F5CAB5 Certification Training: BIG-IP Administration Support and Troubleshooting & F5CAB5 Study Guide & F5CAB5 Exam Bootcamp

Our F5CAB5 exam braindumps are famous for its advantage of high efficiency and good quality which are carefully complied by the professionals. Our excellent professionals are furnishing exam candidates with highly effective F5CAB5 Study Materials, you can even get the desirable outcomes within one week. By concluding quintessential points into F5CAB5 actual exam, you can pass the exam with the least time while huge progress.

F5 F5CAB5 Exam Syllabus Topics:

Topic	Details
Topic 1	• Identify the reason load balancing is not working as expected: This domain addresses troubleshooting load balancing by analyzing persistence, priority groups, rate limits, health monitor configurations, and availability status.
Topic 2	• Given a scenario, interpret traffic flow: This domain covers understanding traffic patterns through client-server communication analysis and interpreting traffic graphs and SNMP results.
Topic 3	• Identify the reason a virtual server is not working as expected: This section covers diagnosing virtual server issues including availability status, profile conflicts and misconfigurations, and incorrect IP addresses or ports.

>> Test F5CAB5 Testking <<

Free PDF Quiz F5 - Valid Test F5CAB5 Testking

We are a leading corporation in this line handling F5CAB5 study questions well with passing rate up to 98 and over percent, which is an unreachable goal for others. So our F5CAB5 preparation exam enjoys good sales for the excellent quality and reasonable prices in recent years. And we are so sure that we can serve you even better than you can imagine with our F5CAB5 learning guide since we are keeping on doing a better job in this career.

F5 BIG-IP Administration Support and Troubleshooting Sample Questions (Q60-Q65):

NEW QUESTION # 60
A BIG-IP Administrator observes the following messages in the /var/log/ltm log:
warning tmm[pid]: 011e0002: sweeper_segment_cb_any: Aggressive mode /Common/default-eviction-policy activated (0) (global memory) (345209/690176 pages) warning tmm[pid]: 011e0003: Aggressive mode sweeper /Common/default-eviction-policy (0) (global memory) 1 connections killed warning tmm[pid]: 011e0003: Aggressive mode sweeper /Common/default-eviction-policy (0)

(global memory) 1 connections killed warning tmm[pid]: 011e0003: Aggressive mode sweeper /Common/default-eviction-policy (0) (global memory) 1 connections killed What is happening when the BIG-IP Administrator sees the messages displayed above? (Choose two answers)

- A. The global eviction policy is triggered due to swap memory being used too high
- B. The BIG-IP system starts reaping connections; all the connections will be dropped
- C. The global eviction policy is triggered due to TMM memory exhaustion
- D. The BIG-IP system starts reaping connections; some connections will be dropped

Answer: C,D

Explanation:
Comprehensive and Detailed 150 to 250 Words Explanation From BIG-IP Administration, Support, and Troubleshooting Documents:
These log messages indicate that the BIG-IP system's Traffic Management Microkernel (TMM) has entered aggressive eviction mode due to high global memory utilization. When TMM memory consumption reaches critical thresholds, BIG-IP activates the default eviction policy to protect system stability and prevent a full traffic processing failure. This condition directly corresponds to Option A, where the global eviction policy is triggered because TMM memory resources are nearing exhaustion.
Once aggressive mode is activated, BIG-IP begins using the connection sweeper mechanism, which selectively terminates existing connections to free memory. The repeated log entries stating "1 connections killed" confirm that the system is reaping some connections, not all connections. This behavior matches Option C. The eviction process is incremental and controlled, targeting idle, low-priority, or least-recently-used connections first to minimize impact on active traffic.
Option B is incorrect because BIG-IP does not drop all connections during aggressive mode; it only removes enough connections to relieve memory pressure. Option D is also incorrect because TMM eviction is based on TMM global memory usage, not swap memory utilization. TMM does not rely on swap space in the same way the host Linux system does.
These messages are a critical warning sign that the system is under memory stress and may require traffic optimization, connection limits, or hardware scaling.

NEW QUESTION # 61
A BIG-IP Administrator needs to view the CPU utilization of a particular Virtual Server. Which section of the Configuration Utility should the administrator use for this purpose?

- A. S70tatistics > Module Statistics >71 Local Traffic > Virtual Addresses
- B. Statistics > Module Statistics > Traffic Summary
- C. Statistics > Module Statistics > Local Traffic > Virtual Servers
- D. Statistics > Analytics > Process CPU Utilization

Answer: C

Explanation:
Monitoring granular resource utilization is essential when troubleshooting performance degradation for specific applications. While global system stats show overall hardware health, they do not pinpoint which virtual server is overconsuming resources during traffic spikes. To identify the specific application causing a high CPU load, the administrator should navigate to Statistics > Module Statistics > Local Traffic > Virtual Servers7474. This section provides detailed metrics for each virtual server, including CPU cycles used for traffic processing and iRule execution75. Identifying a "top-talker" or a problematic virtual server allows the administrator to take targeted action, such as optimizing an inefficient iRule, adjusting compression levels, or offloading the virtual server to a different device group76. This targeted troubleshooting ensures that one high-demand virtual server does not negatively impact the performance of other services running on the same BIG-IP hardware, maintaining overall system stability and resource availability

NEW QUESTION # 62
Refer to the exhibit.

