.16.20.1:80	Common	43.6K	639.1K	48	66	0	2	3	6	0	0
	🟢	– 172.16.20.2:80	Common	30.7K	369.8K	34	44	0	2	3	4	0	0
	🟢	– 172.16.20.3:80	Common	67.8K	537.2K	55	63	0	2	4	11	0	0
	🟢	iOS_pool	Common	0	0	0	0	0	0	0		0	0
	🟢	– ecomm_server:82	Common	0	0	0	0	0	0	0	0	0	0
	🔵	server1_80	Common	24.9M	190.0M	56.4K	56.3K	0	1	9.5K		0	0
	🔵	– 172.16.20.1:80	Common	24.9M	190.0M	56.4K	56.3K	0	1	9.5K	0	0	0
	🔵	server2_80_pool	Common	24.8M	190.1M	56.3K	56.6K	0	1	9.5K		0	0
	🔵	– 172.16.20.2:80	Common	24.8M	190.1M	56.3K	56.6K	0	1	9.5K	0	0	0
	🟢	server_pool	Common	0	0	0	0	0	0	0		0	0
	🟢	– 172.16.20.1:0	Common	0	0	0	0	0	0	0	0	0	0
	🟢	– 172.16.20.2:0	Common	0	0	0	0	0	0	0	0	0	0
	🟢	– 172.16.20.3:0	Common	0	0	0	0	0	0	0	0	0	0
	🔴	webgoat_pool	Common	0	0	0	0	0	0	0		0	0
	🔴	– webgoat_8080:8080	Common	0	0	0	0	0	0	0	0	0	0

-- Exhibit --

Refer to the exhibit.

Which pool can be removed without affecting client traffic?

A. ftp_pool

B. http_pool

C. server1_80

D. server_pool

ANSWER: D

QUESTION NO: 8

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

ssldump -Aed -ni vlan301 'port 443'

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

A. HTTP Version

B. User-Agent

C. ClientHello

D. ServerHello

E. Issuer

ANSWER: C D

QUESTION NO: 9

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 show /sys license

B. tmsh show /sys hardware

C. bigpipe config save /config.ucs

D. tmsh load /sys /ucs rma

E. tmsh load /sys ucs no-license

ANSWER: E

QUESTION NO: 10

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 via ssh to the AOM IP address.

B. Connect via ssh to the management address.

C. Connect to the LTM device via serial connection.

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

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

ANSWER: A C

QUESTION NO: 11

An IT administrator wants to log which server is being load balanced to by a user with IP address 10.10.10.25.

Which iRule should the LTM Specialist use to fulfill the request?

A. when SERVER_CONNECTED {
if { [IP::addr [IP::remote_addr]] equals 10.10.10.25]} {
log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }
}

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

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

D. when CLIENT_ACCEPTED {
if { [IP::addr [IP::remote_addr] equals 10.10.10.25]} {
log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }
}

ANSWER: C

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

-- 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 LTM device is redirecting users to HTTPS.

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

D. The application servers are redirecting users to HTTPS.

ANSWER: D

QUESTION NO: 14

-- Exhibit –

```
                        172.16.1.20(49379) <-> 172.16.20.1(443)
                  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
```

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

```
[~]$ openssl s_client -connect 172.16.20.1:443
CONNECTED(00000003)
depth=0 /O=TurnKey Linux/OU=Software appliances
verify error:num=18:self signed certificate
verify return:1
depth=0 /O=TurnKey Linux/OU=Software appliances
verify return:1
---
Certificate chain
 0 s:/O=TurnKey Linux/OU=Software appliances
   i:/O=TurnKey Linux/OU=Software appliances
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICgzCCAeygAwIBAgIJAImLXVLJqYzBMA0GCSqGSIb3DQEBBQUAMDYxFjAUBgNV
BAoTDVR1cm5LZXkgTGludXgxHDAaBgNVBAsTE1NvZnR3YXJlIGFwcGxpYW5jZXMw
HhcNMTAwNDE1MTkxNDQzWhcNMjAwNDEyMTkxNDQzWjA2MRYwFAYDVQQKEw1UdXJu
S2V5IExpbnV4MRwwGgYDVQQLExNTb2Z0d2FyZSBhcHBsaWFuY2VzMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCV1genrRHsav6R+M/xYyooMJVpXWZbzeKu04ro
euadY0KOwwa2zF9jaD0HDIJ3MtnVYaHMsH2vqoo1Q8EfohP85RfHrO4kMxtvAefm
s1qGE7MkmIxLtwYjjWXmwxW7sCFL19kt6pFOatzqeK3WxbdM5yF/RTHF4R/vyKQI
21Yf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBRG5CDKtO1kiiix7sc2JjoVHajd2zBm
BgNVHSMEXzBdgBRG5CDKtO1kiiix7sc2JjoVHajd26E6pDgwNjEWMBQGA1UEChMN
VHVybktleSBMaW51eDEcMBoGA1UECxMTU29mdHdhcmUgYXBwbGlhbmNlc4IJAImL
XVLJqYzBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEANo2TuXFVZKWG
n6KznFgueLGzn+qgyIz0ZVG5PF8RRzHPYDAIDRU0MEReQHhI4CRImMAwTAFdmhp1
RGH2+IqwglEPB7K6eudRy0D9GqzMHZrdMo9d3ewPB3Bqj0rPhs5yRTgNrZHyasJr
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 Strict Resume.

B. Change Secure Renegotiation to "Request."

C. Enable ProxySSL option in the server SSL profile.

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

ANSWER: B

QUESTION NO: 15

-- Exhibit –

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

-- Exhibit --

Refer to the exhibit.

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

A. /Common/vs1-https-redirect

B. /Common/vs2-https-redirect

C. /Common/vs3-https-redirect

D. /Common/vs4-https-redirect

E. /Common/vs5-https-redirect

ANSWER: A D