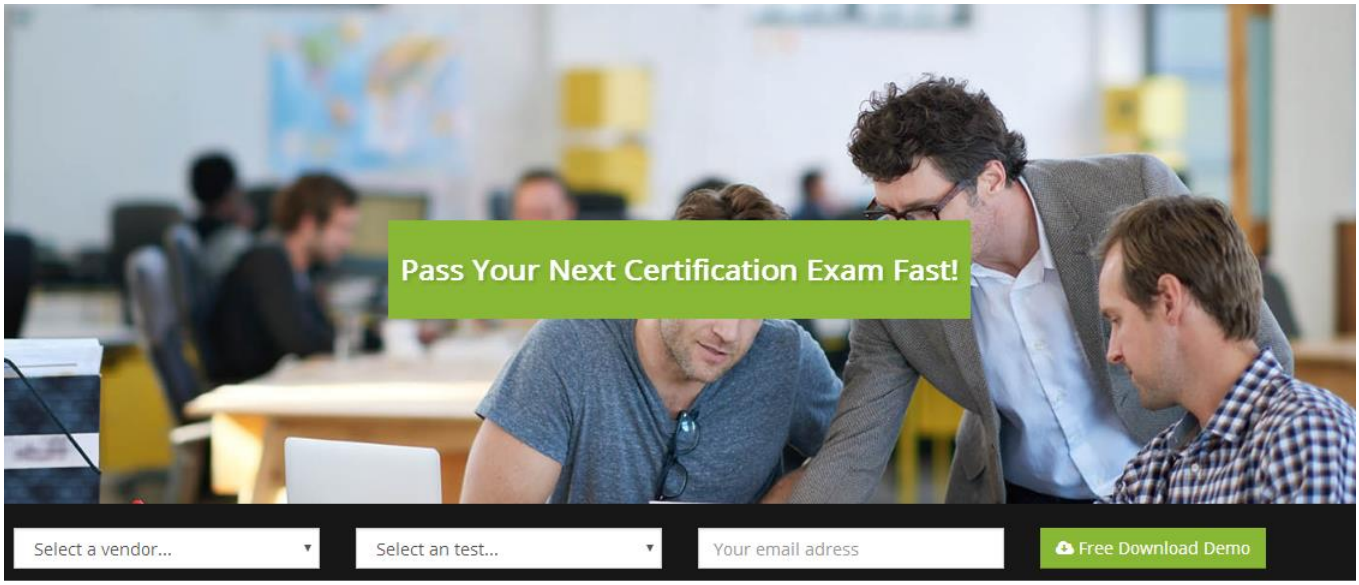
ITPassLeader



Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.itpassleader.com

High-praise Exam Dumps Questions grant you success by high pass rate - ITPassLeader

Exam : **301b**

Title : LTM Specialist: Maintain & Troubleshoot

Vendor : F5

Version : DEMO

NO.1 Which file should be modified to create custom SNMP alerts?
A. /config/alert.conf
B. /etc/alertd/alert.conf
C. /config/user_alert.conf
D. /etc/alertd/user_alert.conf
Answer: C

NO.2 An LTM Specialist is working with an LTM device configured with 10 virtual servers on the same domain with a different key/cert pair per virtual. For examplE. www.example.com; ftp.example.com; ssh.example.com; ftps.example.com.
What should the LTM Specialist do to reduce the number of objects on the LTM device?
A. create a 0 port virtual server and have it answer for all protocols
B. create a 0.0.0.0:0 virtual server thus eliminating all virtual servers
C. create a transparent virtual server thus eliminating all virtual servers
D. create a wildcard certificate and use it on all *.example.com virtual servers
Answer: D

NO.3 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. Enable Datagram LB
B. Disable Datagram LB
C. Set Timeout to Indefinite
D. Set Timeout to Immediate
Answer: A

NO.4 An LTM Specialist is troubleshooting an issue where one LTM device in a three LTM device group is failing to synchronize after a synchronize to group command is issued. The LTM Specialist verifies there are no packet filters, port lock down, or network issues preventing the connection.
What are two reasons the synchronization group is having issues? (Choose two.)
A. Certificates expired on all of the peer LTM devices.
B. Certificates stored for the device trusts on all of the peer LTM devices are corrupted.
C. Admin passwords changed on one of the peer LTM devices that are able to synchronize.
D. Admin password changed on the LTM device NOT receiving the synchronized configurations.
E. Certificates stored for the device trusts on the LTM device NOT receiving the configuration are corrupted.
Answer: D,E

NO.5 A client is attempting to log in to a web application that requires authentication. The following HTTP headers are sent by the client:
GET /owa/ HTTP/1.1 Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ= User-Agent: curl/7.26.0 Host: 10.0.0.14 Accept: */* Accept-EncodinG. gzip,deflate
The web server is responding with the following HTTP headers:
HTTP/1.1 401 Unauthorized Content-TypE. text/html Server: Microsoft-IIS/7.5

