



# 301B<sup>Q&As</sup>

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

## Pass F5 301B Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/301b.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by F5 Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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.

Correct Answer: D

---

**QUESTION 2**

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. promptstatsd
- B. mcpd
- C. sod
- D. bcm56xxd
- E. lind

Correct Answer: B

---

### QUESTION 3

-- Exhibit



```
ltm node /Common/192.168.44.1 {
    address 192.168.44.1
}
ltm node /Common/192.168.44.2 {
    address 192.168.44.2
}
ltm pool /Common/bigip1_gw_pool {
    gateway-failsafe-device /Common/BIGIP1.example.com
    members {
        /Common/192.168.44.1:0 {
            address 192.168.44.1
        }
    }
    min-up-members 1
    min-up-members-checking enabled
    monitor /Common/icmp_gw_monitor
}
ltm pool /Common/bigip2_gw_pool {
    gateway-failsafe-device /Common/BIGIP2.example.com
    members {
        /Common/192.168.44.2:0 {
            address 192.168.44.2
        }
    }
    min-up-members 1
    min-up-members-checking enabled
    monitor /Common/icmp_gw_monitor
}
ltm monitor gateway-icmp /Common/icmp_gw_monitor {
    defaults-from /Common/gateway_icmp
    destination 1.2.2.254:*
    interval 5
    time-until-up 0
    timeout 16
}
net route /Common/external_default_gateway {
    gw 192.168.44.1
    network default
}
```

-- Exhibit -Refer to the exhibit. A pair of LTM devices are deployed in a high-availability (HA) pair as the diagram shows. After inserting a new rule on the firewalls, the LTM devices become Standby. The rule drops all outbound sessions to the Internet. Only inbound

connections are allowed from the Internet. There are no other changes to the environment. What triggered the LTM device failover?

A. HA Group

B. Auto Failback



C. VLAN Failsafe

D. Gateway Failsafe

Correct Answer: D

---

#### QUESTION 4

A new VLAN vlan301 has been configured on a highly available LTM device in partition ApplicationA. A new directly connected backend server has been placed on vlan301. However, there are connectivity issues pinging the default gateway. The VLAN self IPs configured on the LTM devices are 192.168.0.251 and 192.168.0.252 with floating IP 192.168.0.253. The LTM Specialist needs to perform a packet capture to assist with troubleshooting the connectivity.

Which command should the LTM Specialist execute on the LTM device command line interface to capture the attempted pings to the LTM device default gateway on VLAN vlan301?

A. tcpdump -ni /ApplicationA/vlan301 \\\'host 192.168.0.253\\'

B. tcpdump -ni vlan301 \\\'host 192.168.0.253\\'

C. tcpdump -ni /ApplicationA/vlan301 \\\'host 192.168.0.251 or host 192.168.0.252\\'

D. tcpdump -ni vlan301 \\\'host 192.168.0.251 or host 192.168.0.252\\'

Correct Answer: A

---

#### QUESTION 5

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
09:35:11.073931 IP 192.168.136.100.80 > 192.168.136.1.55684: S 2273668949:2273668949(0) ack 869998902 win
4380 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
09:35:11.081928 IP 192.168.116.128.80 > 192.168.136.1.55684: S 4193259095:4193259095(0) ack 685865803 win
5840 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
09:36:11.244152 IP 192.168.136.100.80 > 192.168.116.1.55769: S 3878120666:3878120666(0) ack 3320618939 win
4380 09:36:11.244839 IP 192.168.116.1.55769 > 192.168.136.100.80: . ack 1 win 16425 09:36:11.245830 IP
192.168.116.1.55769 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425 09:36:11.245922 IP 192.168.136.100.80 >
192.168.116.1.55769: . ack 299 win 4678
```

Serverside:

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

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

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

Correct Answer: C

[301B PDF Dumps](#)

[301B Practice Test](#)

[301B Braindumps](#)