A pool member fails the monitor checks for about 30 minutes and then starts passing the monitor checks. New traffic is NOT being sent to the pool member. What is the likely reason for this problem? (Choose one answer)

- A. The pool member is disabled.
- B. Time Until Up is zero.
- C. Manual resume is enabled.
- D. Monitor Type is TCP Half Open.

Answer: C

Explanation:
In BIG-IP LTM, health monitors are used to determine if a pool member or node is "Up" and capable of processing traffic. Based on the provided exhibit, the specific configuration setting causing this behavior is Manual Resume.
Manual Resume (Enabled/Yes): When the Manual Resume setting is set to Yes, it changes the default behavior of how a pool member returns to service. Under normal circumstances (Manual Resume set to No), once a pool member starts passing its health check again, the BIG-IP system automatically marks it as "Up" and resumes sending traffic to it. However, with Manual Resume enabled, the system will continue to mark the pool member as "Down" (or "Unavailable") even after it passes the health check. It requires a manual intervention by an administrator to reset the status and allow traffic to flow again.
Exhibit Analysis: The screenshot clearly shows the Manual Resume radio button is selected as Yes. This explains why, even after the

pool member "starts passing the monitor checks," it does not receive new traffic.
Incorrect Options Analysis:
Time Until Up (0 seconds): This setting defines how long a member must consistently pass health checks before being marked "Up." If it is set to 0, it should actually return to service immediately upon the first successful check.
The pool member is disabled: While a disabled member won't receive traffic, the question focuses on why passing a monitor check didn't restore service, which points specifically to the monitor configuration shown.
Monitor Type is TCP Half Open: This is simply the method used to check the service (sending a SYN and expecting a SYN-ACK, then sending a RST). It determines how the check is performed, not what happens after the check succeeds.
https://my.f5.com/manage/s/article/K83316932

NEW QUESTION # 63
Which two methods should the BIG-IP Administrator troubleshoot a Pool-member that's been marked "DOWN" by its Health Monitor? (Pick the 2 correct responses below)

- A. Review the Pool & Pool-member Statistics table for error data.
- B. Enable Monitor Logging for the Pool-member that's "DOWN".
- C. Review the BIG-IP's routing table using "netstat -rn" to show all routes.
- D. Collect a TCPdump packet capture for the "DOWN" Pool-member.

Answer: B,D

Explanation:
When a health monitor marks a member "Down," the goal is to determine if the issue is at the network level or the application level.
Monitor Logging (Option A): In the Pool Member configuration, an administrator can enable "Monitor Logging". This generates a detailed text file in /var/log/monitors/ that shows the exact "Send" string sent by the BIG-IP and the exact "Receive" string (or lack thereof) returned by the server.
TCPdump (Option C): This is the most definitive way to see if the monitor traffic is even leaving the BIG-IP and if the server is responding with a TCP RST (reset) or an ICMP unreachable message. A command such as tcpdump -ni <vlan> host <member_ip> and port <member_port> is standard for this task.
Why not others? While the routing table (Option B) is useful for general connectivity, if other members in the same subnet are "Up," the routing is likely fine. Statistics (Option D) show that it is down but rarely why it is down at a protocol level.

NEW QUESTION # 64
A traffic group includes four devices. The failover method is HA order. The failover order is:
- BIGIP-D
- BIGIP-B
- BIGIP-C
- BIGIP-A
Auto fallback is enabled. BIGIP-D has been forced to standby. BIGIP-B was active before being rebooted. Which device is active when BIGIP-B is up after the reboot?

- A. BIGIP-B
- B. BIGIP-C
- C. BIGIP-D
- D. BIGIP-A

Answer: A

Explanation:
To understand which device becomes active, we must look at how the BIG-IP system handles HA Order and Auto Fallback within a traffic group.
HA Order Mechanism: When a traffic group is configured with an "HA Order" list, the system prefers to host the traffic group on the highest-ranking available device in that list (1 being the highest).
The Impact of "Forced to Standby": BIGIP-D is the first choice in the order, but it has been
"Forced to Standby." This state is persistent and manual; until an administrator releases the
"Force to Standby" state, the device is ineligible to host the traffic group, effectively removing it from the top of the preference list.
Auto Fallback: When "Auto Fallback" is enabled, the traffic group will automatically migrate back to a higher-priority device in the HA order as soon as that device becomes available and is in a healthy "Standby" state.
The Scenario Logic:

1. BIGIP-D is ineligible (Forced Offline/Standby).
2. BIGIP-B is the next highest device in the HA Order (Rank 2).
3. While BIGIP-B was rebooting, the traffic group would have failed over to BIGIP-C (Rank 3).
4. Once BIGIP-B finishes booting and joins the cluster in a "Standby" state, the Auto Fallback setting triggers.
5. Because BIGIP-B is higher in the HA Order than the current active device (BIGIP-C) and the only device above it (BIGIP-D) is ineligible, the traffic group fails back to BIGIP-B.

NEW QUESTION # 65

.....

Our F5CAB5 exam simulation is selected many experts and constantly supplements and adjust our questions and answers. When you use our F5CAB5 study materials, you can find the information you need at any time. When we update the F5CAB5 preparation questions, we will take into account changes in society, and we will also draw user feedback. If you have any thoughts and opinions in using our F5CAB5 Study Materials, you can tell us. We hope to grow with you and the continuous improvement of F5CAB5 training engine is to give you the best quality experience.