WWW-AuthenticatE. NTLM
DatE. Wed, 16 Aug 1977 19:12:31 GMT
Content-LengtH. 1293
The client has checked the login credentials and believes the correct details are being entered.
What is the reason the destination web server is sending an HTTP 401 response?
A. The username and password are incorrect.
B. The server has an incorrect date configured.
C. The client is using the wrong type of browser.
D. The wrong authentication mechanism is being used.
Answer: D

NO.6 A new VLAN vlan301 has been configured on a highly available LTM device in partition ApplicationA. A new directly connected backend server has been placed on vlan301. However, there are connectivity issues pinging the default gateway. The VLAN self IPs configured on the LTM devices are 192.168.0.251 and 192.168.0.252 with floating IP 192.168.0.253. The LTM Specialist needs to perform a packet capture to assist with troubleshooting the connectivity.
Which command should the LTM Specialist execute on the LTM device command line interface to capture the attempted pings to the LTM device default gateway on VLAN vlan301?
A. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.253'
B. tcpdump -ni vlan301 'host 192.168.0.253'
C. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.251 or host 192.168.0.252'
D. tcpdump -ni vlan301 'host 192.168.0.251 or host 192.168.0.252'
Answer: A

NO.7 An LTM Specialist must perform a hot fix installation from the command line.
What is the correct procedure to ensure that the installation is successful?
A. import the hot fix to the /var/shared/images directory check the integrity of the file with an md5 checksum tmsh apply sys software hotfix volume <volume_name> <hotfix_name>.iso
B. import the hot fix to the /var/shared/images directory check the integrity of the file with an md5 checksum tmsh install sys software hotfix <hotfix_name>.iso volume <volume_name>
C. import the hot fix to the /shared/images directory check the integrity of the file with an md5 checksum tmsh apply sys software hotfix volume <volume_name> <hotfix_name>.iso
D. import the hot fix to the /shared/images directory check the integrity of the file with an md5 checksum tmsh install sys software hotfix <hotfix_name>.iso volume <volume_name>
Answer: D

NO.8 -- Exhibit -

```
PACKET CAPTURE DIRECT TO WEB SERVER

19:50:28.497103 IP 172.31.5.100.49715 > 10.31.80.23.80: S 751670031:751670031(0) win 8192 <mss 1460,nop,wscale
2,nop,nop,sackOK>
19:50:28.501117 IP 10.31.80.23.80 > 172.31.5.100.49715: S 1684731463:1684731463(0) ack 751670032 win 8192 <mss
1460,nop,wscale 8,nop,nop,sackOK>
19:50:28.502839 IP 172.31.5.100.49715 > 10.31.80.23.80: . ack 1 win 16425
19:50:28.524386 IP 172.31.5.100.49715 > 10.31.80.23.80: P 1:249(248) ack 1 win 16425
19:50:28.527024 IP 10.31.80.23.80 > 172.31.5.100.49715: P 1:344(343) ack 249 win 256
19:50:28.738115 IP 172.31.5.100.49715 > 10.31.80.23.80: . ack 344 win 16339
19:50:30.855229 IP 172.31.5.100.49716 > 10.31.80.23.80: S 3248492897:3248492897(0) win 8192 <mss 1460,nop,wscale
2,nop,nop,sackOK>
19:50:30.858672 IP 10.31.80.23.80 > 172.31.5.100.49716: S 1034885901:1034885901(0) ack 3248492898 win 8192 <mss
1460,nop,wscale 8,nop,nop,sackOK>
19:50:30.861972 IP 172.31.5.100.49716 > 10.31.80.23.80: . ack 1 win 16425
19:50:30.861980 IP 172.31.5.100.49716 > 10.31.80.23.80: P 1:202(201) ack 1 win 16425
19:50:30.865070 IP 10.31.80.23.80 > 172.31.5.100.49716: P 1:1406(1405) ack 202 win 256
19:50:30.867112 IP 172.31.5.100.49716 > 10.31.80.23.80: R 202:202(0) ack 1406 win 0
```

```
PACKET CAPTURE THROUGH LTM DEVICE

EXTERNAL VLAN
20:05:33.719423 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:33.958133 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.722498 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.972779 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:42.723128 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,nop,sackOK>
20:05:42.972755 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,nop,sackOK>

INTERNAL VLAN
20:05:33.719791 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:33.958189 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.722525 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.972805 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:42.723147 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,nop,sackOK>
20:05:42.972776 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,nop,sackOK>
```

-- Exhibit -

Refer to the exhibits.

Users are able to access the application when connecting directly to the web server but are unsuccessful when connecting to the virtual server. Return traffic bypasses the LTM device using Layer 2 nPath routing.

Which configuration change resolves this problem?

A. Enable a SNAT pool on the LTM device.

B. Disable address translation on the LTM device.

C. Configure a route on the web server to the client subnet.

D. Configure the virtual server to listen on port 80 on the LTM device.

E. Configure the VIP address on the loopback interface of the web server.

Answer: E

NO.9 Internet clients connecting to a virtual server to download a file are experiencing about 150 ms of latency and no packet loss.

Which built-in client-side TCP profile provides the highest throughput?

A. tcp

B. tcp-legacy

C. tcp-lan-optimized

D. tcp-wan-optimized

Answer: D

NO.10 An LTM Specialist configures a new HTTP virtual server on an LTM device external VLAN. The web servers are connected to the LTM device internal VLAN. Clients trying to connect to the virtual server are unable to establish a connection. A packet capture shows an HTTP response from a web server to the client and then a reset from the client to the web server.
From which two locations could the packet capture have been collected? (Choose two.)
A. network interface of web server
B. network interface of client machine
C. internal VLAN interface of the LTM device
D. external VLAN interface of the LTM device
E. management VLAN interface of the LTM device
Answer: A,B

NO.11 -- Exhibit -

```
New TCP connection #1: 10.1.1.1(32021) <-> 10.1.1.2(443)
1 1  1351011538.3477 (0.1562)  C>S  Handshake
      ClientHello
        Version 3.0
        cipher suites
        SSL_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
        SSL_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
        SSL_DHE_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_AES_256_CBC_SHA
        SSL_RSA_WITH_CAMELLIA_256_CBC_SHA
        SSL_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_RC4_128_SHA
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_DSS_WITH_AES_128_CBC_SHA
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA256
        SSL_RSA_WITH_RC4_128_SHA
        SSL_RSA_WITH_RC4_128_MD5
        SSL_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
1 2  1351011538.3477 (0.0000)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[0]=

        cipherSuite         SSL_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
1 3  1351011538.3477 (0.0000)  S>C  Handshake
      Certificate
1 4  1351011538.3477 (0.0000)  S>C  Handshake
      CertificateRequest
        certificate_types                   rsa_sign
        certificate_authority
          30 81 98 31 0b 30 09 06 03 55 04 06 13 02 55 53
          31 0b 30 09 06 03 55 04 08 13 02 57 41 31 10 30
          0e 06 03 55 04 07 01 07 53 65 61 74 74 6c 65 31
          12 30 10 06 03 55 04 0a 13 09 4d 79 43 6f 6d 70
          61 6e 79 31 0b 30 09 06 03 55 04 0b 13 02 49 54
          31 1e 30 df 06 03 55 04 03 13 15 6c 6f 63 61 6c
          68 6f 73 74 2e 6c 6f 63 61 6c 64 6f 6d 61 69 6e
          31 29 30 27 06 09 2a 86 48 86 f7 0d 01 09 01 16
          1a 72 6f 6f 74 40 6c 6f 63 61 6c 68 6f 73 74 2e
          6c 6f 63 61 6c 64 6f 6d 61 69 6e
1 5  1351011538.3477 (0.0000)  S>C  Handshake
      ServerHelloDone
1 6  1351011538.5112 (0.1635)  C>S  Alert
    level           warning
    value         unknown value
1 7  1351011538.5112 (0.0000)  C>S  Handshake
      ClientKeyExchange
1 8  1351011538.5112 (0.0000)  C>S  ChangeCipherSpec
1 9  1351011538.5112 (0.0000)  C>S  Handshake
      Finished
1 10 1351011538.5113 (0.0000)  S>C  Alert
    level           fatal
    value           handshake_failure
1    1351011538.5113 (0.0000)  S>C  TCP FIN
1    1351011538.6866 (0.1753)  C>S  TCP FIN
```

-- Exhibit -
Refer to the exhibit.
A user is unable to access a secure application via a virtual server.
What is the cause of the issue?
A. The client authentication failed.
B. The virtual server does NOT have a pool configured.
C. The client and server CANNOT agree on a common cipher.
D. The virtual server does NOT have a client SSL profile configured.
Answer: A

NO.12 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

NO.13 A new web application is hosted at www.example.net, but some clients are still pointing to the legacy web application at www.example.com.
Which iRule will allow clients referencing www.example.com to access the new application?
A. when HTTP_REQUEST {
if {[HTTP::host] equals "www.example.*" }{
HTTP::redirect "http://www.example.net" }
}
B. when HTTP_REQUEST {
if {[HTTP::host] equals "www.example.com" }{
HTTP::redirect "http://www.example.net" }
}
C. when HTTP_DATA {
if {[HTTP::host] equals "www.example.*" }{
HTTP::redirect "http://www.example.net" }
}
D. when HTTP_RESPONSE {
if {[HTTP::host] equals "www.example.com" }{
HTTP::redirect "http://www.example.net" }
}
Answer: B

NO.14 An LTM Specialist defines a receive string in the HTTP monitor and then assigns it to the HTTP pool. The monitor has an interval of 5 seconds and a timeout of 16 seconds.
If the receive string is NOT seen in the the HTTP payload after 20 seconds, how does the LTM device mark the monitor status?
A. offline
B. unknown

C. available
D. unavailable
E. forced offline
Answer: A

NO.15 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/trafficgroup-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